DUQUESNE LAW REVIEW

VOLUME 59, NUMBER 2 SUMMER 2021

Duquesne Law Review

Volume 59, Number 2, Summer 2021

In Memoriam

Professional Articles

Student Articles

Duquesne Law Review is published in Pittsburgh, Pennsylvania. Correspondence may be addressed to: *Duquesne Law Review*, Duquesne University School of Law, 600 Forbes Avenue, Pittsburgh, Pennsylvania 15282.

The subscription price is $30.00 per volume. Subscription inquiries should be addressed to the attention of the Business Manager. Subscriptions will be cancelled only after the entire volume for which the subscription has been entered is printed and delivered. Subscriptions are automatically renewed unless otherwise stipulated. Subscribers should report non-receipt of an issue within six months of its mailing. After six months, replacement issues will not be provided free of charge.

This issue is available from *Duquesne Law Review* at $10.00 per copy for three years from its initial printing. Archived issues are available through William S. Hein & Co., Inc., 2350 North Forest Road, Getzville, New York 14068, at $18.00 per copy. Back issues can also be found in electronic format on HeinOnline, http://heinonline.org/.

Citations conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 21st ed. 2020). Readers are invited to submit manuscripts for possible publication. Manuscripts should be addressed to the attention of the Executive Articles Editors. Readers are also invited to submit letters to the Editor in response to the works contained herein. Letters to the Editor should be addressed to the attention of the Editor-in-Chief.

Duquesne Law Review

Volume 59

Published by the students of the Duquesne School of Law
Member, National Association of Law Reviews

DUQUESNE UNIVERSITY
SCHOOL OF LAW
2020–2021

Administration

APRIL M. BARTON, B.S., J.D.
Dean, and Professor of Law

ELLA A. KWISNEK, B.A., J.D., M.S.Ed.
Associate Dean for Students and Assistant Professor

ANN L. SCHIAVONE, B.A., J.D.
Associate Dean for Faculty Scholarship and Associate Professor of Law

TARA WILLKE, B.A., J.D.
Associate Dean for Academic Affairs and Associate Professor of Law

Full-Time Faculty

STEVEN BAICKER-MCKEE, B.A., J.D.
Joseph A. Katarincic Chair of Legal Process and Civil Procedure and Associate Professor of Law

PABLO ECHEVERRI, B.A., J.D.
Assistant Professor of Law

RICHARD GAFFNEY Jr., B.A., M.B.A., J.D.
Director of Advanced Analytics and Assistant Professor of Legal Skills

AMAN GEBRU, S.J.D., LL.M., LL.B.,
Assistant Professor of Law

KENNETH G. GORMLEY, B.A., J.D.
Duquesne University President and Professor of Law

RHONDA GAY HARTMAN, B.A., J.D.
Distinguished Lecturer of Law

RICHARD HEPPNER, B.A., M.A., Ph.D, J.D.
Assistant Professor of Law

MARYANN HERMAN, B.A., J.D.
Director of Academic Excellence and Assistant Professor of Legal Skills

WILSON R. HUHN, B.A., J.D.
Professor of Law

JALILA JEFFERSON-BULLOCK, B.A., M.A., J.D.
Associate Professor of Law

RONA KAUFMAN, B.A., J.D., LL.M.
Associate Professor of Law

ROBERT F. KRAVETZ, B.A., J.D.
Assistant Professor of Law

ELLA A. KWISNEK, B.A., J.D., M.S.Ed.
Associate Dean for Students and Assistant Professor

BRUCE S. LEDEWITZ, B.S.F.S., J.D.
Adrian Van Kaam Endowed Chair in Scholarly Excellence and Professor of Law

JAN M. LEVINE, B.A., J.D.
Director of Legal Research and Writing and Professor of Law

FRANK Y. LIU, LL.B., M.C.J., M.L.S.
Professor Emeritus

ASHLEY LONDON, B.A., J.D.
Director of Bar Studies and Assistant Professor of Legal Skills

EMILE LOZA DE SILES, B.S., M.B.A., J.D.
Assistant Professor of Law

MARISSA MEREDITH, B.A., J.D.
Assistant Professor of Law

JOSEPH SABINO MISTICK, B.A., J.D.
Associate Professor of Law

JANE CAMPBELL MORIARTY, B.A., J.D.
Carol Los Mansmann Chair in Faculty Scholarship, and Professor of Law

KATHERINE NORTON, B.S., J.D.
Director of Clinical and International Programs and Assistant Professor of Law

WESLEY OLIVER, B.A., J.D., LL.M., J.S.D.
Director of Criminal Justice Program, and Professor of Law

SETH C. ORANBURG, B.A., J.D.
Assistant Professor of Law

GRACE W. ORSATTI, B.S., J.D.
Externship and Pro Bono Director and Assistant Professor of Clinical Legal Education

JOHN T. RAGO, B.A., J.D.
Associate Professor of Law

ANN L. SCHIAVONE, B.A., J.D.
Associate Dean for Faculty Scholarship and Associate Professor of Law

TIFFANY SIZEMORE-THOMPSON, B.S., J.D.
Assistant Professor of Clinical Legal Education

TARA WILLKE, B.A., J.D.
Associate Dean for Academic Affairs and Associate Professor of Law

Law Librarian Faculty

TSEGAYE BERU, B.A., M.L.I.S., J.D.
Associate Director for Faculty Research and Outreach Services

AMY LOVELL, B.A., M.L.S.
Assistant Director for Resource Development and Metadata Services

CHARLES SPROWLS, B.S.I.S., M.L.I.S.
Head of Information Access and

Student Services
JULIE TEDJESKE, M.L.S, M.S, J.D.
Electronic Resources and Instructional Services Librarian

Adjunct Faculty
DEAN ALDERUCCI, B.S., M.S., LL.M.
ANNE ALTIERI-DELANEY, B.S., M.A.L.D., J.D.
WILLIAM AXTMAN, J.D.
ROBERT S. BARKER, B.A., J.D., M.A.
DAVID BELCZYK, B.S., J.D.
MARK BERGSTROM, M.P.A., B.A.
JOSEPH BUCCI, B.A., J.D.
THOMAS CORBETT, B.A., J.D.
Executive in Residence
ROBERT F. DALEY, B.S., J.D.
JOSEPH DECKER, B.S., J.D.
Honorable JEFFERY DELLER, B.A., J.D.
ELIZABETH A. DELOSA, J.D., B.A.
Managing Attorney for the Pennsylvania Innocence Project's Pittsburgh Office
JENNIFER DIGIOVANNI, B.A., J.D.
JAMES G. DILMORE, J.D., M.S./Ph.D
KEVIN GARBER, J.D.
A. MICHAEL GIANANTONIO, B.A., J.D.
PETER GIGLIONE, B.A., J.D.
Coordinator of Trial Advocacy Program
JULIA M. GLENCER, B.A., J.D.
Associate Director for Thomas R. Kline Center for Judicial Education
JAMES F. (JAY) GLUNT, B.S., J.D.
JOHN D. GOETZ, B.A., J.D.
BARBARA GRIFFIN, B.S., J.D.
ROSALYN GUY-MCCORKLE, J.D.
Honorable THOMAS M. HARDIMAN B.A., J.D.
Honorable ELLIOT HOWSIE, B.S., M.S., J.D.
KATHERINE JANOCSKO, B.A., J.D.
DAVID JAMISON, B.A., M.A., J.D.
ERIN R. KARSMAN, B.A., J.D.
Director of Thomas R. Kline Center for Judicial Education and Director of the Appellate Program
SHANICKA KENNEDY, B.A., J.D.
CARL KRASIK, A.B., J.D.
DANIEL KUNZ, B.S., M.B.A., J.D.
THOMAS KUNZ, JCD, STL
Honorable MAUREEN E. LALLY-GREEN, B.S., J.D.
DOROTHEE M. LANDGRAF, LL.M
GREGORY LANDGRAF, J.D., CPA/ABV, CGMA, CFE
TRACEY MCCANTS LEWIS, B.A., J.D.
Honorable JEFFREY A. MANNING, B.A., J.D.
MARTIN MCKOWN, B.S., J.D.
APRIL L. MILBURN-KNIZNER, B.A., J.D.
JONATHAN MOORE, B.A., J.D.
GREGORY NORTON, B.A., J.D.
JACQULYN OBARA, B.S., J.D.
BETHANY PARKER, B.A., J.D.
STACIE PATTERSON, B.A., J.D., M.A.
ADRIAN N. ROE, B.A., J.D.
JUSTIN ROMANO, J.D.
ERICA SABATINI, B.S., J.D.
DAVID SCHRAMM, B.S., J.D.
BARBARA SIMANEK, B.A., M.B.A., J.D.
MICHAEL D. SIMON, J.D., B.A.
SAMUEL SIMON, B.S., J.D.
MARCY SMOREY-GIGER, B.S., M.S., J.D.
HENRY M. SNEATH, B.A., J.D.
PATRICK SOREK, B.A., J.D., LL.M.
DAVID SPURGEON, B.A., J.D.
STACEY STEINER, J.D.
CYRIL H. WECHT, B.S., M.D., J.D.
DAVID WECHT, J.D.
JACQUELINE WOODWARD, B.A., M.A., J.D.

IN MEMORIAM: RHONDA GAY HARTMAN

The editors of the *Duquesne Law Review* respectfully dedicate Volume 59 to the late Professor Rhonda Gay Hartman, a lawyer and wonderful teacher who by her dedication to legal rights of children inspired us all.

Remembering Professor Rhonda Gay Hartman

*Ken Gormley**

Professor Rhonda Gay Hartman, who passed away unexpectedly in April of 2021 as this issue of the *Duquesne Law Review* was being finalized, was an elegant, forward-thinking, brilliant scholar and teacher. She left a lasting imprint on legal academia, on the Duquesne community, and on the thousands of students whom she taught and mentored for over twenty-five years.

I was privileged to meet Rhonda when she was a student in my State Constitutional Law course at the University of Pittsburgh School of Law in the late 1980s. Already an advanced student completing graduate studies in public and international affairs, she was light-years ahead of most law students beginning their studies. When the Kentucky Supreme Court asked me to write an article on Kentucky constitutional law, I found myself facing a quandary: I already had committed myself to writing a major law journal article on privacy law and had no time to embark on another project, at least by myself. I discussed the idea with Rhonda, who was finishing up her legal studies, knowing that her ultimate goal was to be a legal scholar, writer, and teacher. She immediately accepted the challenge and agreed to collaborate on the project. The finished product, *The Kentucky Bill of Rights: A Bicentennial Celebration*, appeared in the *Kentucky Law Journal* in the 1992 issue.[1]

Shortly thereafter, we collaborated on a second piece, *Privacy and the States*, published by *Temple Law Review* in 1992,[2] which focused on state constitutional privacy protections. Rhonda's writing and scholarship were impeccable. She was thorough, innately analytical, and cared deeply about helping to develop the law in this then-emerging field. Two decades later, those two pieces have contributed to the evolution of state constitutional law in Kentucky, Pennsylvania, and nationally.[3]

---

* President, Duquesne University, Professor of Law, and former Dean of the School of Law.

1. Ken Gormley & Rhonda G. Hartman, *The Kentucky Bill of Rights: A Bicentennial Celebration*, 80 KY. L.J. 1 (1992).

2. Ken Gormley & Rhonda G. Hartman, *Privacy and the States*, 65 TEMP. L. REV. 1279 (1992).

3. Hunter v. Commonwealth, 587 S.W.3d 298, 305 (Ky. 2019); Posey v. Commonwealth, 185 S.W.3d 170, 182 (Ky. 2006) (Roach, J., concurring); Commonwealth v. Wasson, 842

Fortunately, those early projects did not define, or limit, Rhonda's growth as a legal scholar. After serving as a law clerk to U.S. District Judge Alan N. Bloch of the Western District of Pennsylvania, she began collaborating on projects involving health care law and ethics, primarily at the University of Pittsburgh. When I accepted a permanent teaching post at Duquesne University School of Law in 1994, I immediately urged the dean to hire Rhonda to serve as an adjunct faculty member and research scholar at the law school, recognizing her potential as a rising star.

In short order, she was placing articles in nationally prominent journals at a time when Duquesne University School of Law was seeking to enhance its visibility through first-rate scholarship. During this time, Rhonda became Professor Hartman and began developing a passion for health care ethics, adolescent rights, and other topics that would come to define her life and work as a legal scholar.

In 1993, Professor Hartman authored *Beyond* Moore*: Issues of Law and Policy Impacting Human Cell and Genetic Research in the Age of Biotechnology*,[4] the first in what would become an impressive portfolio of scholarly writings in this area. The article, published in the Journal of Legal Medicine, examined the California Supreme Court's landmark decision in *Moore v. Regents of the University of California*[5] to impose a fiduciary duty of disclosure on physicians who had a personal interest, whether research-oriented or commercial in purpose, in a patient's genetic material.

Professor Hartman persuasively argued that the law and public policy had to expand to address the novel issues that were bound to arise in the emerging field of genetic engineering. She further contended that a balance had to be struck between upholding a patient's right of self-determination to make decisions about his or her genetic material and incentivizing investments in biomedical research. The article generated sufficient interest that Professor Hartman presented it to colleagues at the University of Pittsburgh's Center of Medical Ethics. This was the first of many presentations she would make in sharing her work throughout her distinguished career.

S.W.2d 487, 492 (Ky. 1993). *See also*, *e.g.*, Daniel J. Canon, *Challenges to the Residency Requirements of the Personal Responsibility and Work Opportunity Reconciliation Act Under the Kentucky Constitution*, 45 BRANDEIS L.J. 151, 162 (2006); Seth F. Kreimer, *The Right to Privacy in the Pennsylvania Constitution*, 3 WIDENER J. PUB. L. 77, 89 (1993); Jason Reiser, *III. Individual Rights*, 28 RUTGERS L.J. 932, 950 (1997).

4. Rhonda G. Hartman, *Beyond* Moore*: Issues of Law and Policy Impacting Human Cell and Genetic Research in the Age of Biotechnology*, 14 J. LEGAL MED. 463 (1993).

5. Moore v. Regents of the University of California, 793 P.2d 479 (Cal. 1990).

In 2000, Professor Hartman authored *Adolescent Autonomy: Clarifying an Ageless Conundrum*, published in the *Hastings Law Journal*.[6] The article was an impressive accomplishment for a junior law school faculty member; to this day, it remains a highly influential work of scholarship on the topic of adolescent decision-making, having been cited in seventy-six scholarly pieces.[7]

The article showcased Professor Hartman's new and specialized interest in adolescent autonomy and rights, a subject she would cultivate into an area of expertise. This was much more than an academic exercise for her. As a person who cared deeply about others, she was convinced the issue was worthy of understanding because it affected real people in the real world. In fact, Professor Hartman explained that the inspiration for the piece was a discussion she had with pediatricians who recounted the difficulties they faced in treating their adolescent patients because children and youth under eighteen were presumed to lack the ability to make their own health care choices.

Professor Hartman's thesis in the article was that the traditional presumption of adolescent decisional incapacity was an outdated artifact. To drive home her point, she presented an in-depth discussion of adolescent decisional capacity in numerous arenas of law, including health care, end-of-life, mental health treatment, medical experimentation, organ transplantation, and procreative choice. Professor Hartman then proposed an adolescent autonomy model based on adolescent decisional capacity that helped to provide the foundation for legal rules and legislative policies in those circumstances in which adolescents were competent to decide what was best for them.

Subsequently, in *Adolescent Decisional Autonomy for Medical Care: Physician Perceptions and Practices*,[8] an article that appeared in a University of Chicago Law School Roundtable, Professor Hartman combined her growing expertise in the topic of adolescent autonomy, her interest in health care issues, and her desire to provide concrete guidance to policymakers. In meticulous detail, a feature that typified all of her writing, she discussed a study that revealed

---

6. Rhonda Gay Hartman, *Adolescent Autonomy: Clarifying an Ageless Conundrum*, 51 HASTINGS L.J. 1265 (2000).

7. *See, e.g.*, Tamar R. Birckhead, *Toward a Theory of Procedural Justice for Juveniles*, 57 BUFF. L. REV. 1447 (2009); Kimberly M. Mutcherson, *Whose Body Is It Anyway? An Updated Model of Healthcare Decision-Making Rights for Adolescents*, 14 CORNELL J.L. & PUB. POL'Y 251 (2005); Jennifer L. Rosato, *Let's Get Real: Quilting a Principled Approach to Adolescent Empowerment in Health Care Decision-Making*, 51 DEPAUL L. REV. 769 (2002).

8. Rhonda Gay Hartman, *Adolescent Decisional Autonomy for Medical Care: Physician Perceptions and Practices*, 8 U. CHI. L. SCH. ROUNDTABLE 87 (2001).

physicians' belief that adolescents were capable of making health care decisions for themselves but benefitted from consulting with a "trusted adult" during the decision-making process. Professor Hartman addressed the lessons the study provided for medical practitioners. She also listed areas of inquiry that could provide policymakers with the kind of concrete data they would need to formulate policies that respected the capacity of adolescents to direct their own health care choices.

More articles followed, including *Coming of Age: Devising Legislation for Adolescent Medical Decision-Making*,[9] published by the *American Journal of Law & Medicine*, *AIDS and Adolescents*,[10] which appeared in the *Journal of Health Care Law & Policy*, and *Word from the Academies: A Primer for Legal Policy Analysis Regarding Adolescent Research Participation*,[11] published in the *Rutgers Journal of Law & Public Policy*. Through this steady body of work, Professor Hartman made a name for herself in the fields of health care law and adolescent rights. As a result, she was invited to share her expertise at seminars and conferences sponsored by law schools, interdisciplinary centers of study, healthcare entities, medical institutions, and policy think tanks regionally and around the country.

Professor Hartman's scholarship took an interesting turn toward a new subject in 2005, bringing her additional accolades, when she became interested in reconstructive transplant surgery and the thorny legal and ethical issues arising from newly developed face and hand transplants. The theme that ran throughout her writings was that the scientific strides making face transplants possible should continue; however, progress had to proceed carefully because a person's face is so deeply intrinsic to that person's identity and sense of self.

In *Face Value: Challenges of Transplant Technology*,[12] published in the *American Journal of Law and Medicine*, Professor Hartman explored the benefits and risks of face transplantation, the donation and informed consent processes, the procedures for selecting recipients, and the desirability of regulatory oversight of the field. In *The Face of Dignity: Principled Oversight of Biomedical*

9. Rhonda Gay Hartman, *Coming of Age: Devising Legislation for Adolescent Medical Decision-Making*, 28 AM. J.L. & MED. 409 (2002).

10. Rhonda Gay Hartman, *AIDS and Adolescents*, 7 J. HEALTH CARE L. & POL'Y 280 (2004).

11. Rhonda Gay Hartman, *Word from the Academies: A Primer for Legal Policy Analysis Regarding Adolescent Research Participation*, 4 RUTGERS J.L. & PUB. POL'Y 151 (2006).

12. Rhonda Gay Hartman, *Face Value: Challenges of Transplant Technology*, 31 AM. J.L. & MED. 7 (2005).

Innovation,[13] she went on to offer a thought-provoking premise: she argued that, because the face is so deeply tied to personhood, the concept of dignity—i.e., the idea that each one of us has inherent value—deserved a special place in shaping public debate on, and steering scientific progress in, this type of human transplantation. This article generated so much interest that the British Broadcasting Corporation and France's premier medical and scientific institution, the Université Pierre et Marie Curie, invited Professor Hartman to discuss her ideas through interviews and presentations.

Professor Hartman's scholarship in this area also led to the inclusion of her ideas in a chapter in *Transplantation of Composite Tissue Allografts*, the field's seminal medical treatise.[14] It further led to invitations to share her expertise with reconstructive surgery teams who cared for injured U.S. veterans, plastic surgeons at several of the nation's top-notch medical institutions, and to collaborations with surgeons at The Johns Hopkins Hospital and the University of Pittsburgh Medical Center to establish protocols for reconstructive transplantation.

The *Duquesne Law Review* was privileged to publish *Noblesse Oblige: States' Obligations to Minors Living with Life-Limiting Conditions*,[15] an article in which Professor Hartman provided a detailed examination of the issues surrounding minors grappling with incurable diseases and conditions. In Professor Hartman's view, such minors had not received sufficient attention from state legislative policymakers—a striking contrast to the scrutiny afforded the interests of adults living with similar conditions. In the article, Professor Hartman shone a light on the distinct challenges prevalent among minors suffering from life-limiting conditions and illuminated the crucial role state lawmakers must play in protecting their unique interests.

As Professor Hartman herself noted, the impetus for the article was her work in 2008 as a member of the Commonwealth's Pediatric Palliative and Hospice Care Task Force, which was established to examine the availability and administration of pediatric palliative and hospice care options in Pennsylvania. It was the perfect vehicle for Professor Hartman as it involved facilitating statewide discussions with patients, parents, health care providers, and other

13. Rhonda Gay Hartman, *The Face of Dignity: Principled Oversight of Biomedical Innovation*, 47 SANTA CLARA L. REV. 55 (2007).

14. Rhonda Gay Hartman, *Ethical and Policy Concerns of Hand/Face Transplantation*, *in* TRANSPLANTATION OF COMPOSITE TISSUE ALLOGRAFTS 429 (Charles W. Hewitt et al. eds., 2008).

15. Rhonda Gay Hartman, *Noblesse Oblige: States' Obligations to Minors Living with Life-Limiting Conditions*, 50 DUQ. L. REV. 333 (2012).

professionals devoted to caring for children facing life-shortening or life-threatening conditions. Professor Hartman contributed to the task force's final report, a consequential document that cogently identified the challenges and systemic gaps children and their families encountered when attempting to access palliative and end-of-life care in Pennsylvania. It also recommended ways to enhance Pennsylvania's delivery of palliative and hospice care services to the children and families who needed them most.

Professor Hartman's scholarship also drew significant attention in the medical community. In 2017, she accomplished what few attorneys manage to do—get an article she authored accepted by a peer-reviewed medical publication. The *Journal of the American Medical Association, Pediatrics* published *Implementing Public Health Goals for Human Immunodeficiency Virus Infection Through Law*, which focused on the lack of progress that had been made in treating adolescents with human immunodeficiency virus (HIV) despite worldwide gains in eradicating the epidemic in adults.[16] Reiterating the theme that ran though her writings, starting in her groundbreaking piece on adolescent decision-making capacity in the *Hastings Law Journal* in 2000,[17] Professor Hartman proposed that giving adolescents access to confidential HIV testing and treatment, independent of their parents, would go a long way toward addressing untreated HIV infection among adolescents.

Professor Hartman's work generated increasing national and international interest. She was invited to lecture at Université Pierre et Marie Curie and Université de Paris-Sorbonne in Paris, France; Hofstra University in Hempstead, New York; Yale University in New Haven, Connecticut; Johns Hopkins University in Baltimore, Maryland; Georgetown University Law Center in Washington, D.C.; and University of Pittsburgh School of Medicine in Pittsburgh, Pennsylvania. Of course, Professor Hartman never turned down an invitation from colleagues at Duquesne University to lecture in schools across campus, and she did so frequently.

Professor Hartman was a forward-thinking, disciplined, and unflagging scholar. Yet, for all of her talent as a writer and academician, she was an even better teacher. For her, there was no greater joy than instilling in her students a passion for law and razor-sharp analytical thinking. She viewed each of these as powerful tools of change, and she wanted her students to enter the legal world fully equipped with a mastery and appreciation of these implements.

16. Rhonda Gay Hartman, *Implementing Public Health Goals for Human Immunodeficiency Virus Infection Through Law*, 171 JAMA PEDIATRICS 315 (2017).

17. Hartman, *supra* note 6.

Professor Hartman was unfailingly kind, generous, empathetic, gracious, and graceful in her role as an instructor in the classroom. She cared about each student, knew every person's name within five minutes, and reveled in the joys and successes of her students. She helped to lead annual trips to Washington, D.C. with faculty colleagues at the Duquesne University School of Pharmacy so that students could advocate for legislation that allowed pharmacists to better assist underprivileged patients. She invited groups of students to the elegant Duquesne Club—on her own dime—to discuss job interviewing skills and strategies for presenting themselves favorably in professional settings. She even gave new suits of clothing to women in her class who were preparing for important law firm interviews and told them to keep them so they would be prepared for their first jobs. Professor Hartman lived for each new class of law students, understanding that they were the shining instruments of positive change in the law, society, and communities where they would share their abundant talents.

It is fitting, then, that the editors of the *Duquesne Law Review* would choose to dedicate this final issue of 2021 to Professor Rhonda Hartman. She valued immensely the power of legal scholarship. She cherished, more than anything, the gift of teaching students at Duquesne University School of Law, of whom she was fiercely proud. And she prayed, in her quiet fashion, that her students would go forth and change the world and the system of laws for the better, using a tiny piece of the knowledge and passion that she passed along to them.

Now, her legacy will be secure in scores of graduates who will make contributions in every field imaginable, who have been shaped—at least in some small measure—by an extraordinary faculty member who foresaw their successes and gave them gifts that will always be with them.

Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities That Are Inextricably Linked

April Falcon Doss[*]

* April Falcon Doss is Executive Director for the Georgetown Institute for Technology Law & Policy at the Georgetown University Law Center. Prior to that, she chaired the cybersecurity and privacy practice of a major U.S. law firm, served as Senior Minority Counsel for the Russia Investigation in the United States Senate Select Committee on Intelligence, and spent over a decade at the National Security Agency, where she was Associate General Counsel for Intelligence Law.

I. INTRODUCTION

Traditionally, issues relating to information privacy have been viewed in a set of distinct, and not always helpful, stovepipes—or, as my former government colleagues often said, tongue-in-cheek, in other contexts—separate "cylinders of excellence." Thanks to the convergence of technologies and information, the once-separate realms of personal data privacy, consumer protection, and national security are increasingly interconnected. As Congress and national policymakers consider proposals for federal data privacy legislation, regulation of social media platforms, and how to prevent abuses of foreign intelligence and homeland security powers, they should be examining each of these challenges in light of the others, actively looking for synergies and overlap in the protections they may be considering for protection of personal data, individual privacy, and civil liberties.[1]

1. It should be noted that this need for cross-pollination of issues and approaches is not limited to the United States. The European Union has, for some years, taken a stove-piped view of data protection in the EU, while examining data privacy in the U.S. through a converged view that blends the commercial context of cross-border data transfers with government-directed national security activities. This difference in approach has resulted in the European insistence that commercial transactions between U.S. and European entities be subject to heightened protections for cross-border data flows because of EU objections to U.S. foreign intelligence activities, despite the fact that a great deal of U.S. intelligence analysis is shared with allied European governments. These concerns have been apparent in the establishment of restrictions on cross-border data flows under the Data Protection Directive and European negotiation of the Safe Harbor data transfer scheme with the U.S.; the collapse of the Safe Harbor regime following revelations about U.S. surveillance programs; the enactment of new cross-border data transfer restrictions under the General Data Protection Regulation; the establishment of the new Privacy Shield mechanism for cross-border transfers; and the invalidation of Privacy Shield under the *Schrems II* decision of the Court of Justice of the European Union in the summer of 2020. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, 2020 E.C.R. I-559. The dissonance between European approaches to internal and external legal regimes stems from the fact that the EU lacks competence over national security programs of its member nations—positioning the EU to criticize the U.S. without having to undertake similarly close examination of surveillance programs of EU nations, even where those programs may be similarly intrusive and less transparent. As a result, the cross-border data transfer restrictions of the GDPR are at risk of functioning more as a market protection mechanism, forcing data localization in the EU that redounds to the commercial benefit of EU-based technology platform companies, without meaningfully increasing the privacy protections of EU residents, who remain subject to surveillance pursuant to the national authorities of the member nations of the European Economic Area, where their data may be freely transported without restriction and largely without review of national security, domestic security, or other government uses of personal data.

II. "CYLINDERS OF EXCELLENCE": VIEWING DATA-RELATED ISSUES THROUGH DIFFERENT LENSES OF LAW

Historically, information privacy in the U.S. has been governed through a series of separate legal frameworks that sometimes run parallel to each other with little overlap, and other times align in ways that are orthogonal to each other. The approaches to personal information protection in the consumer privacy and national security contexts have followed largely separate paths, while the expansive territory of consumer data protection includes examples of a number of different approaches that sit, conceptually, at right angles to each other.

Consumer privacy as a whole has been regulated as a somewhat amorphous, or at least variable, concept, with different jurisdictions taking different approaches to different kinds of information, some providing only for regulatory enforcement,[2] while others support statutory damages and a private right of action.[3] One set of approaches can best be described as a mile wide but an inch deep: the classic example of this is state data breach laws, which generally aim to protect all residents in a jurisdiction and impose notification obligations on most organizations that holding those individuals' information; but those laws only cover a narrowly defined set of information, generally focused on government-issued identification numbers and financial account information.[4] In recent years, a growing number of states have enacted laws extending some rights

---

See, e.g., APRIL FALCON DOSS, CYBER PRIVACY: WHO HAS YOUR DATA AND WHY YOU SHOULD CARE 242–46 (2020).

2. For examples of federal privacy-related statutes that include regulatory enforcement mechanisms but do not support a private right of action, *see, e.g.*, Federal Trade Commission (FTC) Act, 15 U.S.C. § 45; Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506; Graham-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6821–6827; Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in 42 U.S.C. § 1320d-6).

3. For examples of federal privacy-related statutes that support a private right of action, *see, e.g.*, Privacy Act, 5 U.S.C. § 552; Fair Credit Reporting Act, 15 U.S.C. § 1681p; Video Privacy Protection Act, 18 U.S.C. § 2710(c); Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3). For examples of state privacy laws that include a private right of action, *see, e.g.*, California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.100–1798.199; Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. ANN. 14/5.

4. All fifty states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted legislation that requires the government or private entities to inform consumers of data breaches that involve personally identifiable information. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGIS. (July 17, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

and obligations to biometric information[5] and the sweeping California Consumer Privacy Act (CCPA),[6] and the amendments passed by ballot referendum as the California Privacy Rights Act, which expanded consumer rights and company obligations with respect to personal data in a number of significant ways.[7] At the federal level, consumer privacy was regulated by the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act's prohibition on unfair and deceptive acts and practices.[8] The FTC has regulated a series of privacy-related laws governing specific areas of information privacy, ranging from laws intended to protect specific groups, like the Children's Online Privacy Protection Act (COPPA),[9] to laws aimed at regulating specific industries, like the Graham-Leach-Bliley Act (GLBA)[10] regulation of the financial services industry. Employment privacy has generally been left unaddressed by federal statute,[11] while a specific, and somewhat narrow, slice of health-related privacy has been governed by the Health Insurance Portability and Accountability Act (HIPAA)[12] and HiTECH Act,[13] regulated and enforced by the Department of Health and Human Services' (DHHS) Office of Civil Rights (OCR), and a similarly specific, and somewhat narrow, side of education-related information has been subject to privacy protections under the Family Education Rights and Privacy Act (FERPA),[14] administered by the Department of Education.

Meanwhile, use of information for national security, homeland security, and law enforcement purposes has been underpinned by the Fourth Amendment to the Constitution and further regulated by a host of statutes, including the Foreign Intelligence Surveillance Act (FISA),[15] Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of

5. *See* CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; LA. STAT. ANN. §§ 51:3071–51:3077; N.Y. GEN. BUS. LAW § 899-bb; OR. REV. STAT. §§ 646A.600–646A.628.

6. CCPA §§ 1798.100–1798.199.

7. The California Privacy Rights Act was passed as Proposition 24 on the November 2020 ballot and amends key provisions of CCPA. *Id.*

8. 15 U.S.C. § 45.

9. 15 U.S.C. §§ 6501–6506.

10. 15 U.S.C. §§ 6821–6827.

11. Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. 710, 761 (2019).

12. 42 U.S.C. § 1320d-6.

13. Pub. L. No. 111-5, 123 Stat. 115 (codified at 42 U.S.C. § 300jj–300jj-51).

14. 20 U.S.C. § 1232g.

15. 50 U.S.C. §§ 1801–1813.

2001 (USA PATRIOT Act),[16] USA Freedom Act,[17] the Electronic Communications Privacy Act (ECPA),[18] the Wiretap Act,[19] the Stored Communications Act (SCA),[20] and Executive Orders, including Executive Order (EO) 12333, and federal and state laws on computer crimes, including the Computer Fraud and Abuse Act (CFAA) and similar state laws.[21]

At first blush, this separate treatment of consumer data protection and privacy in national security not only makes historical sense but appears reasonable today as well. After all, government action is appropriately subject to Constitutional constraints, including the First and Fourth Amendments, while private action by commercial or other nongovernmental actors is generally not subject to those constraints. Action by the government can have more dire consequences to civil rights and civil liberties, as one recent commenter posted on social media[22]:

For all these reasons and more, perhaps it is no wonder that recent news articles have sounded a note of alarm in their coverage of programs under which the U.S. intelligence community is allegedly purchasing commercially available information from data brokers who amass detailed personal profiles on individuals based on their

16. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (amending provisions throughout sections of the U.S. Code, such as at 50 U.S.C. § 1861(a)(1)).

17. Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in 50 U.S.C. 1881a).

18. 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3127.

19. 18 U.S.C. §§ 2510–2522.

20. 18 U.S.C. §§ 2701–2711.

21. *See* 18 U.S.C. § 1030; *see also Computer Crime Statutes*, NAT'L CONF. STATE LEGIS. (Feb. 24, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (providing a state by state breakdown of computer crimes statutes).

22. @SaysMyDerbyWife, TWITTER (Jan. 22, 2021, 1:41 PM), https://twitter.com/SaysMyDerbyWife/status/1352687762999300102.

usage of mobile phone apps.[23] Although information from cell phone apps is widely available for purchase as part of the multi-billion-dollar advertising technology, or adtech, industry,[24] the idea of its use by government officials raises any number of concerns about a possible dystopian surveillance state.

A different way of understanding these issues, however, is to look at the growing number of events in recent years in which technology and information have intersected in ways that impact individuals, geopolitics, and national and domestic security risks, and to conclude that this convergence of facts argues in favor of greater integration of legal and policy approaches as well. Viewed in that light, the news reports about the U.S. Intelligence Community (USIC) purchasing commercially available information can be seen not so much as a threat to traditional Fourth Amendment legal theory, but instead as an opportunity to holistically assess what rights, obligations, and remedies should be imposed under a cross-functional legal theory that tries to balance legitimate government aims with reasonable consumer protections and formulate a predictable set of boundaries, guardrails, and constraints.

III. UNDERSTANDING HOW THE SAME PERSONAL DATA CREATES RISKS FOR INDIVIDUAL PRIVACY AND FOR NATIONAL SECURITY

Over the past five years, a series of events have underscored the ways in which personal information and social media platforms, can be used to heighten geopolitical tensions, increase national security risk, and—to borrow a phrase from the nation's founders—threaten domestic tranquility. The most obvious categories are election security, cybersecurity threats, foreign counterintelligence operations, and domestic terrorism and insurrection, each of which is summarized with brief highlights from recent events, below.

First, election security. The Russian government's interference with the 2016 U.S. presidential election has been well documented.

---

23. *See, e.g.*, Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html (Jan. 25, 2021); Byron Tau, *Military Intelligence Agency Says It Monitored U.S. Cellphone Movements Without Warrant*, WALL ST. J. (Jan. 22, 2021, 4:19 PM), https://www.wsj.com/articles/military-intelligence-agency-says-it-monitored-u-s-cellphone-movements-without-warrant-11611350374.

24. *See, e.g.*, *Mobile Advertising Market Size, Share & Industry Analysis, by Advertising Type (In-App Ads, Mobile Rich Media, Video Ads, Banner Ads, Others), by Vertical (Retail, Media & Entertainment, Healthcare, BFSI, E-Commerce, Travel & Tourism, Automotive, Others), and Regional Forecast, 2019–2026*, FORTUNE BUS. INSIGHTS (Mar. 2020), https://www.fortunebusinessinsights.com/mobile-advertising-market-102496.

The Senate Select Committee on Intelligence (SSCI) conducted a lengthy investigation into the Russian active measures campaign, an investigation that included dozens of witness interviews, review of thousands of pages of documents, open and closed hearings, and that resulted in a lengthy, five-volume report.[25] Among other conclusions, the Senate report noted:

> [i]n 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency (IRA) used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States. . . . Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election.[26]

One key to the Russian information operation: personal data of Americans. In testimony before the Senate Judiciary Committee, Christopher Wylie, the former research director of the political consulting firm Cambridge Analytica and UK defense contractor SCL Group, described the ways in which detailed personal information about individual Facebook users was leveraged by Cambridge Analytica (CA) as part of a set of information operations intended to influence the 2016 presidential campaign. Wylie explained how SCL Group created CA with funding from American billionaire Robert Mercer, installing political operative Steve Bannon as one of CA's senior officers "to build an arsenal of informational weapons he could deploy on the American population."[27] Wylie emphasized in his written testimony that:

> [t]he purpose . . . was to develop and scale psychological profiling algorithms for use in American political campaigns. To be clear, the work of CA and SCL is not equivalent to traditional

25. *See generally* S. REP. NO. 116-290 (2020).

26. 2 S. REP. NO. 116-290, at 3 (2020).

27. *In the Matter of Cambridge Analytica and Other Related Issues: Written Statement to the U.S. S. Comm. on the Judiciary*, 115th Cong. 2 (2018) (testimony of Christopher Wylie, former Research Director, Cambridge Analytica) (available at https://www.judiciary.senate.gov/imo/media/doc/05-16-18%20Wylie%20Testimony.pdf) [hereinafter Testimony of Christopher Wylie].

> marketing, as has been claimed by some. This false equivalence is misleading. CA [specialized] in disinformation, spreading [rumors], kompromat and propaganda. Using machine learning algorithms, CA worked on moving these tactics beyond its operations in Africa or Asia and into American cyberspace.[28]

Specifically, Mr. Wylie noted:

> CA sought to identify mental and emotional vulnerabilities in certain subsets of the American population and worked to exploit those vulnerabilities by targeting information designed to activate some of the worst characteristics in people, such as neuroticism, paranoia and racial biases. This was targeted at narrow segments of the population.[29]

Wylie's sentiments are shared by others, including some U.S. legislators. Appended to the SSCI report on Russian interference with the 2016 election were the additional views expressed by individual Senators, including Sen. Ron Wyden of Oregon, who noted that at one of the Committee's hearings:

> I asked Facebook's Chief Operating Officer Sheryl Sandberg and Twitter's Chief Executive Officer Jack Dorsey whether increased protections and controls to defend personal privacy should be a national security priority. Both witnesses answered in the affirmative. *Weak data privacy policies increase the ability of foreign adversaries to micro-target Americans for purposes of election interference.* Facebook's total failure to prevent Cambridge Analytica and Aleksandr Kogan from obtaining sensitive personal data about Facebook users, as well as Facebook's troubling data-sharing partnerships with Chinese smart phone manufacturers, demonstrate *clear gaps in federal data privacy laws and highlight obvious weaknesses that could be exploited in future influence campaigns*.[30]

The known and suspected connections between CA's work and the Russian government efforts are complicated.[31] However, it is clear that the same techniques that CA was using to influence the 2016 election were also top of mind for the internet trolls at the

28. *Id.* at 5–6.
29. *Id.* at 6.
30. 2 S. REP. NO. 116-290, at 84 (2020) (emphasis added).
31. *See generally* Testimony of Christopher Wylie, *supra* note 27, at 8–10.

Russian-government-backed Internet Research Agency (IRA). Details of those activities are described in the criminal indictment that resulted from the investigation led by Special Counsel Robert Mueller.[32] Since 2016, adversarial foreign governments have continued to use social media as a vector for influencing popular opinion and attempting to influence politics and election outcomes in the United States. During the 2020 presidential campaign season, social media platforms removed accounts linked to Cuba, Russia, Saudi Arabia, Thailand, and Iran.[33] Nor is the threat limited to the U.S., as Facebook has announced the removal of networks of inauthentic accounts sponsored by the governments of Russia and Iran that were spreading misinformation, it noted that those networks sought to disrupt elections in North Africa and Latin America as well as in the U.S.[34] Of course, social media can also be a powerful medium for the growth of democracy, as witnessed by the groundswell of popular support that led to the Arab Spring.[35] While the openness of social media can be a boon for speech and democracy, examples like the 2016 Russian active measures campaign demonstrate that it can also be leveraged to destabilize democracies. The use of detailed personal profiles as a way to target social media messaging relating to political, social, and cultural issues will likely continue to be a tactic that governments around the world exploit to influence public sentiment in years to come.

Second, cybersecurity. The SolarWinds hack announced in December 2020 was the latest in a series of high-profile cybersecurity attacks that are largely believed to have been carried out by the intelligence services of an adversarial foreign government.[36] The

32. *See* Criminal Indictment, United States v. Internet Rsch. Agency LLC, No. 1:18-cr-00032-DLF, 2018 WL 914777 (D.D.C. Feb. 16, 2018).

33. *See, e.g.*, Meysam Alizadeh et al., *Are Influence Campaigns Trolling Your Social Media Feeds?*, WASH. POST (Oct. 13, 2020, 6:00 AM), https://www.washingtonpost.com/politics/2020/10/13/are-influence-campaigns-trolling-your-social-media-feeds/; Julian E. Barnes & David E. Sanger, *Iran and Russia Seek to Influence Election in Final Days, U.S. Officials Warn*, N.Y. TIMES (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html.

34. *See* Eric Tucker, *Threat to US Elections in 2020 Is Not Limited to Russia*, AP NEWS (Oct. 30, 2019), https://apnews.com/article/1af297b4625c4dd585274dfaf1c39aeb.

35. Catherine O'Donnell, *New Study Quantifies Use of Social Media in Arab Spring*, UW NEWS (Sept. 12, 2011), https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/ ("After analyzing more than 3 million tweets, gigabytes of YouTube content and thousands of blog posts, a new study finds that social media played a central role in shaping political debates in the Arab Spring. Conversations about revolution often preceded major events, and social media has carried inspiring stories of protest across international borders.")

36. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., COMMODIFICATION OF CYBER CAPABILITIES: A GRAND CYBER ARMS BAZAAR 4 (2019), https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

SolarWinds incident, also referred to by the moniker Sunburst, is named for the Texas-based technology company whose Orion software product suite was compromised by this incident.[37] Through a series of actions that cybersecurity researchers have assessed as being notably sophisticated and complex, cyber actors were able to inject malicious code into automated software updates that Orion users uploaded between March and June 2020, and then carry out further computer network operations on selected victims. The end result: as many as 18,000 SolarWinds customers may have uploaded the malicious code, enabling the hackers to launch additional exploits that gave them wide-ranging access to accounts, credentials, networks, and information of the exploited targets.

Although investigations into this incident were still ongoing at the time this article was being written, it has been widely—if informally—attributed to a group often referred to as APT29 or Cozy Bear, reliably believed to be the SVR component of the Russian government's intelligence services. The impact has been global, affecting government and private sector networks in the U.S., the United Kingdom, Canada, Mexico, Spain, Belgium, and elsewhere around the world. Within the U.S., the incident has been confirmed to have resulted in compromise of networks and accounts used by the Department of Justice, Department of Homeland Security, Department of Energy, Department of Commerce, and other government agencies.[38]

Although it is too soon to know precisely how personal information obtained through the SolarWinds incident may be used, other recent cyberattacks provide examples of the risks to personal data. The Equifax data breach resulted in the compromise of information relating to some 140 million Americans.[39] In January 2020,

37. SolarWinds provides a range of information technology security tools, including network monitoring products used by U.S. government agencies and companies around the world (including some 425 of the Fortune 500). *See* Jason Murdock, *Hacked Software Firm SolarWinds' Clients Include Ford, Microsoft, AT&T*, (Dec. 14, 2020, 6:08 AM), https://www.newsweek.com/solarwinds-hack-customer-list-suspected-russian-cyberattack-1554467#:~:text=SolarWinds%20says%20it%20serves%20more,branches%20of%20the%20U.S.%20military; *see also IT Security Management Tools*, SOLARWINDS, https://www.solarwinds.com/it-security-management-tools (last visited Feb. 14, 2021).

38. *See, e.g.*, Lucian Constantin, *SolarWinds Attack Explained: And Why It Was So Hard to Detect*, CSO (Dec. 15, 2020, 3:44 AM), https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html; David E. Sanger et al., *As Understanding of Russian Hacking Grows, So Does Alarm*, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html (Jan. 5, 2021).

39. *See, e.g.*, Josh Fruhlinger, *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO (Feb. 12, 2020, 8:09 AM), https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html; U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-559, DATA PROTECTION: ACTIONS TAKEN

the Department of Justice indicted four members of the Chinese military charged with carrying out the attack[40]—suggesting the hack was one of a number of cyber incidents believed to have been carried out by the People's Liberation Army and Chinese intelligence agencies.[41] Similarly, the cyberattack on the U.S. Office of Personnel Management, carried out in 2013–2014, resulted in the compromise of personal information of some 5 million government employees and contractors, as well as their family members and contacts—including the exceptionally detailed information contained in the SF-86 forms filled out by individuals applying for security clearances.[42] Like the Equifax incident, the OPM breach is widely believed to have been carried out by the Chinese government and is assessed to have provided a wealth of information that could be used for counterintelligence operations by the Chinese military and intelligence services.[43]

Wide-reaching cyber incidents like the supply chain attack on SolarWinds software and the data breaches involving Equifax and OPM threaten the integrity of critical infrastructure, personal information, commerce, and other national interests. Despite these risks, software companies are largely unregulated, with effective security measures being relegated to business decisions and perceived competitive advantage rather than requirements; and state data breach laws focus on providing notification to affected individuals, but few of these laws impose specific requirements that companies or other entities that collect or process personal information adopt specific cybersecurity measures.[44] While U.S. government

---

BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 1 (2018) (available at https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf).

40. *See* Criminal Indictment, United States v. Zhiyong, No. 2:20-CD046 (N.D. Ga. Jan. 28, 2020).

41. *See, e.g.*, Katie Benner, *U.S. Charges Chinese Military Officers in 2017 Equifax Hacking*, N.Y. TIMES, https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html (May 7, 2020).

42. *See, e.g.*, MAJORITY STAFF REP. OF H.R. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED NATIONAL SECURITY FOR MORE THAN A GENERATION v–vi (Comm. Print 2016); Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSO (Feb. 12, 2020, 8:15 AM), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

43. Ian Smith, *Bolton Confirms China Was Behind OPM Data Breaches*, FEDSMITH (Sept. 21, 2018, 5:00 PM), https://www.fedsmith.com/2018/09/21/bolton-confirms-china-behind-opm-data-breaches/.

44. One notable exception to this trend is the New York Department of Financial Services (NYDFS) Reg. 500, which requires entities that are licensed and regulated by the NYDFS to consider and adopt specific cybersecurity measures. N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).

departments and agencies with cybersecurity responsibilities can carry out foreign intelligence gathering and law enforcement investigation to identify emerging cyber risks, they—appropriately—lack authority to monitor private sector networks in the U.S. Thus, nation-state adversaries who attack private entities for geopolitical reasons find that those private networks, and the personal information they contain, are defended by private sector means—which can vary greatly in their level of cybersecurity preparedness and protection. Existing consumer protection measures, like state data breach notification laws, do little to address the underlying threat, or to provide meaningful assistance either to those private sector networks that are targeted or to the individuals whose personal data may be breached as a result.

Third, foreign counterintelligence operations. The Russian government's interference with the 2016 U.S. presidential election has included well-documented intelligence components alongside the social media campaigns.[45] Russia is not, however, the only adversarial foreign government about which the U.S. has had counterintelligence concerns. For example, in August 2020, William Evanina, then the Director of the National Counterintelligence and Security Center (NCSC) issued a statement warning that:

> [a]head of the 2020 U.S. elections, foreign states will continue to use covert and overt influence measures in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process. . . . We are primarily concerned about the ongoing and potential activity by China, Russia, and Iran.[46]

The counterintelligence threat to the U.S. is, in the view of U.S. government officials and agencies, not limited to election security and integrity and democratic processes. In an address given in July 2020, Federal Bureau of Investigation (FBI) Director Christopher Wray cautioned that, "[t]he greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by

45. These efforts were documented at length by the Senate Select Committee on Intelligence. *See* 5 S. REP. NO. 116-290, at v (2020).

46. Press Release, William Evanina, Director, National Counterintelligence & Security Center, Election Threat Update for the American Public (Aug. 7, 2020, 1:07 PM), https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

extension, to our national security."[47] Wray went on to articulate this threat at length over the course of his remarks, beginning with the most direct and personal impact on individuals. "If you are an American adult, it is more likely than not that China has stolen your personal data."[48] Noting the widespread impact of the Equifax hack, Wray continued, "[o]ur data isn't the only thing at stake here—so are our health, our livelihoods, and our security."[49] To underscore the magnitude of the threat, Wray noted that the FBI opened a new China-related counterintelligence investigation about every ten hours, and that China-related matters comprise nearly half of all counterintelligence investigations being actively worked by the FBI.[50] Specific areas of concern: "at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research[,]"[51] as well as being culpable for the OPM hack and the massive data breach that affected American health insurer Anthem, as well as the Equifax breach.[52] The potential harms were multi-faceted, according to Wray: compromise of the data itself; use of the data to feed and train the artificial intelligence algorithms being developed by the Chinese government; and using the information to identify Americans who can be targeted for human intelligence operations aimed at obtaining sensitive government information, to be recruited for covert malign influence operations, and to target Chinese nationals outside of China who are seen as threats to the current Chinese Communist Party (CCP) regime.[53] Director Wray described the longstanding concerns regarding Chinese government theft of U.S. intellectual property and noted the ways in which companies like Huawei, which makes networking equipment, could provide a vantage point for wide-ranging collection of information from individuals as well as across all sectors of the economy.[54]

Against this backdrop of concerns, 2019–2020 saw unprecedented focus by the U.S. government on Chinese-owned technology companies that had access to U.S. telecommunications infrastructure and

47. Christopher Wray, FBI Director, Address to the Hudson Institute: The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States (July 7, 2020).
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*

personal information.[55] The Trump administration imposed additional tariffs on Chinese trade,[56] imposed sanctions on specific Chinese companies tied to the Chinese government and CCP,[57] and announced a ban—a mix of trade sanctions and consumer restrictions—on two popular mobile phone apps, TikTok and WeChat.[58] U.S. government entities had been eyeing TikTok warily as it grew in popularity, concerned about personal data being siphoned off by the Chinese government and with TikTok algorithms that seemed to suppress some content and promote other content in ways designed to please CCP censors. The company had already been fined by the FTC for violating children's privacy protection laws, investigated by the Committee on Foreign Investments in the U.S. (CFIUS), and banned by the U.S. Navy—all the while, however, the app continued to gain subscribers in the U.S.[59] Against this backdrop, in August 2020, then-President Trump signed an EO banning various commercial transactions with TikTok.[60] The EO made broad allegations that "the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States."[61] However, although commentators have pointed out that there are genuine risks that users' personal information might be harvested by the Chinese government in ways that undermine personal privacy and free speech and create counterintelligence risks,[62] they have also

55. The U.S. government measures included actions against Huawei and Executive Order 13,959, announcing new sanctions against Chinese-owned companies, signed by then-President Donald Trump on November 12, 2020. Those actions, although relevant for context, are not addressed in any detail in this article. *See* Exec. Order No. 13959, 85 Fed. Reg. 73,185 (Nov. 12, 2020); *see also* Sherisse Pham, *New US Sanctions Could Slowly Strangle Huawei's Smartphone Business*, CNN BUS., https://edition.cnn.com/2020/08/14/tech/huawei-kirin-chipsets-hnk-intl/index.html (Aug. 14, 2020, 12:02 AM).

56. Tom Lee & Jacqueline Varas, *The Total Cost of U.S. Tariffs*, AM. ACTION F. (Sept. 16, 2020), https://www.americanactionforum.org/research/the-total-cost-of-trumps-new-tariffs/.

57. Humeyra Pamuk & Matt Spetalnick, *U.S. Preparing New Sanctions on Chinese Officials over Hong Kong Crackdown*, REUTERS (Dec. 6, 2020, 8:19 PM), https://www.reuters.com/article/usa-china-sanctions/exclusive-u-s-preparing-new-sanctions-on-chinese-officials-over-hong-kong-crackdown-sources-idUSL4N2IN0AO; *see* Exec. Order No. 13,959, 85 Fed. Reg. 73,185 (Nov. 12, 2020).

58. Tali Arbel et al., *US Bans WeChat, TikTok from App Stores, Threatens Shutdowns*, AP NEWS (Sept. 18, 2020), https://apnews.com/article/national-security-china-archive-united-states-a439ead01b75fc958c722daf40f9307c.

59. *See, e.g.*, Rita Liao & Catherine Shu, *TikTok's Epic Rise and Stumble*, TECHCRUNCH (Nov. 26, 2020, 4:11 AM), https://techcrunch.com/2020/11/26/tiktok-timeline/.

60. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020); *see also* Press Release, U.S. Dep't of Com., *supra* note 58.

61. Exec. Order No. 13,942, 85 Fed Reg. 48,637.

62. *See, e.g.*, Lindsay Gorman, *Q&A with Lindsay Gorman: How Does TikTok Pose a National Security Risk to the United States?*, GERMAN MARSHALL FUND (Aug. 25, 2020),

noted that the EO did little to make clear the precise nature of the concerns and how this EO might meaningfully address them.[63] According to one critic, the ban was inarticulate and vague: "[d]epending on one's perspective, concerns might be raised about TikTok collecting data on U.S. government employees, TikTok collecting data on U.S. persons not employed by the government, . . . TikTok censoring information *beyond* China at Beijing's behest, or disinformation on the TikTok platform."[64] For other commentators, the ban risked sending the U.S. down the road to totalitarianism, as:

> "the blunt, chaotic and process-free unilateral action on TikTok has failed to draw a clear distinction between democratic and autocratic measures taken in the name of national security. In the absence of clearly defined criteria around ownership, data storage, data access and algorithmic influence—all thorny components of the global information contest in which democracies find themselves—the United States risks emulating the authoritarian model" for dealing with technology platforms and providers.[65]

Meanwhile, as TikTok litigated the validity of the EO, the risks of authoritarian misuse of personal data were underscored in a lawsuit filed by WeChat users against the app's parent company, Tencent, alleging that user accounts were cut off precisely because of Chinese government surveillance and censorship of app users' chats.[66]

Shortly after inauguration, (when this article was being prepared for publication), the Biden-Harris administration had reportedly not yet made a decision about whether to continue to or change course on the previous administration's position on TikTok and

---

https://securingdemocracy.gmfus.org/qa-with-lindsay-gorman-how-does-tiktok-pose-a-national-security-risk-to-the-united-states/.

63. *See, e.g.*, Justin Sherman, *Building a Better U.S. Approach to TikTok and Beyond*, LAWFARE (Dec. 28, 2020, 10:25 AM), https://www.lawfareblog.com/improving-tech-policy ("The Trump administration's TikTok executive order was more of a tactical move against a single tech firm than a fully developed policy. . . . Going forward, any executive branch policy on foreign software needs to explicitly specify the scope of the cybersecurity concerns at issue," which might include targeted foreign espionage through software systems, censorship conducted by foreign-owned platforms, and foreign governments "potentially collecting massive amounts of U.S. citizen data through software.").

64. *Id.*

65. Lindsay Gorman, *A Way Forward for U.S. Policy on TikTok*, LAWFARE (Nov. 10, 2020, 8:01 AM), https://www.lawfareblog.com/way-forward-us-policy-tiktok.

66. *See, e.g.*, Bloomberg, *Six California WeChat Users Sue Tencent for Alleged Chat Surveillance*, L.A. TIMES (Jan. 11, 2021, 6:22 PM), https://www.latimes.com/business/story/2021-01-11/california-wechat-users-sue-tencent-for-alleged-surveillance.

Huawei.[67] Whatever approach the new administration adopts, these issues of the vulnerability and collection of personal and corporate information by adversarial foreign governments is sure to remain a concern—as are the ways in which personal information and tech platforms are similarly used to influence domestic terrorism, civil discourse, and even insurrection.

Fourth, domestic terrorism and insurrection. On October 8, 2020, federal officials unsealed charges against thirteen people who had, according to the indictment, plotted to kidnap Michigan Governor Gretchen Whitmer, attack law enforcement, overthrow the government, and start a civil war.[68] The plot was shocking in its details: the suspects, part of a self-styled militia group in Michigan, had participated in field training exercises, created improvised explosive devices, and developed a detailed plan to kidnap Whitmer from her personal vacation home or official summer residence. They bought specialized equipment for a nighttime raid, took photographs and video of the vacation home, and made plans to blow up a nearby bridge to impede the ability of police to respond. At least some of the plotters appeared, from their comments, to be prepared to kill Governor Whitmer.[69]

Social media played a key role in the criminal conspiracy: according to the indictment, the men carried out much of their planning on and through private groups on Facebook. Experts in disinformation were quoted at the time as saying, "[s]ocial media companies have been allowing these communities to build and grow, ignoring the mounting evidence that memes, posts and images encouraging violence can and do translate into actual violence[.]"[70] Perhaps this should have been no surprise, as researchers had been warning for some time about the spread of far-right extremism on the internet. Following the August 2017 Unite the Right rally in Charlottesville, Virginia, social scientists pointed to the ways in which social media was serving as a recruiting ground for white supremacist groups.[71]

67. *See, e.g.*, Sean Lyngaas, *No Decisions Yet on Any Changes to TikTok or Huawei Cases, White House Says*, CYBERSCOOP (Jan. 25, 2021), https://www.cyberscoop.com/huawei-tiktok-china-biden-white-house/.

68. *See* Affidavit of FBI Special Agent Richard J. Trask II, United States v. Fox, No. 1:20-mj-00416-SJB (W.D. Mich. Oct. 16, 2020), ECF No. 1-1.

69. *Id.* at 7–8 ("Have one person go to her house. Knock on the door and when she answers it just cap her . . . catch her walking into the building and act like a passers-by and fixing dome her then yourself . . . ."); *id.* at 13 ("Kidnapping, arson, death. I don't care.").

70. Craig Timberg & Isaac Stanley-Becker, *Michigan Kidnapping Plot, Like So Many Other Extremist Crimes, Foreshadowed on Social Media*, WASH. POST (Oct. 8, 2020, 6:42 PM), https://www.washingtonpost.com/technology/2020/10/08/michigan-plot-kidnapping-boogaloo-socialmedia/ (quoting Cindy Otis, Vice President of Analysis for Aletha Group).

71. Francie Diep, *How Social Media Helped Organize and Radicalize America's White Supremacists*, PAC. STANDARD (Aug. 15, 2017), https://psmag.com/social-justice/how-social-

The protest had been a deadly and brazen display of white supremacist ideology in which a woman was killed when a man drove his car into a crowd of peaceful counter-demonstrators.[72] The man who drove the car was only twenty years old, but reportedly deeply immersed in white supremacist ideology.[73]

Research remains ongoing to better understand what makes individuals susceptible to radicalization, and how to counteract those forces. There is consensus, however, that the internet, and social media in particular, play a role. According to one expert, the key components for radicalization are an individual's quest for significance, encountering a narrative that serves as a vehicle for that significance, and having a network of support for those views.[74] Although we do not know how much impact social media and online radicalization may have had on this man's decision to drive his car into a crowd of protestors, we know that the Unite the Right rally was planned on Facebook.[75] And we know that Facebook's own research has shown that nearly two-thirds of the platform's users to join extremist groups on Facebook do so after Facebook's own algorithms recommend the extremist groups to them.[76]

The issues have become more urgent since 2017, as a toxic mix of disinformation has spread online, ranging from the QAnon conspiracy theory to baseless allegations of election fraud, and from white supremacist ideology to fact-free claims that the coronavirus is a hoax and that COVID vaccines will be used to inject people with microchips.[77]

None of these conspiracy theories or ideologies exists solely online; to greater and lesser extents, they spread offline as well. But in order to achieve maximum scope and reach, all of these threat vectors depend on access to the massive quantities of

---

media-helped-organize-and-radicalize-americas-newest-white-supremacists ("[T]he tools of the Internet Age have helped white supremacists and other bigots to share ideas and organize.").

72. Mitch Smith, *James Fields Sentenced to Life in Prison for Death of Heather Heyer in Charlottesville*, N.Y. TIMES (June 28, 2019), https://www.nytimes.com/2019/06/28/us/james-fields-sentencing.html.

73. Alexa Liautaud, *How the Charlottesville Suspect Became Radicalized*, VICE NEWS (Aug. 14, 2017, 3:14 PM), https://www.vice.com/en/article/zmy8n8/how-the-charlottesville-attacker-became-radicalized.

74. *Id.*

75. Diep, *supra* note 71.

76. Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*, WALL ST. J. (May 26, 2020, 11:38 AM), https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

77. *See, e.g.*, Jack Goodman & Flora Carmichael, *Coronavirus: Bill Gates 'Microchip' Conspiracy Theory and Other Vaccine Claims Fact-Checked*, BBC (May 30, 2020), https://www.bbc.com/news/52847648.

personal information and the detailed personal behavioral profiles that make targeted advertising, recommender algorithms, private groups, and other key tools of information—and disinformation—spread and targeted messaging possible in today's digital ecosystem.

The cumulative frenzy of this partially-online ecosystem spilled over into real life on January 6, 2021, when a mob of right-wing protesters stormed the U.S. Capitol building in an attempt to prevent certification of the Electoral College votes that would formalize Joe Biden's win in the 2020 U.S. presidential election.[78] Even as events were unfolding, experts quickly pointed to the fact that the attempted insurrection had been hiding in plain sight for weeks or months, organized on social media.[79]

In some respects, this should have come as no surprise. Online radicalization had been a source of concern in the national security community for decades. In the aftermath of the terrorist attacks of 9/11, the U.S. government and intelligence agencies around the world were pouring time and energy into understanding how the internet had become a vehicle for radicalizing supporters of al-Qaeda and other international terrorist groups.[80] By 2011, analysts in the U.S. who were studying online radicalization were still often focused on older internet technologies such as web forums, closed communities of anonymous users where groups like al-Qaeda proselytized to its members and newer recruits found inspiration.[81] There was some recognition, however, of the power of the internet and the ways in which the technology was impacting radicalization:

> [c]omputers affect how we experience media and how we interact with others. Extremists are as susceptible to these effects

78. Dan Barry et al., *'Our President Wants Us Here': The Mob That Stormed the Capitol*, N.Y. TIMES, https://www.nytimes.com/2021/01/09/us/capitol-rioters.html (Feb. 13, 2021); Amy Brittain et al., *The Capitol Mob: A Raging Collection of Grievances and Disillusionment*, WASH. POST (Jan. 10, 2021), https://www.washingtonpost.com/investigations/2021/01/10/capitol-rioters-identified-arrested/?arc404=true; *Mob Attack, Incited by Trump, Delays Election Certification*, N.Y. TIMES, https://www.nytimes.com/live/2021/01/06/us/electoral-vote (Jan. 20, 2021, 11:40 AM).

79. *See, e.g.*, Sheera Frenkel, *The Storming of Capitol Hill Was Organized on Social Media*, N.Y. TIMES (Jan. 6, 2021, 4:41 PM), https://nyti.ms/3q0L6dn.

80. *See, e.g.*, Dana Janbek & Valerie Williams, *The Role of the Internet Post-9/11 in Terrorism and Counterterrorism*, 20 BROWN J. WORLD AFFS. 297 (2014); *see also Jihadist Use of Social Media—How to Prevent Terrorism and Preserve Innovation*: *Hearing Before the Subcomm. on Counterterrorism & Intel. of the Comm. on Homeland Sec.*, 112th Cong. 14 (2011) (testimony of Andrew Aaron Weisburd) ("The U.S. intelligence community is already making very effective use of the internet to identify and investigate extremists.") [hereinafter *Jihadist Use of Social Media*].

81. *See, e.g.*, *Jihadist Use of Social Media*, *supra* note 80, at 11 (testimony of Andrew Aaron Weisburd).

> as we are. The on-line environment is immersive. We feel we are in a place, often called cyberspace. When we are on a social media site, we feel that we are virtually together with our friends, family, and comrades in arms. We feel we are present in the videos we watch. On-line interaction brings people closer, faster. On-line relationships get off to a strong start, and then move off-line if possible.[82]

However, as evidenced by one expert's comments, there still was an understanding that social networks largely mirrored offline networks—and perhaps underestimated the extent to which social media would be shaping offline networks and driving offline behavior, either then or in the future.[83] Perhaps for this reason, much of the focus was on countering slickly produced films, digital magazines, and other media produced by terrorist organizations, rather than anticipating the ways in which the interactive nature of the internet itself would make radical recruitment messaging harder to resist.

Branding in terrorist media is a sign of authenticity, and terrorist media is readily identifiable as such due to the presence of trademarks known to be associated with particular organizations. The objective should be not to drive all terrorist media off-line, but to drive it to the margins and deprive it of the power of branding, as well as to leave homegrown extremists unable to verify the authenticity of any given product.[84]

The witnesses were not interested in deplatforming terrorists—on the contrary, they pointed out that law enforcement benefited greatly from the ability to track the connections and communications between and among suspected terrorist actors online.[85]

---

82. *Id.* at 13.

83. *Id.* ("On-line social networks tend to mirror off-line social networks. People—extremists included—use social media to keep in touch with people they already know. An individual's ability to get involved in terrorism is directly related to who they know, and this is precisely what social media sites reveal to us.").

84. *Id.* at 14.

85. *See id.* at 13 ("An individual's ability to get involved in terrorism is directly related to who they know, and this is precisely what social media sites reveal to us. The benefits of this to law enforcement are enormous.") (testimony of Andrew Aaron Weisburd). The Senior Advisor to the President, Rand Corporation continued:

> this on-line discussion and these postings are a source of valuable intelligence. So rather than devoting vast resources to shutting down content and being dragged into a frustrating game of whack-a-mole—as we shut down sites, they open up new ones. Instead, we probably should devote our resources to facilitating intelligence collection and criminal investigations so that we can continue to achieve the successes that we have had thus far in identifying these individuals, uncovering these plots and apprehending these individuals.

Id. at 15 (testimony of Brian Michael Jenkins).

Just five years later, the government's approach to countering violent extremism had expanded to recognize the growing role of social media interactions in addition to display of propagandistic content.[86] In the wake of the Orlando nightclub shooting, a senior official at the Department of Homeland Security explained:

> [t]he threat from homegrown violent extremism requires going beyond traditional counterterrorism approaches and focusing not just on mitigation efforts but also on preventing and intervening in the process of radicalization. This prevention framework is known as "countering violent extremism," or the acronym CVE. . . . Terrorist groups such as ISIL have undertaken a deliberate strategy of using social media to reach individuals susceptible to their message and recruit and inspire them to violence.[87]

Perhaps naïvely, in 2011 at least one expert noted that,

> [p]roducing and distributing media for Foreign Terrorist Organizations constitutes material support for terrorism. I would argue that a service provider who knowingly assists in the distribution of terrorist media is also culpable. While it is in no one's interests to prosecute internet service providers, they must be made to realize that they can neither turn a blind eye to the use of their services by terrorist organizations, nor can they continue to put the onus of identifying and removing terrorist media on private citizens. I don't believe that Google, operator of YouTube, has an interest in promoting violent

86. *See, e.g.*, *Isis Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media: Hearing Before the Permanent Subcomm. on Investigations of the Comm. on Homeland Sec. and Governmental Affs.*, 114th Cong. (2016). Michael Steinbach, Executive Assistant Director, National Security Branch, FBI stated,

> ISIL's messaging blends both officially endorsed sophisticated propaganda with that of informal peer-to-peer recruitment through digital communication platforms. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago. Like never before, social media allows for overseas terrorists to reach into our local communities to target our citizens as well as to radicalize and recruit.

Id. at 8; *see also id.* at 11–12 (testimony of Meagen M. LaGraffe, Chief of Staff to the Coordinator and Special Envoy, Global Engagement Center, U.S. Department of State) ("[W]hile al-Qaeda was producing videos that took months to get out, our adversary today is using social media in ways not seen before.").

87. *Id.* at 10 (testimony of George Selim, Director, Office of Community Partnerships, U.S. Department of Homeland Security, and Director, Interagency Task Force on Countering Violent Extremism).

> extremism, and they have already made some effort to address this issue, but they can and should do more.[88]

That expert might have been surprised to see the politically charged debates taking place a decade later over content moderation and deplatforming of accounts both before and after the mob assault on the Capitol in 2021.

IV. PRIVACY AND NATIONAL SECURITY ARE NOT ALL: THE INTERSECTIONS AMONG DEPLATFORMING, CONTENT MODERATION, ANTITRUST, AND ONLINE HARMS

To put the growth of online conspiracy theories and disinformation into context, it is useful to remember the recency of social media as a communication tool, and of complex and detailed personal being collected as a ubiquitous part of daily life. Facebook was launched in 2004.[89] Since then, the platform and its family of apps has amassed nearly 3 billion users—nearly half the world's population.[90] The first smartphone became available when the iPhone entered the market in 2007,[91] and smartphones are now used by an estimated 3.8 billion people around the world.[92] Data brokers create personal profiles based on thousands of data points about individuals,[93] in a business worth an estimated $200 billion.[94] The online profiling carried out by data brokers and platforms is not limited to location, demographic facts, or behavior; it also includes personality modeling and behavioral prediction. Perhaps the most

---

88. *Jihadist Use of Social Media*, *supra* note 80, at 14 (testimony of Andrew Aaron Weisburd).

89. Mark Hall, *Facebook*, BRITANNICA, https://www.britannica.com/topic/Facebook (Feb. 4, 2021).

90. Facebook recorded some 2.6 billion active users in the third quarter of 2020, and its family of apps—Facebook, WhatsApp, Instagram—surpassed 3 billion users in the first quarter of 2020. *See* H. Tankovska, *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2020*, STATISTA (Feb. 2, 2021), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/; *see also* Khari Johnson, *Facebook Apps Now Used Monthly by More than 3 Billion People*, VENTUREBEAT (Apr. 29, 2020, 2:31 PM), https://venturebeat.com/2020/04/29/facebook-earnings-q1-2020/.

91. John Markoff, *Apple Introduces Innovative Cellphone*, N.Y. TIMES (Jan. 10, 2007), https://www.nytimes.com/2007/01/10/technology/10apple.html.

92. S. O'Dea, *Number of Smartphone Users Worldwide from 2016 to 2023*, STATISTA (Mar. 18, 2021), https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

93. *See, e.g.*, Aliya Ram & Madhumita Murgia, *Data Brokers: Regulators Try to Rein in the 'Privacy Deathstars'*, FIN. TIMES (Jan. 8, 2019), https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.

94. David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019, 8:00 AM), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

notorious recent example of this took place on Facebook, which has used information about users' behavior both on and off the platform to assess where individuals fell within the set of personality traits measured by the "OCEAN" standard of a person's tendency towards Openness, Conscientiousness, Extroversion, Agreeableness, and Neuroticism,[95] and to assess its users' behavior and personalities so thoroughly that, according to at least one study, Facebook's algorithms were more accurate at predicting an individual's personality traits than even their own family members.[96]

The Silicon Valley industry that was once heralded as the hub of global innovation has, in recent years, come under increasing scrutiny by privacy advocates, antitrust regulators, and legislators in the U.S. and Europe over concerns ranging from market dominance to intrusive data collection practices.[97] December 2020 brought illustrative examples, with three significant measures likely to impact the future of data-driven platforms and cross-platform data sharing.

In the first, the FTC filed a complaint against Facebook, charging the company with anticompetitive practices tied to its purchase of Instagram and WhatsApp and the policies through which Facebook restricts the activities of third party developers who create online services designed to connect to the Facebook platform.[98] The complaint, which focuses on monopolistic practices and market effects, refers to privacy impacts as well, noting that if there were greater competition in social media, benefits to users could include rival platforms that offer greater data protection options for users.[99]

Just a week later, the FTC announced that it was launching an inquiry into the privacy practices of the major social media and

95. *See, e.g.*, Erin Brodwin, *Here's the Personality Test Cambridge Analytica Had Facebook Users Take*, BUS. INSIDER (Mar. 19, 2018, 4:01 PM), https://www.businessinsider.com/facebook-personality-test-cambridge-analytica-data-trump-election-2018-3.

96. *See, e.g.*, Frank Luerweg, *The Internet Knows You Better than Your Spouse Does*, SCI. AM. (Mar. 14, 2019), https://www.scientificamerican.com/article/the-internet-knows-you-better-than-your-spouse-does/; Douglas Quenqua, *Facebook Knows You Better than Anyone Else*, N.Y. TIMES (Jan. 19, 2015), https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html.

97. *See, e.g.*, Adam Satariano, *'This Is a New Phase': Europe Shifts Tactics to Limit Tech's Power*, N.Y. TIMES (July 30, 2020), https://www.nytimes.com/2020/07/30/technology/europe-new-phase-tech-amazon-apple-facebook-google.html; Daisuke Wakabayashi et al., *13 Ways the Government Went After Google, Facebook and Other Tech Giants This Year*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/technology/tech-investigations.html (Dec. 16, 2020).

98. Press Release, Federal Trade Commission, FTC Sues Facebook for Illegal Monopolization (Dec. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization; Complaint at 1, FTC v. Facebook, Inc., No. 1:20-cv-03590-JEB (D.D.C. Jan. 13, 2021), ECF No. 51.

99. Complaint, *supra* note 98, at 12.

video streaming services, including Facebook, YouTube, ByteDance, Twitch, Reddit, and Discord.[100] The accompanying fifty-three-page Order catalogues an extensive list of information that the FTC is seeking, including user counts, usage statistics, and financial data, as well as questions that get to the heart of the platforms' business models, such as the nature of each user attribute that the platforms use, track, estimate, or derive about their users; the dollar value to the platforms of their users; and the nature of algorithms run on the platforms.[101]

At the same time, the UK announced that it was moving forward with a set of legislation intended to address online harms that included terrorist groups and gangs using online platforms for recruitment and radicalization of new members.[102] The proposals were first introduced in April 2019, and the December 2020 announcement signaled the end of the consultation period and implementation of the new approach[103] with issuance of interim codes of practice intended to address a number of online ills, including terrorist content and activity online.[104] The UK legislation carries with it echoes of the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online[105] that followed the terrorist attack on two New Zealand mosques,[106] as well as laws in France and Germany and legislative proposals elsewhere that are directed at countering violent extremism and requiring minimum standards of content moderation for certain kinds of content posted

100. Press Release, Federal Trade Commission, Joint Statement of FTC Commissioners Chopra, Slaughter, and Wilson Regarding Social Media and Video Streaming Service Providers' Privacy Practices (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/public_statements/1584150/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.

101. FTC Res. P205402 (2020).

102. The legislation is also aimed at curbing other forms of online harms, such as child sexual exploitation and abuse and drug trafficking. Press Release, Dep't for Digital, Culture, Media & Sport, UK to Introduce World First Online Safety Laws (Apr. 8, 2019), https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws.

103. Caroline Dinenage, *Consultation Outcome: The Government Report on Transparency Reporting in Relation to Online Harms*, GOV.UK, https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/government-transparency-report (Dec. 15, 2020); Baroness Morgan of Cotes & Priti Patel, *Consultation Outcome: Online Harms White Paper—Initial Consultation Response*, GOV.UK, https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response (Dec. 15, 2020).

104. *Online Harms: Interim Codes of Practice*, GOV.UK (Dec. 15, 2020), https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice.

105. *ChristChurch Call: To Eliminate Terrorist and Violent Extremist Content Online*, CHRISTCHURCH CALL, https://www.christchurchcall.com/call.html (last vistited Feb. 14, 2020).

106. *Id.*

online.[107] Although the UK guidance on online harms is tied to definitions in the UK Terrorism Act of 2006, the kinds of activities it seeks to address include those that have been the focus of efforts to counter violent extremism worldwide, such as online statements that glorify, encourage, incite, or provide inducements for terrorist activities[108]—precisely the kinds of discourse that are central to the U.S. federal charges against Capitol rioters[109] and the House impeachment managers in considering how to present the impeachment case against former president Donald J. Trump for inciting an insurrection that erupted into violence on January 6, 2021.[110]

One of the most striking responses to online disinformation and the provocation of offline violence came from platform providers in the wake of the January 6 attack on the Capitol.[111] Within days, then-President Trump had been deplatformed—his account removed—from Twitter, Facebook, Twitch, and other major social media sites, and major Trump-oriented channels had been removed from other sites, such as Reddit's r/TheDonald and The Donald server on Discord.[112] Meanwhile, the far-right platform Parler was

---

107. *See Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act*, *NetzDG*), BUNDESMINISTERIUM DER JUSTIZ AND FÜR VERBRAUCHERSCHUTZ (2017), https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html; *see also* Loi 2020-766 du 24 Juin 2020 de Proposition de loi visant a lutter contre les contenus haineux sur internet [Law 2020-766 of June 24, 2020 on Fighting Hate on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O. OFFICIAL GAZETTE OF FRANCE], June 25, 2020. The main provisions of the proposition were declared unconstitutional by the French Constitutional Council on June 18, 2020. *See French Avia Law Declared Unconstitutional: What Does This Teach Us at EU Level?*, EDRI (June 24, 2020), https://edri.org/our-work/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/; *see also Current Approaches to Terrorist and Violent Extremist Content Among the Global Top 50 Online Content-Sharing Services*, ORG. FOR ECON. CO-OPERATION & DEV. 19–25 (Aug. 14, 2020), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP(2019)15/FINAL&docLanguage=En.

108. INTERIM CODE OF PRACTICE ON TERRORIST CONTENT AND ACTIVITY ONLINE 16–17 (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944036/1704b_ICOP__online_terrorist_content_v.2_11-12-20.pdf.

109. Press Release, U.S. Dep't of Justice, Thirteen Charged in Federal Court Following Riot at the United States Capitol (Jan. 8, 2021), https://www.justice.gov/opa/pr/thirteen-charged-federal-court-following-riot-united-states-capitol; Marie Fazio, *Notable Arrests After the Riot at the Capitol*, N.Y. TIMES, https://www.nytimes.com/2021/01/10/us/politics/capitol-arrests.html (Mar. 5, 2021).

110. *See* Mike DeBonis et al., *House Democrats Building Elaborate, Emotionally Charged Case Against Trump*, WASH. POST (Jan. 29, 2021, 8:21 PM), https://www.washingtonpost.com/politics/house-democrats-building-elaborate-emotionally-charged-case-against-trump/2021/01/29/d35170fe-626c-11eb-9061-07abcc1f9229_story.html; Nicholas Fandos, *Trump Impeached for Inciting Insurrection*, N.Y. TIMES, https://www.nytimes.com/2021/01/13/us/politics/trump-impeached.html (Feb. 12, 2021).

111. Frenkel, *supra* note 79.

112. Sara Fischer & Ashley Gold, *All the Platforms That Have Banned or Restricted Trump So Far*, AXIOS, https://www.axios.com/platforms-social-media-ban-restrict-trump-d9e44f3c-8366-4ba9-a8a1-7f3114f920f1.html (Jan. 11, 2021).

removed from the Apple and Google app stores, and Amazon Web Service announced it would no longer host Parler, making the platform essentially unavailable for download (from app stores) or use (with no hosting platform).[113] These moves have prompted litigation,[114] and come at a time when politicians and activists across the political spectrum were already issuing widespread calls to reform Section 230 of the Communications Decency Act, the often-misunderstood provision of federal law that grants online platforms immunity from liability for content posted by their users.[115] Despite widespread complaints from the political right that its views were being silenced on social media, the data prior to January 6, 2021 demonstrated otherwise, with research from Facebook-owned CrowdTangle consistently showing that the top-performing posts on Facebook came from conservative commentators and outlets.[116]

Post-January 6, the landscape is less clear, as it may take some time for additional data to emerge. However, extremist alt-right content is likely to continue to be readily available in the U.S. The conclusion reached by some: "[I]t's likely that fringe and extremist websites will continue to seek refuge in other jurisdictions like Russia and China where they can more readily withstand diplomatic, political, and legal pressure."[117] This analysis underscores the intersection between national security, geopolitics, domestic extremism, and online outlets. Or, put more succinctly, "[t]he founder of neo-Nazi rag the *Daily Stormer* had some advice for the people who

---

113. *See, e.g.*, Jack Nicas & Davey Alba, *Amazon, Apple and Google Cut Off Parler, an App That Drew Trump Supporters*, N.Y. TIMES, https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html (Jan. 13, 2021); Sarah Perez, *This Week in Apps: Parler Deplatformed, Alt Apps Rise, Looking Back at 2020 Trends*, TECHCRUNCH (Jan. 16, 2021, 11:00 AM), https://techcrunch.com/2021/01/16/this-week-in-apps-parler-deplatformed-alt-apps-rise-looking-back-at-2020-trends/.

114. *See, e.g.*, Bobby Allyn, *Judge Refuses to Reinstate Parler After Amazon Shut It Down*, NPR (Jan. 21, 2021, 3:14 PM) https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down.

115. *See, e.g.*, David McCabe, *Tech Companies Shift Their Posture on a Legal Shield, Wary of Being Left Behind*, N.Y. TIMES (Dec. 15, 2020), https://www.nytimes.com/2020/12/15/technology/tech-section-230-congress.html; Daisuke Wakabayashi, *Legal Shield for Social Media Is Targeted by Lawmakers*, N.Y. TIMES, https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html (Dec. 15, 2020).

116. *See, e.g.*, Oliver Darcy, *Trump Says Right-wing Voices Are Being Censored. The Data Says Something Else*, CNN BUS., https://www.cnn.com/2020/05/28/media/trump-social-media-conservative-censorship/index.html (May 28, 2020, 7:54 PM); Mark Scott, *Despite Cries of Censorship, Conservatives Dominate Social Media*, POLITICO, https://www.politico.com/news/2020/10/26/censorship-conservatives-social-media-432643 (Oct. 27, 2020, 1:38 PM).

117. Fergus Ryan, *Why Are Moscow and Beijing Happy to Host the U.S. Far-Right Online?*, FOREIGN POL'Y (Jan. 22, 2021, 1:37 PM), https://foreignpolicy.com/2021/01/22/russia-beijing-web-host-far-right-parler-daily-stormer/.

ran Parler, after the app was purged from the Internet last week: Ask China or Russia for help."[118]

In the words of the United Kingdom's Digital Secretary Jeremy Wright, "[t]he era of self-regulation for online companies is over."[119]

V. LESSONS IN OVERSIGHT—AND HOW TO IMPROVE PRIVACY AND DATA PROTECTIONS WHILE ALLOWING REASONABLE GOVERNMENT USE

There are a number of sound reasons why legal theories relating to the regulation of government access to data is more mature, with jurisprudence of longer standing, than legal theories addressing private sector use of data—but the two areas of law may have useful lessons for each other. The scope of government power and the consequences of its misuse, America's historical roots in rebellion against a tyrannical regime, and the language of the Constitution itself, along with historical examples of government misuse of personal data, are among the reasons for focusing on harms, remedies, and constraints involving government use of information. For example, government misuse of personal information during the decades from World War II through the Vietnam War have been investigated and extensively documented, including in the Congressional hearings in the specially-designated Committees for intelligence oversight that came to be colloquially known as the Church and Pike Committees. The multi-volume report issued by the Senate's Church Committee incorporated a wealth of details about government overreach, as well as recommendations for how to prevent similar abuses going forward.[120] During the course of the Church and Pike Committee hearings, it became evident that there were multiple reasons for the challenges that Congress faced in overseeing the U.S. intelligence community documented by the Church and Pike Committees, including gaps in committee jurisdiction and insufficient resources and expertise to grapple with the implications of emerging technology.[121] The outcome was recognition of the need

118. *Id.*

119. UK to Introduce World First Online Safety Laws, *supra* note 102 (quoting the comments of Jeremy Wright accompanying the release of *Online Harms White Paper*).

120. Although the House of Representatives' Pike Committee never issued a final report, the transcripts of its hearings remain available, and excerpts from a draft version of the report were published in the newspaper *The Village Voice*. *See generally The CIA Report the President Doesn't Want You to Read*, VILL. VOICE (Feb. 16, 1976), https://www.villagevoice.com/1976/02/16/the-cia-report-the-president-doesnt-want-you-to-read/.

121. *See* April Falcon Doss, *Time for a New Tech-Centric Church-Pike: Historical Lessons from Intelligence Oversight Could Help Congress Tackle Today's Data-Driven Technologies*, 15 J. BUS. & TECH. L. 1, 1–2 (2019).

for a multifaceted approach that included all three branches of government, resulting in Executive Orders, legislation, judicial involvement in reviewing electronic surveillance, and the establishment of standing Congressional oversight committees. The work of those committees created a sweeping set of boundaries on the USIC, along with a comprehensive framework for oversight that has endured and, by and large, served the nation's multiple interests—protection of national security and of civil liberties and privacy—well.

Even within this framework, there have been a number of government programs that have raised legal or Constitutional questions or objections. For example, the NSA's bulk metadata collection program, first revealed through unauthorized disclosures by former government contractor Edward Snowden,[122] quickly prompted concerns over the program's legality, with groups like the American Civil Liberties Union (ACLU) arguing that the program violated the PATRIOT Act as well the First and Fourth Amendments to the Constitution.[123] The program had, in fact, been reviewed and approved dozens of times by independent judges sitting on the Foreign Intelligence Surveillance Court (FISC),[124] and the program had been briefed to members of Congress.[125] But the program had never previously been publicly disclosed, and there was little about the statutory language or the legal premises upon which the program relied that would have given the public at large reason to think that such activities were happening.[126] In other words, for

122. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 6:05 PM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

123. *See, e.g.*, Press Release, ACLU, ACLU Files Lawsuit Challenging Constitutionality of NSA Phone Spying Program (June 11, 2013), https://www.aclu.org/press-releases/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program?redirect=national-security/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program.

124. *See, e.g.*, Scott F. Mann, *Fact Sheet: Section 215 of the USA PATRIOT Act*, CSIS (Feb. 27, 2014), https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act; *see also Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs: Hearing Before the S. Comm. on the Judiciary*, 113 Cong. 113–334 (2013) (statement of James M. Cole, Deputy Attorney General of the U.S.); *see also In re* Application of the Fed. Bureau of Investigation for an Ord. Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, 2013 WL 5741573, at *2–3 (FISA Ct. Aug. 29, 2013).

125. *In re Application of the Fed. Bureau of Investigation*, 2013 WL 5741573, at *24–26.

126. *See, e.g.*, Jim Sensenbrenner, *NSA Abused Trust, Must Be Reined In*, MILWAUKEE J. SENTINEL (Nov. 2, 2013), http://archive.jsonline.com/news/opinion/nsa-abused-trust-must-be-reined-in-b99131601z1-230292131.html/ ("I led a bicameral group of legislators that came together and passed the USA [PATRIOT] Act with strong bipartisan support. . . . But the National Security Agency abused that trust. It ignored restrictions painstakingly crafted by lawmakers and assumed a plenary authority never imagined by Congress."). Sensenbrenner was, at the time this opinion piece was published, the chair of the House Judiciary

those steeped in the arcane details of foreign intelligence surveillance law—including the judges of the FISC—the program had appeared to fall within the boundaries set by the Constitution and law.[127] But the program was so unexpected that when its existence became publicly known, the outcry from civil libertarians, politicians, and many members of the public at large was swift and fierce.

The FAA 702 program, in contrast, followed a very different trajectory: although information about the program was also leaked by Edward Snowden, the activities carried out under the 702 program were tethered far more directly and predictably to clearly defined provisions of law and procedure.[128] The rationale for the program was explained in unprecedented detail at open hearings before Congress, as senior officials of the Intelligence community articulated why the mechanics of modern telecommunications infrastructure made it necessary to use access points within the United States to collect the communications of intelligence targets who were not U.S. persons and who were outside the U.S.[129] The language of the law, as ultimately passed and as subsequently amended, was clear in describing the intent of the law and providing predictability into

---

Committee's Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, and was one of the authors of the USA PATRIOT Act.

127. *See generally Strengthening Privacy Rights and National* Security, *supra* note 124 (testimony of Deputy Attorney General James Cole; Robert Litt, General Counsel of the Office of the Director of National Intelligence, and John C. Inglis, Deputy Director of the National Security Agency).

128. *See* PRIV. & C. L. OVERSIGHT BD., 113TH CONG., REP. ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 5 (2014).

129. *See, e.g.*, *Testimony of General Michael V. Hayden, Director, CIA, Before the S. Comm. on the Judiciary*, 109th Cong. (2006); *see also Hearing on the Protect America Act of 2007 Before the H. Permanent Select Comm. on Intel.*, 110th Cong. (2007) (statement of J. Michael McConnell, Director of National Intelligence); *Hearing on the Foreign Intelligence Surveillance Act and Implementation of the Protect America Act Before the S. Comm. on the Judiciary*, 110th Cong. 9 (2007) (statement of J. Michael McConnell, Director of National Intelligence); *Modernizing the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intel.*, 110th Cong. (2007) (statement of J. Michael McConnell, Director of National Intelligence). These, and other public statements and testimony during 2007, were focused on the specific FISA modernization proposal that would become the Protect America Act (PAA), a piece of federal legislation that temporarily authorized a legal framework to carry out foreign intelligence surveillance in a manner fundamentally similar to the program that would later become FAA 702. Because the PAA was set to sunset after only six months, Congressional passage of FAA 702 in 2008 was based in large part on the factual framework and policy justifications that had been put forward in 2007 during debate on FISA modernization and PAA. For more details on the history of the transition from the FISA Modernization Act to the PAA to FAA 702, *see generally* David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: A Working Paper of the Series on Counterterrorism and American Statutory Law* (Brookings Inst., Working Paper, 2007).

how it would be administered and applied.[130] Consequently, although the FAA 702 program has both supporters and critics, the debates have not, by and large, been sidetracked with concerns founded on unpredictability or surprise; instead, they focus where one might appropriately expect them to: on whether the statute's scope is sound policy, and whether courts ought to reconsider the long line of jurisprudence that has consistently found the program to be constitutional.[131]

More recently, a number of Trump-era uses of personal data have raised concerns that demonstrate the ways in which, even within a longstanding legal framework, the rise of new technologies continues to raise new questions about the scope of personal data by government actors. Examples include the practice of searching social media accounts as well as laptops, smartphones, and other devices at border crossing locations,[132] and the use of DNA testing for immigrants and refugees.[133] Historically, expanded search and surveillance activities at border crossings have been upheld, based on the reduced expectation of privacy and heightened governmental interests at international borders.[134] However, the increasingly expansive use of this authority by the Department of Homeland Security (DHS) has led to alarm,[135] and to litigation, as travelers protested the DHS policy of employing both "basic" and "advanced" searches, with advanced searches allowing officers to analyze, search, and copy the contents of electronic devices.[136] In one such

130. *See, e.g.*, PRIV. & C. L. OVERSIGHT BD., *supra* note 128, at 8–9 ("On the whole, the text of Section 702 provides the public with transparency into the legal framework for collection, and it publicly outlines the basic structure of the program.").

131. *See, e.g.*, *The Privacy Concerns at the Heart of the FISA Renewal Debate*, PBS NEWSHOUR (Jan. 11, 2018, 6:35 PM), https://www.pbs.org/newshour/show/the-privacy-concerns-at-the-heart-of-the-fisa-renewal-debate.

132. *See, e.g.*, HILLEL R. SMITH, CONG. RSCH. SERV., LSB10387, DO WARRANTLESS SEARCHES OF ELECTRONIC DEVICES AT THE BORDER VIOLATE THE FOURTH AMENDMENT? (2019).

133. *See, e.g.*, Abigail Hauslohner, *U.S. Immigration Authorities Will Collect DNA from Detained Migrants*, WASH. POST (Mar. 6, 2020, 2:59 PM), https://www.washingtonpost.com/immigration/us-immigration-authorities-will-collect-dna-from-detained-migrants/2020/03/06/63376696-5fc7-11ea-9055-5fa12981bbbf_story.html.

134. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("Consistently, therefore, with Congress' power to protect the Nation by stopping and examining persons entering this country, the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant, and first-class mail may be opened without a warrant on less than probably cause . . . . These cases reflect longstanding concern for the protection of the integrity of the border.") (footnote omitted).

135. *See, e.g.*, Carrie DeCell, *"Dehumanized" at the Border, Travelers Push Back*, KNIGHT FIRST AMEND. INST. (Feb. 2, 2018), https://knightcolumbia.org/content/dehumanized-border-travelers-push-back.

136. Alasaad v. Nielsen, No. 1:17-cv-11730-DJC, at 4 (D. Mass. Nov. 12, 2019).

case, *Alasaad v. Nielsen*, the plaintiffs were U.S. citizens or legal permanent residents who objected to Customs and Border Patrol (CBP) searches of the photos, contacts, social media, and other information that appeared on the travelers' electronic device. In that case, the federal district court held that, despite the border exception to the Fourth Amendment, officers must demonstrate reasonable suspicion prior to carrying out such searches.[137] In oral argument on appeal, the panel of First Circuit judges appeared skeptical of arguments that it ought to go beyond even the reasonable suspicion requirement found by the District Court and impose a requirement for individualized warrants for electronic device searches at the border, but at the time this article was being prepared for publication, no decision had yet been rendered in the matter.[138]

All of these policy debates are necessary to inform national security policy, as they have been in the law enforcement context, where courts have attempted to guide Fourth Amendment jurisprudence in a manner that keeps pace with changing technology.[139] However, there has been far less attention paid to the extraordinarily intrusive data collection, analysis, and behavioral prediction that is possible in the private sector. The term "surveillance capitalism" was coined as a catch-all phrase to encompass the many forms this takes.[140] This private sector scrutiny of our personal lives takes myriad forms and extends far beyond the social media environment and digital advertising contexts. It includes workplace demands that employees install location tracking apps on their personal

137. *Id.* at 38 (holding that "reasonable suspicion and not the heightened warrant requirement supported by probable cause . . . is warranted here").

138. Brian Dowling, *1st Circ. Wary of Border Phone Search Warrant Requirement*, LAW360 (Jan. 5, 2021, 3:01 PM), https://www.law360.com/articles/1341883/1st-circ-wary-of-border-phone-search-warrant-requirement; Andrea Vittorio, *Searches of Digital Devices Face Appeals Court Scrutiny*, BLOOMBERG L., https://news.bloomberglaw.com/privacy-and-data-security/border-searches-of-digital-devices-face-appeals-court-scrutiny-1 (Jan. 5, 2021, 2:58 PM).

139. Some of the most notable decisions arise in the context of Supreme Court decisions of the past twenty years. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (government acquisition of an individual's cell site location records constitutes a Fourth Amendment search); Riley v. California, 573 U.S. 373, 402 (2014) (police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested); United States v. Jones, 565 U.S. 400, 411 (2012) (continuous use of a GPS tracking device requires a warrant under the Fourth Amendment). However, digital data maintained by a third party does not fit neatly under existing precedents but lies at the intersection of two lines of cases, exemplified by GPS data privacy in *Jones* and the Third Party doctrine founded on United States v. Miller. 425 U.S. 435, 444 (1976) (no expectation of privacy in financial information held by a bank); Smith v. Maryland, 442 U.S. 735, 743–45 (1979) (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company).

140. *See generally* Mariano-Florentino Cuéllar & Aziz Z. Huq, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 133 HARV. L. REV. 1280 (2020).

phones, or wear RFID-enabled smart badges that track an employee's location through the workplace and even monitor the tone and volume of their voice when talking while wearing the badge.[141] It includes facial recognition technology being used in schools, and internet-enabled devices that can monitor and record the interactions of children in the classroom.[142] And of course it includes all of the ways that platforms that do not charge use fees rely on a business model which, at its heart, rests on monetization of user information. Despite these widespread uses, and the growing number of ways in which personal data can be used, or perhaps misused, by private actors, federal circuit courts remain split on the question of what facts are required in order for plaintiffs to have standing to sue for privacy-related claims in federal courts.[143] The Ninth Circuit, citing its own precedent as well as Third Circuit case law, noted that:

> advances in technology can increase the potential for unreasonable intrusions into personal privacy. . . . As the Third Circuit has noted, "[i]n an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion . . . that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data . . . is untenable. Nothing in *Spokeo* or any other Supreme Court decision suggests otherwise."[144]

VI. HOW CAN, OR SHOULD, THESE AREAS OF LAW INTERSECT?

What do these seemingly disparate threads have in common? All depend on the seemingly inexhaustible supply of personal data. The reforms, too, need to rest on a data-focused approach, one that recognizes that the convergence of technologies has inevitably led

---

141. DOSS, *supra* note 1, at 115–23.

142. *Id.* at 126–29.

143. *See, e.g.*, *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 598 (9th Cir. 2020) ("[V]iolations of the right to privacy have long been actionable at common law.") (alteration in original) (quoting Patel v. Facebook, 932 F.3d 1264, 1272 (9th Cir. 2019)); *id.* ("A right to privacy 'encompass[es] the individual's control of information concerning his or her person.'") (alteration in original) (quoting Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017)) (internal citations omitted); *see also* Jason S. Wasserman, *Stand in the Place Where Data Live: Data Breaches as Article III Injuries*, 15 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 201, 202 (2020) ("Courts, however, do not even agree on whether or when data breach victims can sue, or in other words, when the victims suffer cognizable legal injuries that create Article III standing.").

144. *In re Facebook, Inc. Internet Tracking*, 956 F.3d at 599 (alterations and omissions in original) (citing *Patel*, 932 F.3d at 1272 and *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 934 F.3d 316, 325 (3d Cir. 2019)).

to an intersection of ills—and those ills can best be addressed through intersecting approaches to law and policy.

Each of these issues—consumer data privacy, national security, domestic terrorism, speech, platform liability protections—are complex in their own right. Combining them into a single framework for analysis and potential solutions might seem to be a fool's errand—a combination that, by including more dimensions, makes the puzzle infinitely more complex. It is more likely, however, that the opposite is true: the puzzle is already complex and multi-faceted, regardless of whether we choose to acknowledge or leverage the interrelatedness of these issues. The irreducible fact is that significant dimensions of each of these problems already intersect in ways that we cannot unravel.

To put it another way: we are often treating each of these major areas of legal uncertainty and evolving legal doctrine as if they are separate, standalone jigsaw puzzles; if only we can find pieces of the right shape and color, and orient them in the right way, we can solve the puzzle of consumer data privacy, or election-related information operations, or national security surveillance, or platform liability for speech or online harms, or antitrust implications of technology providers, bringing each of these disparate areas into focus as a clear and coherent two-dimensional picture, with each completed puzzle resting on its own table, on its own puzzle mat, having been worked by an independent team of advocates, experts, and practitioners who are steeped in that particular set of issues. This approach, however, is likely as outdated as the analog paper storage and retrieval mechanisms that have largely been replaced by digitized, complex, data and algorithms. In our interconnected, digital ecosystem, in which personal information underpins so many seemingly disparate actions and interactions, the problem set is no longer a library of independent two-dimensional jigsaw puzzles, each of which can be solved on its own. Instead, they are more like a Rubik's cube: trying to solve one side of the puzzle in isolation from the others does nothing to move towards an overall scheme—in fact, the opposite is true, since solving for one side hopelessly scrambles the cube's other five surfaces, making them less coherent than before. The only way to solve the Rubik's cube and align its colors is to solve for all six of its sides at once, knowing that in the process there may be times when the tension between sides—the impact of one set of moves on the other surfaces—at first appears to be counterproductive, but is a necessary accommodation to consider in order to reach the end-state solution.

Privacy rights, civil liberties, technology innovation, freedom of speech, and national security are all, of course, weightier issues by far than aligning colors on a Rubik's cube; it is no surprise that the analogy is an imperfect one, and it particularly breaks down when it comes to sacrificing important interests in one sphere of law in order to optimize another. So while scrambling one side of a Rubik's cube to solve the overall puzzle is an easy decision to make, policymakers and privacy advocates alike ought to avoid situations in which one side of the multidimensional data puzzle gets scrambled in an effort to make gains on another side.[145] With the significance of different policy choices top of mind, the list below provides a modest selection of ways that policymakers and legislators can go about addressing the interrelated bundle of issues that form distinct but interrelated parts of this multidimensional personal data puzzle.

A. Acknowledge the Convergence of Technology—and Embrace Cross-Pollination of Legal Theories

During the FISA modernization hearings of 2007, a frequent refrain was technology convergence, and the ways in which the internet and twenty-first century telecommunications raised new challenges: intelligence targets were using the same free webmail services, internet forums, and other modes of communication used by ordinary people in the U.S. and around the world, and an ever-more-pressing challenge of intelligence gathering was separating out the signal from the noise, of finding the terrorist communication among the proliferation of cat videos. That challenge has only grown more acute in the years since then, as social media, encrypted messaging, mobile advertising, personal data profiles, mobile apps, Internet of Things devices, and more become a ubiquitous part of everyday life, and as companies maintain storehouses of

145. This is arguably what has resulted from the European Union's decisions over the years to tie permission for international transfer of commercial data to its concerns about U.S. national security activities. In the *Schrems II* decision, the CJEU invalidated the Privacy Shield framework and cast doubt on the future viability of standard contractual clauses—key mechanisms supporting the transfer of personal data. However, the impact—the cost, burden, limitations on commerce, etc.—of this decision falls on private sector entities who have no ability to influence U.S. surveillance law. While it is conceivable that the U.S. Congress might at some point structure U.S. intelligence gathering activities in ways that satisfy European courts and privacy advocates, it is not at all clear that that's the case, for a great many reasons not discussed here. The end result is that a European privacy regulation has been interpreted in such a way as to scramble the international commerce side of the Rubik's cube in hopes that the resulting pressure will force the U.S. to solve the national security side of the puzzle in a way that is to the EU's liking. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, 2020 E.C.R. I-559.

data on individuals that dwarfs anything held by governments, including by national security and law enforcement agencies in the U.S.

Proposals for reform of Section 230's liability protections, new legal theories relating to content moderation, and discussions of government purchases of commercially available information that forms part of the digital advertising market should all be considered in the overall context of surveillance law, consumer data privacy, and cybersecurity obligations and data breach notification laws.

B. Expand Data-Related Regulations on the Private Sector

With the inauguration of a new administration, policy recommendations abound, as think tanks, civil society groups, and others offer comments on ways that the federal government can consider addressing the most pressing issues associated with personal data and technology platforms.[146] Proposals for a federal data privacy law have circulated for years; the 117th Congress presents a unique opportunity to capitalize on that momentum by passing a comprehensive data privacy law that would impose minimum principles and standards for handling of personal information. If privacy legislation includes obligations of transparency and mechanisms for oversight and redress of violations, then private sector use of information can be removed from the current landscape, in which individuals are often out-leveraged by large corporations and placed on a more equal footing with the more highly regulated uses of information by government actors.

C. Level the Playing Field in Government Regulations

One of the issues that has become apparent is that there is no uniform set of standards, regulations, procedures, or approaches governing the activities of local, state, and federal agencies that handle personal information. Whether government entities acquire data directly, through mechanisms like government-operated street

146. *See, e.g.*, April Falcon Doss, *Data and Democracy: Three Things the Biden-Harris Administration Should Do to Tackle Big Tech*, JUST SEC. (Nov. 30, 2020), https://www.justsecurity.org/73538/data-and-democracy-three-things-the-biden-harris-administration-should-do-to-tackle-big-tech/; Alexandra Reeve Givens, *CDT Recommendations to the Biden Administration and 117th Congress to Advance Civil Rights & Civil Liberties in the Digital Age*, CDT (Jan. 20, 2021), https://cdt.org/insights/cdt-recommendations-to-the-biden-administration-and-117th-congress-to-advance-civil-rights-civil-liberties-in-the-digital-age/; India McKinney & Ernesto Falcon, *EFF's Top Recommendations for the Biden Administration*, EFF (Jan. 21, 2021), https://www.eff.org/deeplinks/2021/01/effs-top-recommendations-biden-administration.

cameras or surveillance drones, or indirectly, by obtaining it from private sector data collectors, it is essential for government departments and agencies to provide transparency about their data practices, and for those practices to be subject to robust and effective oversight mechanisms. While state and local government uses of data will continue to be a matter for state and local control, the federal government can and should assess government-wide use of data and look to level the playing field of federal government regulations and oversight where gaps currently exist.

D. Prioritize Education and Public Awareness Campaigns

Providing improved digital literacy education and public awareness campaigns is becoming an increasingly vital need. Focusing on media literacy and related topics in schools is important but insufficient; research has shown that older Americans are more susceptible to online disinformation than younger ones.[147] With that dynamic in mind, outreach could include measures like traditional producing television-format public service announcements intended to reach older Americans who watch television and who also may be prone to sharing misinformation on their Facebook feeds. Separate lines of research have shown that librarians consistently are viewed as highly trusted sources of reliable information[148] and may be able to play a key role in combatting online disinformation—although resources and other constraints currently pose challenges.[149]

Sound policy proposals for combatting online disinformation abound.[150] These proposals should be given serious consideration, tried, and then tested for efficacy, and then expanded upon.

---

147. *See, e.g.*, *Troll Watch: Study Shows Older Americans Share the Most Fake News*, NPR (Jan. 13, 2019, 5:21 PM), https://www.npr.org/2019/01/13/684994772/troll-watch-study-shows-older-americans-share-the-most-fake-news.

148. A.W. Geiger, *Most Americans—Especially Millennials—Say Libraries Can Help Them Find Reliable, Trustworthy Information*, PEW RSCH. CTR. (Aug. 30, 2017), https://www.pewresearch.org/fact-tank/2017/08/30/most-americans-especially-millennials-say-libraries-can-help-them-find-reliable-trustworthy-information/.

149. *See, e.g.*, Suzanne LaPierre, *New Research Explores How Public Libraries Can Best Combat Misinformation*, PUB. LIBR. ASS'N (Nov. 23, 2020), http://publiclibrariesonline.org/2020/11/new-research-explores-how-public-libraries-can-best-combat-misinformation/.

150. *See, e.g.*, Nina Jankowicz, *How to Defeat Disinformation: An Agenda for the Biden Administration*, FOREIGN AFFS. (Nov. 19, 2020), https://www.foreignaffairs.com/articles/united-states/2020-11-19/how-defeat-disinformation.

E. Empower Congressional Oversight with Cross-Committee Jurisdiction

The range of legal and social issues stemming from data-driven technologies currently spans multiple committees in both houses of Congress.[151] Adopting a model that supports robust cross-committee jurisdiction will help advance opportunities for sensible cross-pollination of ideas.[152]

F. Assess the Need for Additional Independent Oversight Bodies

Government entities at local, state, and federal levels are all subject to Constitutional constraints[153] and are typically subject to some form of political control,[154] transparency obligations,[155] and independent oversight, which may be carried out by courts, by inspectors general, by independent commissions, or by other duly authorized bodies. Even where the public is not afforded direct access to information about data collection or handling—such as in the national security context, in which many government programs are classified and information about them is therefore tightly controlled—there frequently exists some set of overseers who have been granted authority to review all pertinent information regarding a program or activity and stand in the shoes of the people for purposes of scrutinizing the lawfulness and prudence of the programs at issue.[156]

Private entities, however, lack these mechanisms. Their status as private entities means they are only subject to the particular controls that might apply to their specific industry (such as OCR's

151. *See generally* Doss, *supra* note 121.

152. *See generally id.*

153. In the case of state and local government entities, those constraints may be heightened by the provisions of state constitutions as well as state statutes or local ordinances that impose additional privacy and speech protections that are conferred by the U.S. Constitution.

154. Political control may come from voters as well as from a legislative branch of government at the federal, state, or local level—whether it be by Congress or a City Council, executive branch agencies at federal, state, and local levels are generally subject to legislative scrutiny as well as mechanisms for accountability to the people they serve.

155. Through federal laws, such as the Privacy Act and Freedom of Information Act, federal agencies are required to provide transparency into a variety of government activities relating to the use of personal information. All fifty states have some form of freedom of information or open records legislation, and some local government entities have additional transparency requirements. *See, e.g.*, *State Freedom of Information Laws*, NAT'L FREEDOM INFO. COAL., https://www.nfoic.org/coalitions/state-foi-resources/state-freedom-of-information-laws (last visited Feb. 15, 2021).

156. In the national security context, these overseers include the U.S. House and Senate intelligence committees, the Foreign Intelligence Surveillance Court, the Privacy and Civil Liberties Oversight Board, and the inspectors general of all of the departments and agencies that comprise the U.S. intelligence community.

authority to carry out investigations of HIPAA covered entities) or status (such as the SEC's authority to carry out investigations into certain activities of publicly traded companies). Consumers have only a limited ability to pressure companies into providing greater transparency or accountability—particularly when the company holds a dominant market share for a particular good or service, leaving consumers with few alternative providers; companies that recognize the inherent power created by holding a dominant market position may feel little incentive to respond to consumer concerns, whether those relate to personal data privacy, algorithmic functions and bias, content moderation policies, data sharing practices, or other aspects of a company's operations and use of personal information. This transparency can, however, be significantly bolstered through a regulatory framework of the type noted in Section II, above. The FTC has long made use of its Section 5 authority to create a sort of regulatory bootstrapping: where a company was initially subject only to general obligations to refrain from unfair or deceptive acts or practices, a company that has entered into a consent decree with the FTC is frequently subject thereafter to very specific obligations, and any failure to comply could result in fines or other regulatory consequences for failing to abide by the terms of the consent agreement. A more direct approach would be to create specific regulatory obligations in federal legislation governing data privacy, security of personal information, and other key areas at the intersection of personal data and pressing policy concerns. Such a regulatory framework could expand the staffing, authority, and role of the FTC, or create one or more new regulatory bodies to carry out investigations and oversight. It could require regular transparency reporting of the kind currently required for the intelligence community.

VII. CONCLUSION

As the online ecosystem grows ever more complex, so do the intersections among previously-disparate fields of law. Consumer data privacy and national security are two areas in which these intersections have become particularly striking. Antitrust, transparency of election-related advertising and other paid political content, and the ongoing need for Fourth Amendment jurisprudence in the law enforcement context are, as briefly alluded to above, other areas of law that strain to keep pace with the critical intersections between new technologies and the many ways in which personal information can be created, collected, collated, manipulated,

organized, analyzed, assessed, sold, shared, and more. As legislators, policymakers, advocacy groups, and academics continue assessing how law can be used as a tool of public policy to protect individual rights, protect national security, and preserve domestic tranquility, their chances of arriving at successful approaches goes up if these challenges are treated like the intersecting faces of a Rubik's cube, rather than confined to separate "cylinders of excellence."

The Evolution of Legal Risks Pertaining to Patch Management and Vulnerability Management

James T. Kitchen[*]
David R. Coogan[**] *& Keeton H. Christian*[***]

The views and opinions set forth herein are the personal views or opinions of the author; they do not necessarily reflect views or opinions of the law firm with which [he/she] is associated.

* Partner, Jones Day. Jimmy Kitchen is a former Assistant U.S. Attorney who has led groundbreaking cyber investigations, including one that led to the first-ever corporate cyber-espionage indictment of Chinese military hackers in the landmark case of *U.S. v. Wang Dong*. He assists companies with cybersecurity and breach response and other internal investigations and compliance.

** Associate, Jones Day. David Coogan is a former Marine Corps intelligence officer and prosecutor. He advises companies on cybersecurity and privacy compliance as well as related litigation.

*** Associate, Jones Day. Keeton Christian is a member of the New Lawyers Group.

I. INTRODUCTION

In May 2017, WannaCry malware spread across the globe by exploiting a known vulnerability in Windows called EternalBlue.[1] WannaCry encrypted files on infected Windows systems.[2] The malware impacted schools, hospitals, and businesses in over 150 countries,[3] including the British National Health System, which spent nearly $100 million to fix its systems.[4] Two months earlier, Windows had released patches for the EternalBlue vulnerability.[5] Had the patches been installed, the malware would not have impacted

1. Ionut Arghire, *NSA's EternalBlue Exploit Fully Ported to Metasploit*, SEC. WK. (May 16, 2017), https://www.securityweek.com/nsas-eternalblue-exploit-fully-ported-metasploit.

2. Russell Goldman, *What We Know and Don't Know About the International Cyberattack*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html.

3. *Id.*

4. Danny Palmer, *This Is How Much the WannaCry Ransomware Attack Cost the NHS*, ZDNET (Oct. 12, 2018, 5:59 AM), https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/.

5. *Security Update for Microsoft Windows SMB Server (4013389)*, MICROSOFT, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (Oct. 11, 2017).

the Windows systems.[6] In June 2017, another piece of malware, known as NotPetya, exploited the same Windows vulnerability to cause even more damage.[7] NotPetya irreversibly encrypted computers in a way that made it impossible to recover the computer or the data on it.[8] NotPetya caused large, multinational companies to go offline for weeks and caused billions in damages.[9] It has been called the "most destructive and costly cyber-attack in history."[10]

Not only did the malware impact operations at affected companies, it also had legal impacts. In June 2017, Nuance, a speech recognition software vendor, was a victim of the NotPetya attack, which cost the company more than $90 million.[11] Nuance was also the defendant in two lawsuits brought by two of Nuance's customers.[12] The lawsuits alleged Nuance failed to use reasonable care in its information security practices.[13] Specifically, one of the customers alleged that although in March 2017 the customer had installed the Windows patch for EternalBlue on its Windows systems, Nuance did not.[14] The customer alleged that because Nuance's network had administrator-level credentials to the customer's network, the malware entered the customer's network and caused nearly $11 million in damage.[15]

Each year software and hardware vendors release thousands of updates to patch vulnerabilities in their software.[16] Over the past

---

6. *Customer Guidance for WannaCrypt Attacks*, MICROSOFT SEC. RESPONSE CTR. (May 12, 2017), https://msrc-blog.microsoft.com/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

7. Lawrence J. Trautman & Peter C. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 531–32 (2019).

8. *Id.* at 532.

9. Press Briefing, The White House, Statement from the Press Sec'y (Feb. 15, 2018) (archived at https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/).

10. *Id.*

11. Nuance Commc'ns, Inc., Quarterly Report (Form 10-Q) 23 (Feb. 9, 2018).

12. Heritage Valley Health Sys., Inc. v. Nuance Commc'ns, Inc., 479 F. Supp. 3d 175 (W.D. Pa. 2020); Princeton Cmty. Hosp. Ass'n, Inc. v. Nuance Commc'ns, Inc., No. 1:19-00265, 2020 WL 1698363 (S.D. W. Va. Apr. 7, 2020).

13. *Heritage Valley Health Sys., Inc.*, 479 F. Supp. 3d at 188–89; *Princeton Cmty. Hosp. Ass'n, Inc.*, 2020 WL 1698363, at *1.

14. Complaint at ¶¶ 25–26, *Princeton Cmty. Hosp. Ass'n, Inc.*, 2020 WL 1698363 (S.D. W. Va. Apr. 11, 2019) (No. 19-C-59). This lawsuit was jointly dismissed by the parties after the court denied Nuance's motion to dismiss. *See* Joint Stipulation & Order of Dismissal with Prejudice, *Princeton Cmty. Hosp. Ass'n, Inc.*, 2020 WL 1698363 (S.D. W. Va. Aug. 11, 2020) (No. 19-C-59). The other lawsuit was dismissed because the court found that Nuance did not owe a duty to its customer beyond the obligations in the contract between the parties. *Heritage Valley Health Sys., Inc.*, 479 F. Supp. 3d at 187.

15. Complaint, *supra* note 14, at ¶¶ 37, 56.

16. *Is Software More Vulnerable Today?*, EUR. UNION AGENCY FOR CYBERSECURITY (Mar. 12, 2018), https://www.enisa.europa.eu/publications/info-notes/is-software-more-vulnerable-today.

twenty years, the number of vulnerabilities has largely increased each year.[17] Companies that rely on the software and hardware to run their businesses must sift through the deluge of notifications and determine which patch should be prioritized in order to prevent a hacker from exploiting an unpatched vulnerability and using it to get inside the company network.[18] Vendors typically assign a score, using the Common Vulnerability Scoring System (CVSS), to each vulnerability to indicate the likelihood and impact of exploitation.[19] Some vulnerabilities are considered important enough that the United States Department of Homeland Security orders all federal agencies to implement a patch within a particular time period.[20] In fact, in May 2017, President Trump issued an Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure which found that "[k]nown but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies."[21] These "[k]nown vulnerabilities include[d] using operating systems or hardware beyond the vendor's support lifecycle" and "declining to implement a vendor's security patch."[22]

Many data breaches that occur each year are due to unpatched vulnerabilities.[23] Reports vary about how many data breaches are due to known unpatched vulnerabilities. One study reported sixty percent of the breaches could have occurred because a patch was available for a known vulnerability but not applied.[24] Another report found that one in three breaches are caused by unpatched vulnerabilities.[25]

---

17. *National Vulnerability Database: Statistics Results*, NAT'L INST. STANDARDS & TECH., https://nvd.nist.gov/vuln/search/statistics (last visited Mar. 8, 2021). The number of vulnerabilities dramatically increased beginning in 2017. *See* Rob Lemos, *The State of Vulnerability Reports: What the CVE Surge Means*, TECHBEACON, https://techbeacon.com/security/state-vulnerability-reports-what-cve-surge-means (last visited Mar. 8, 2021).

18. *See* Jason Bloomberg, *To Patch or Not to Patch? Surprisingly, That Is the Question*, FORBES (Apr. 16, 2018, 9:10 AM), https://www.forbes.com/sites/jasonbloomberg/2018/04/16/to-patch-or-not-to-patch-surprisingly-that-is-the-question/?sh=4997f33d58fe.

19. *Common Vulnerability Scoring System SIG*, FIRST, https://www.first.org/cvss/ (last visited Mar. 8, 2021).

20. *See, e.g.*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., EMERGENCY DIRECTIVE 20-04, MITIGATE NETLOGON ELEVATION OF PRIVILEGE VULNERABILITY FROM AUGUST 2020 PATCH TUESDAY (2020).

21. Exec. Order No. 13,800, 82 Fed. Reg. 22,391, 22,391 (May 11, 2017).

22. *Id.*

23. Taylor Armerding, *Patch Now or Pay Later: Report*, FORBES (June 6, 2019, 9:37 AM), https://www.forbes.com/sites/taylorarmerding/2019/06/06/report-if-you-dont-patch-you-will-pay/?sh=2e3fe0693acd.

24. PONEMON INST. LLC, COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE 3 (2020).

25. Steve Ranger, *Cybersecurity: One in Three Breaches Are Caused by Unpatched Vulnerabilities*, ZDNET (June 4, 2019, 2:15 PM), https://www.zdnet.com/google-

Although the process of prioritizing and implementing patches is technical and typically not the responsibility of an organization's legal department, unpatched software is a legal risk for organizations. With the evolution of cybersecurity regulation and litigation, legal liability relating to vulnerability and patch management is no longer theoretical.[26] Because software vendors typically notify their customers about vulnerabilities in their software and the availability of updates,[27] regulators may take the position that companies that use the software are generally on notice of the vulnerabilities. Due to the increase in the number of disclosed vulnerabilities and the increased general acceptance of security standards, regulators have been paying greater attention to whether companies are patching known software vulnerabilities. Because company lawyers may not be sufficiently technically knowledgeable to understand the IT department's approach to vulnerability and patch management, it can be a blind spot for the legal department. Conversely, the IT department may not understand the legal implications of the work they do in this arena. This article attempts to bridge that gap.

This article begins with an overview, in non-technical terms, of the tools generally available and processes implemented for vulnerability management and patch management. Section II identifies some of the evolving security standards that regulators and plaintiffs may rely on to show that companies are legally required to have vulnerability management and patch management. Section III identifies U.S. legal implications of vulnerability management and patch management and factors that a court and regulators may consider.

---

amp/article/cybersecurity-one-in-three-breaches-are-caused-by-unpatched-vulnerabilities/. The other end of the spectrum is reporting that the root cause of only two percent of breaches was missing patches. *See* SARA BODDY & RAY POMPON, THREAT INTELLIGENCE REPORT: LESSONS LEARNED FROM A DECADE OF DATA BREACHES (2017), https://www.f5.com/content/dam/f5/downloads/F5_Labs_Lessons_Learned_from_a_Decade_of_Data_Breaches_rev.pdf. This report points out that some phishing cases are only successful if the end user's machine is not patched properly. *Id.* at 36 ("For phishing cases that rely on users opening a malicious file (which can then exploit a vulnerability on the system), patch, update, and patch again!").

26. *See generally* STEWART BAKER & MAURY SHENK, A PATCH IN TIME SAVES NINE: LIABILITY RISKS FOR UNPATCHED SOFTWARE, STEPTOE & JOHNSON (Oct. 2003), https://www.steptoe.com/publications/274a.pdf.

27. Cristian Florian, *Security Patching Trends for Major Software Vendors*, TECHTALK (Mar. 13, 2012), https://techtalk.gfi.com/security-patching-trends-for-major-software-vendors/.

II. OVERVIEW OF VULNERABILITY MANAGEMENT AND PATCH MANAGEMENT

Most computer users are familiar with software updates. Whether it is an update for the operating system on a Windows computer or an iPhone, the update fixes bugs or vulnerabilities in the software.[28] In a business setting, the employees who use a laptop to carry out their duties, also called "end users," are generally unaware of the various software on the company's network and the updates. The responsibility for identifying the software that needs to be updated, prioritizing the updates, and implementing the updates usually falls to the information technology and information security teams.[29] The technical terms for these processes are vulnerability management and patch management.[30] A non-technical overview of the tools used for these processes are explained below.

A. Vulnerability Management

The processes by which vulnerabilities are identified are varied. Every day, computer security researchers[31] examine software for problems in the computer code that cause the software to do something it is not intended to do.[32] These weaknesses, or vulnerabilities, in the software could be exploited by an attacker to perform an unauthorized action within a computer system.[33] Ideally, before publicly disclosing the vulnerability, the computer security researcher notifies the software vendor about the vulnerability and gives the vendor an opportunity to create a "patch" that fixes the vulnerability.[34] Once the vulnerability has been publicly disclosed,

---

28. *See Understanding Patches and Software Updates*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://us-cert.cisa.gov/ncas/tips/ST04-006 (Nov. 19, 2019).

29. Armerding, *supra* note 23.

30. This article addresses vulnerabilities in software and the application of patches to mitigate those vulnerabilities. Others use the term "vulnerability management" to broadly refer to a variety of weaknesses including mismanagement of IT hardware and software or even physical security issues. *See, e.g.*, Sean Atkinson, *Cybersecurity Tech Basics: Vulnerability Management: Overview*, THOMSON REUTERS (2018), https://www.cisecurity.org/wp-content/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf.

31. Software companies employ security researchers and others to identify vulnerabilities in their software. For example, these researchers may examine the code within malware in circulation in order to determine whether malware can be used to exploit a previously unknown vulnerability within software. Independent security researchers who work for security firms unaffiliated with software companies similarly investigate and identify these vulnerabilities.

32. Atkinson, *supra* note 30, at 1.

33. *Id.*

34. Vulnerability disclosure best practices are discussed in Allen D. Householder et al., *The CERT Guide to Coordinated Vulnerability Disclosure*, CARNEGIE MELLON UNIV.:

the Mitre Corporation (MITRE), a federally funded research center, assigns the vulnerability a unique Common Vulnerability Enumeration (CVE),[35] and the National Institute of Standards and Technology (NIST) publishes information about the vulnerability in the National Vulnerability Database (NVD).[36] Within an organization, the IT team or information security team is responsible for reviewing the software on the organization's network to identify, classify, remediate, and mitigate the software vulnerabilities.[37] The process of "identifying, classifying, remediating, and mitigating vulnerabilities" is called vulnerability management.[38]

There are several different ways an IT team can become aware of a newly identified software vulnerability. One typical way is through email notifications directly from the software vendor.[39] Typically, the IT team signs up for these notifications based on the software the business is running.[40] Another typical way is through the use of software—vulnerability scanners—to "scan" systems and networks for hosts using outdated or unsupported software.[41] A "host" includes servers, desktop personal computers, or personal electronic devices.[42] The vulnerability scanners generate a report that identifies the total number of identified hosts and vulnerabilities, including a risk level for each vulnerability.[43] In addition to identifying software vulnerabilities that require patching, the results from the vulnerability scanners can identify vulnerabilities

---

SOFTWARE ENG'G INST. (Aug. 2017), https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

35. *About CVE*, COMMON VULNERABILITIES & EXPOSURES, https://cve.mitre.org/about/index.html (Mar. 29, 2021).

36. *National Vulnerability Database: Statistics Results*, *supra* note 17.

37. *See generally* Tom Palmaers, *Implementing a Vulnerability Management Process*, GLOB. INFO. ASSURANCE CERTIFICATION (Mar. 23, 2013), https://www.giac.org/paper/gsec/32851/implementing-vulnerability-management-process/112555.

38. PARK FOREMAN, VULNERABILITY MANAGEMENT 1 (2d ed. 2019).

39. *See, e.g.*, *Adobe Security Notifications Registration: Security Notification Service*, ADOBE, https://www.adobe.com/subscription/adbeSecurityNotifications.html (last visited Feb. 11, 2021).

40. *See, e.g.*, *id.*

41. Common vulnerability scanning software vendors include Tenable, Qualys, Rapid7, and Nexpose. *See, e.g.*, *Close Your Cyber-Exposure Gap*, TENABLE, https://www.tenable.com/products (last visited Mar. 10, 2021); *Nexpose Vulnerability Scanner*, RAPID7, https://www.rapid7.com/products/nexpose/ (last visited Mar. 10, 2021); *Vulnerability Management That's Accurate and Scales!*, QUALYS, https://www.qualys.com/lp/vulnerability-management/ (last visited Mar. 10, 2021).

42. Miles Tracy et al., *Guidelines on Securing Public Web Servers: Recommendations of the National Institute of Standards and Technology*, NAT'L INST. STANDARDS & TECH. app. B, at B-1 (Sept. 2007), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf.

43. *See, e.g.*, Warlock, *Vulnerability Assessment with Nexpose*, INFOSEC RES. (Dec. 27, 2013), https://resources.infosecinstitute.com/topic/vulnerability-assessment-nexpose/.

due to configuration problems or outdated certificates.[44] While these are vulnerabilities that the IT and information security teams should address, they are separate from vulnerabilities that require patching.

Traditionally, vulnerability scanners were "agentless," but agent-based scanning is also now available.[45] In addition to the decision about whether to use agentless scanning, agent-based scanning, or both, the IT and information security teams must decide how often to scan and what to scan.[46] Agentless scanning and agent-based scanning offer different features for identifying vulnerabilities which are explained below.

1. Agentless Scanning

Agentless scanning relies on one or more servers to perform network scanning of each host. The scan collects information about the host, including what versions of different software the host is running.[47] Agentless scanning can be "credentialed" or "non-credentialed."[48] Credentialed scanning requires that the IT team enter an administrator username and password into the scanning application.[49] The application then has greater access to the host to return more accurate scanning results. In a given network, there is likely more than one set of administrator credentials. The process of ensuring the scanning application has the correct administrator credentials can be burdensome. The analogies for the difference between "credentialed" or "non-credentialed" are many, including the difference between an x-ray and an MRI or a home inspection conducted from the sidewalk versus going inside the home.[50]

The scope of agentless scanning is limited to hosts on the local network. This means laptops and mobile devices not on the network during the scan are omitted from the results.[51] Other

---

44. Atkinson, *supra* note 30.

45. *See* Murugiah Souppaya & Karen Scarfone, *Guide to Enterprise Patch Management Technologies*, NAT'L INST. STANDARDS & TECH. 8 (July 2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf.

46. *See id.*

47. *Id.*

48. This is also referred to as "authenticated" or "unauthenticated" scanning. *See* Lucian Constantin, *What Are Vulnerability Scanners and How Do They Work?*, CSO ONLINE (Apr. 10, 2020, 3:00 AM), https://www.csoonline.com/article/3537230/what-are-vulnerability-scanners-and-how-do-they-work.html.

49. *Id.* Because the administrator password can be intercepted, some IT teams use keys or certificates for credentialed scans.

50. *See, e.g.*, Lascon, *Vulnerability Management: You're Doing It Wrong*, YOUTUBE (Jan. 21, 2019), https://youtu.be/yUZ_YFSNQQE (referencing material at time stamp 19:30).

51. Souppaya & Scarfone, *supra* note 45, at 9.

limitations of agentless scanning include other security controls that may inadvertently block the scanning and considerations due to the scanning consuming excessive amounts of bandwidth.[52]

2. Agent-Based

Unlike agentless scanning, agent-based scanning requires the installation of software, an "agent," on each host. The agent has administrator privileges, which ensures every scan is "credentialed." The agent sends the information back to a server that collects information about the host including what versions of software the host is running. Unlike agentless scanning, agent-based scanning is not dependent on the host being on the corporate network.

B. Patch Management

The scale of correctly and safely implementing a patch across an entire organization can be challenging. Prior to releasing a patch, software vendors test the patch to ensure the software continues to properly function. However, it is not possible for the software vendor to test how every application or third-party software will react to the patch. This task is left to IT departments. Typically, the IT department tests the patch in a test environment to see whether it causes other applications to perform in unexpected ways, including causing other applications to crash or run slowly. After testing the patched software, the IT department will decide to install the patch or not. In some cases, companies have found it prudent to delay the installation of a patch while awaiting any report of security issues related to the patch itself. If the IT department installs the patch, the final step in the process is verifying the installation. This resource intensive process of "identifying, acquiring, installing, and verifying patches for products and systems" is called patch management.[53]

Because the process is resource intensive, IT departments must make decisions about how to optimally patch the vulnerabilities that pose the greatest risk to the organization. Typically, the process is formalized in a patch management process or procedure and may include a service-level agreement (SLA) between the IT and information security teams. The process, procedure, and SLA can vary in terms of the level of detail it contains, including the length of time available for the IT department to patch vulnerabilities

52. *Id.*
53. *Id.* at 2.

based on severity rating, *e.g.*, critical vulnerabilities must be patched within one week.[54]

Organizations typically consider the following characteristics when making decisions about which vulnerabilities to prioritize.

1. Severity Based on CVSS

The CVSS is a de facto international standard for measuring the severity of a vulnerability.[55] The CVSS score uses eight characteristics of a vulnerability to produce a numeric score between zero and ten, which corresponds to a severity rating: low (0.1–3.9), medium (4.0–6.9), high (7.0–8.9), and critical (9.0–10.0).[56] As explained above, the severity of the EternalBlue vulnerabilities used in the NotPetya and WannaCry malware was "high." One of the EternalBlue vulnerabilities was CVE-2017-0143. The numeric score for the vulnerability was 8.1. As an example of the CVSS rating, the eight characteristics for the vulnerability and a brief explanation of the applicable characteristic are as follows:

- Attack Vector—Network. The vulnerability can be executed remotely.
- Attack Complexity—High. A successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation before a successful attack can be expected.
- Privileges Required—None. The attacker does not require any prior access to settings or files to carry out the attack.
- User Interaction—None. The vulnerable system can be exploited without any interaction by a user. For example, it does not require a user to open a file or click on something.
- Scope—Unchanged. The exploited vulnerability can only affect systems managed by the same authority.
- Confidentiality—High. The attacker is able to divulge all the resources within the impacted system.
- Integrity—High. The attacker is able to modify all files protected by the impacted system.

---

54. When an SLA identifies required due dates for different vulnerabilities based on severity, the SLA due dates may have to account for situations where a CVE does not have a patch immediately available.

55. Jay Jacobs et al., *Improving Vulnerability Remediation Through Better Exploit Prediction*, J. CYBERSECURITY, July 17, 2020, at 4.

56. *National Vulnerability Database: Vulnerability Metrics*, NAT'L INST. STANDARDS & TECH., https://nvd.nist.gov/vuln-metrics/cvss (last visited Feb. 12, 2021).

- Availability—High. The attacker is able to fully deny access to resources in the impacted system.

One common approach to patch management is to prioritize patches based on the CVSS score.[57] For internet-accessible systems, the Department of Homeland Security requires federal agencies remediate critical vulnerabilities within fifteen calendar days of initial detection and high vulnerabilities within thirty calendar days of initial detection.[58] Similarly, the Payment Card Industry Data Security Standard (PCI-DSS) contains a requirement that no medium, high, or critical vulnerabilities be present on internet-accessible systems within the payment card environment, absent compensating controls.[59]

Even if an organization limits its patch management to critical and high vulnerabilities, the number of vulnerabilities can be overwhelming. Between 2017 and 2020, there were more than 4,000 critical and high vulnerabilities reported by US-CERT each year.[60]

2. Availability and Use of an Exploit

A different approach to patch management focuses on whether attackers have exploited the vulnerability or whether an exploit is available. A vulnerability is only a weakness in particular software.[61] In order for an attacker to exploit the vulnerability, the attacker needs a written exploit—software code that takes advantage of the vulnerability. Of the thousands of vulnerabilities identified in software every year, written exploits are available for only a small percentage.[62] An even smaller number of exploits are

---

57. Jacobs et al., *supra* note 55, at 6.

58. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., BINDING OPERATIONAL DIRECTIVE 19-02, VULNERABILITY REMEDIATION REQUIREMENTS FOR INTERNET-ACCESSIBLE SYSTEMS (2019) (available at https://cyber.dhs.gov/assets/report/bod-19-02.pdf).

59. PAYMENT CARD INDUS. DATA SEC. STANDARD, REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 99 (May 2018) (Requirement 11.2.2–11.2.3).

60. *National Vulnerability Database: CVSS Severity Distribution over Time*, NAT'L INST. STANDARDS & TECH., https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time (last visited Feb. 12, 2021). The chart relies on CVSS V2 scores, instead of the current CVSS V3. *See id.* Under CVSS V2, a numeric value of seven or greater was a high severity vulnerability. *Id.* CVSS V3 added an additional severity level of critical for numeric values of nine or greater. *Id.*

61. Gary Stoneburner et al., *Risk Management Guide for Information Technology Systems*, NAT'L INST. STANDARDS & TECH. 15 (July 2002), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf.

62. MEHRAN BOZORGI ET AL., BEYOND HEURISTICS: LEARNING TO CLASSIFY VULNERABILITIES AND PREDICT EXPLOITS (2010), https://cseweb.ucsd.edu/~saul/papers/kdd10_exploit.pdf (estimating written exploits are available for 10–15% of vulnerabilities); Jacobs et al., *supra* note 55, at 5 (estimating written exploits are available for approximately 12% of vulnerabilities).

actually used to target corporate networks.[63] One approach suggested by security researchers is to prioritize patching based on whether a published exploit is available.[64]

3. Characteristics of the System

A third consideration for determining which systems to patch is the characteristics of the system. Important characteristics include whether or not the system is internet facing and how critical the system is to the business. A system that is internet facing is more vulnerable to exploitation because an attacker does not need to be on the same network to exploit the vulnerability. The criticality of the system to the business is important because critical systems should be prioritized for patching.

C. Other Compensating Controls

Sometimes patching a piece of software is not practical because it would be too disruptive to the organization. Some older systems may be "fragile" and critical to the business. Because the system is fragile, patching the system may break the critical application or service. Other operating systems may not be able to be patched because they have applications that do not work with newer versions of the operating system. This can occur when a version of Microsoft Windows reaches its end of life. For example, Microsoft stopped supporting Windows 7 in January 2020, and it will end support for Windows 10 in May 2021.[65]

When this occurs, the IT and information security teams will typically rely on other techniques, or "compensating controls," to reduce the risk that the vulnerability will be exploited. The other techniques can include increasing logging and monitoring on the unpatched systems or reducing accessibility to the system through

63. CARL SABOTTKE ET AL., VULNERABILITY DISCLOSURE IN THE AGE OF SOCIAL MEDIA: EXPLOITING TWITTER FOR PREDICTING REAL-WORLD EXPLOITS (2015), https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sabottke.pdf (observing exploits in the wild for 1.3% of vulnerabilities); Jacobs et al., *supra* note 55, at 2 (observing exploits in the wild for 5.5% of vulnerabilities).

64. Jacobs et al., *supra* note 55, at 10 ("For example, if a firm addresses vulnerabilities that have a proof-of-concept code published in Exploit DB, our model will achieve a comparable level of coverage, '*but at one-quarter the level of effort*.'") (emphasis added).

65. *Products Ending Support in 2021*, MICROSOFT, https://docs.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2021 (Mar. 11, 2021); *Support for Windows 7 Has Ended*, MICROSOFT, https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-7-support (last visited Feb. 12, 2021).

an "allow list."[66] An allow list is a list of IP addresses that are permitted to access the unpatched system.

III. OVERVIEW OF SECURITY STANDARDS RELATING TO VULNERABILITY AND PATCH MANAGEMENT

Like many other technical areas of responsibility, non-profit organizations and government agencies provide technical standards to guide information security professionals. The standards address a wide range of security concepts and establish "best practices" for different aspects of a comprehensive information security program. All of the leading security standards now reference vulnerability management and patch management. The leading security standards include the National Institute of Standards and Technology (NIST), Center for Internet Security's Critical Security Controls, International Organization for Standardization (ISO) 27000 standards, and PCI-DSS. These standards have been endorsed by the California Attorney General's Office and the Ohio Data Protection Act.[67] An overview of the leading security standards and their references to vulnerability management and patch management are provided below.

A. NIST

NIST is an agency of the United States Department of Commerce that functions as the "lead national laboratory for providing the measurements, calibrations, and quality assurance techniques which underpin United States commerce, technological progress, improved product reliability and manufacturing processes, and public safety."[68] In 2014, Congress amended the National Institute of Standards and Technology Act and directed NIST to develop a "voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to

66. Katie Stewart, *Establish and Maintain Whitelists (Part 5 of 7: Mitigating Risks of Unsupported Operating Systems)*, CARNEGIE MELLON UNIV.: SOFTWARE ENG'G INST. (Oct. 25, 2017), https://insights.sei.cmu.edu/insider-threat/2017/10/establish-and-maintain-whitelists-part-5-of-7-mitigating-risks-of-unsupported-operating-systems.html. The term whitelist is also known as "allow list." Emma W, *Terminology: It's Not Black and White*, NAT'L CYBER SEC. CTR. (Apr. 30, 2020), https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white. Many organizations, including the United Kingdom's National Cyber Security Centre, have stopped using the term "whitelist" and use "allow list" instead. *Id.*

67. *See* KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT 2012–2015, at 30 (Feb. 2016) (available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf); *see also* Ohio Data Protection Act, OHIO REV. CODE ANN. §§ 1354.01–1354.05.

68. 15 U.S.C. § 271(b)(1).

cost-effectively reduce cyber risks to critical infrastructure."[69] The same year, NIST published version 1.0 of the NIST Cybersecurity Framework.[70] In April 2018, NIST published version 1.1, the current version of the NIST Cybersecurity Framework (NIST Framework).[71] The NIST Framework identifies five core "functions" for cybersecurity and matches each function with a subcategory and an informative reference for existing standards and guidelines.[72] The following subcategories notably identify and address vulnerability management and patch management as part of these best practices:

- DE.CM-8: Vulnerability scans are performed.
- ID.RA-1: Asset vulnerabilities are identified and documented.

Another relevant NIST publication is NIST's flagship information security publication, Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, which provides a catalog of security and privacy controls for information systems and organizations.[73] In this document, two controls relevant to vulnerability management and patch management are set forth: Control RA-5, Vulnerability Monitoring and Scanning, cites monitoring and scanning for vulnerabilities in the system at a frequency defined by the organization,[74] while Control SI-2, Flaw Remediation, recommends that organizations test software updates then install "security-relevant" software updates within an "organization-defined time period" after release of the update.[75]

B. Center for Internet Security Controls

The Center for Internet Security (CIS) is a nonprofit organization whose mission is "to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves

69. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

70. *See Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*, NAT'L INST. STANDARDS & TECH. (Feb. 12, 2014), https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

71. *See Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*, NAT'L INST. STANDARDS & TECH. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

72. *Id.* at 6–7.

73. *See generally* Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, NAT'L INST. STANDARDS & TECH. (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

74. *Id.* at 269.

75. *Id.* at 333.

against pervasive cyber threats."[76] Similar to NIST, CIS has developed the "CIS Controls," a set of twenty security controls.[77] Among the six priority controls, referred to as the "Basic CIS Controls," is CIS Control 3: "Continuous Vulnerability Management."[78] The subcontrols for CIS Control 3 address the specific requirements to implement the control:

- CIS Control 3.1: Run Automated Vulnerability Scanning Tools
- CIS Control 3.2: Perform Authenticated Vulnerability Scanning
- CIS Control 3.3: Protect Dedicated Assessment Accounts
- CIS Control 3.4: Deploy Automated Operating System Patch Management Tools
- CIS Control 3.5: Deploy Automated Software Patch Management Tools
- CIS Control 3.6: Compare Back-to-back Vulnerability Scans
- CIS Control 3.7: Utilize a Risk-rating Process

Additionally, CIS Control 18.8, relating to Application Software Security, requires that organizations "[e]stablish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact [the organization's] security group."[79]

C. ISO

The ISO is an international organization that publishes standards for different industries, including information security.[80] The ISO 27000 standards series, which are published jointly by the ISO and the International Electrotechnical Commission (IEC), is meant to provide best practices for information security management.[81]

---

76. *About Us*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/about-us/ (last visited Feb. 13, 2021).

77. *CIS Controls Navigator*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/cis-controls-implementation-groups/ (last visited Feb. 13, 2021).

78. *Continuous Vulnerability Management*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/continuous-vulnerability-management/ (last visited Feb. 13, 2021).

79. *18.8: Establish a Process to Accept and Address Reports of Software Vulnerabilities*, CONTROLS ASSESSMENT SPECIFICATION, https://controls-assessment-specification.readthedocs.io/en/latest/control-18/control-18.8.html (last visited Feb. 13, 2021).

80. *See generally Standards*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/standards.html (last visited Jan. 18, 2021).

81. ISO/IEC 27001:2013(en), INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (last visited Mar. 1, 2021). This version was reviewed and confirmed in 2019. ISO/IEC 27001:2013, INT'L ORG. FOR STANDARDIZATION (Oct. 2013), https://www.iso.org/standard/54534.html.

Organizations that adopt and implement ISO 27000 can hire third-party auditors to certify the company as compliant with different standards that are part of the series. A common standard for certification is ISO 27001.[82] The next standard in the series, ISO 27002, provides a reference for organizations implementing ISO 27001. One of the controls, or measures taken to reduce information security risks, identified in ISO 27002 is control A.12.6—Technical vulnerability management.[83] This control requires that "[i]nformation about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk."[84] A series of other steps and implementation guidance includes maintaining an accurate inventory of assets on the network, identifying roles and responsibilities for members of the organization who support vulnerability management, creating a timeline for the process, and analyzing the risks for implementing a patch.

D. PCI-DSS

The PCI-DSS is a standard promulgated by the payment card industry that applies to the various entities that process payment cards—merchants, processors, service providers, and banks.[85] First released in 2004 and updated periodically, the standard sets a baseline of technical and operational requirements that the payment card brands direct entities to follow. The current version requires organizations to scan for internal and external security vulnerabilities and patch or mitigate them. In addition, PCI-DSS explicitly requires the minimum frequency for scanning, the time in which patches must be applied, and the risk rating score for patching:

- Requirement 6.1: Establish a process to identify security vulnerabilities using reputable outside sources for security vulnerability information and assign a risk ranking (for example as "high" "medium" or "low") to newly discovered security vulnerabilities.
- Requirement 6.2: Ensure that all system components and software are protected from known vulnerabilities by

82. ISO/IEC 27002:2013, INT'L ORG. FOR STANDARDIZATION (Oct. 2013), https://www.iso.org/standard/54533.html.

83. *Id.*

84. *Id.*

85. *About Us*, PAYMENT CARD INDUS. SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us/ (last visited Feb. 14, 2021).

installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

- Requirement 11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations changes in network topology firewall rule modifications product upgrades).
- Requirement 11.2.1: Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.
- Requirement 11.2.2: Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

IV. LEGAL RISKS

Following a data breach, the victim organization can face regulatory investigations and enforcement actions, as well as civil litigation, often in the form of class actions.[86] The potential legal liability depends on a variety of factors, including the data the attacker accesses or acquires and what the company did to protect itself and its data. A review of regulatory enforcement actions and guidance, as well as evolving case law, reveal that issues relating to vulnerability and patch management have been recognized as the basis for liability.

A. Regulators

A variety of state and federal regulators take the position that they have jurisdiction to bring legal action against a company in response to a breach. Specific industry regulators may have enforcement authority under statutes that apply to particular industries. For example, the Federal Trade Commission (FTC) enforces the Federal Trade Commission Act (FTCA) (in the context of consumer protection) and the Gramm-Leach-Bliley Act (GLBA) (in the

86. This article does not address legal implications under contract law or foreign legal requirements. Both should also be considered and may impose additional legal risks.

context of financial institutions), the Department of Health and Human Services Office of Civil Rights (HHS OCR) enforces the Health Insurance Portability and Accountability Act (HIPAA), and the Securities and Exchange Commission (SEC) enforces the Safeguards Rule of Regulation S-P. Beginning with an enforcement action against Guess? and through publications about information security,[87] the FTC has indicated that effective vulnerability management and patch management are important considerations in its determination of whether companies, including vendors, have "reasonable" information security practices. HHS OCR has similarly indicated that it considers vulnerability management and vulnerability management to be important parts of an information security program. The SEC has not brought an enforcement action for failure to implement vulnerability management and risk management, but it has discussed the importance of them in publications.

1. Federal Trade Commission

The FTC is an independent federal agency aimed at protecting consumers and competition.[88] Through enforcement, education, and advocacy, it protects consumers from unfair and deceptive practices in vast sectors of the economy.[89] The FTC brings a variety of enforcement actions, addressing an array of issues. Relevant to information security are the FTC's enforcement actions under both the "deceptiveness" and "unfairness" prongs of Section 5 of the FTC Act and the Safeguards Rule under the GLBA.[90] In recent enforcement actions and in official publications, the FTC has demonstrated a growing interest in vulnerability management and patch management.

a. Enforcement Under the FTCA

Purporting to act under its authority to prevent "unfair" practices in commerce, the FTC has brought enforcement actions against companies for a failure to implement reasonable cybersecurity measures. While the existence and scope of that jurisdiction continues to be debated, in *FTC v. Wyndham Worldwide Corporation*,

87. Guess?, Inc., 136 F.T.C. 507, 511 (2003) (Complaint) (FTC alleged Guess? failed "to implement reasonable and appropriate measures to secure and protect the databases that support or connect to the website" by failing to "test or otherwise assess the website's or the application's vulnerability to attacks . . . .").

88. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Dec. 28, 2020).

89. *Id.*

90. 15 U.S.C. § 45(a)(1); 16 C.F.R. §§ 314.1–314.5 (2002).

the Court of Appeals for the Third Circuit affirmed the FTC's authority to regulate cybersecurity under the unfairness prong of Title 15 U.S.C. Section 45(a).[91] This decision has been criticized on a number of grounds, including because the FTC failed to provide notice to companies about what constitutes "reasonable" information security practices.[92] In *FTC v. Wyndham Worldwide Corporation*, the Third Circuit held that fair notice is satisfied when a company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.[93] The court observed that the relevant inquiry under subsection 45(n) for unreasonableness is a cost-benefit analysis that considers "the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[94]

In the *Wyndham* case, the FTC alleged that hackers attacked the Wyndham Corporation's computer systems in three separate incidents in 2008 and 2009, stealing hundreds of thousands of consumers' PII and leading to over $10 million in fraudulent charges.[95] Following the attacks, the FTC filed suit in federal district court alleging Wyndham engaged in "unfair cybersecurity practices" and the corporation "unreasonably and unnecessarily exposed consumers" PII to attack.[96] The FTC alleged Wyndham "permitt[ed] Wyndham-branded hotels 'to connect insecure servers to [h]otels and [r]esorts' networks, including servers using outdated operating systems that could not receive security updates or patches to address known security vulnerabilities.'"[97] This is one of many complaints by the FTC that allege a company did not have "reasonable" information security practices, in part, due to unpatched or unsupported software.

---

91. 799 F.3d 236, 240 (3d Cir. 2015). Relevant here, one of the charges against Wyndham, involved insufficient patch management on network connect computers. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014).

92. *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 719 (2013); *see also* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 183 (2008). *See generally* Geoffrey A. Manne & Kristian Stout, *When "Reasonable" Isn't: The FTC's Standardless Data Security Standard*, 15 J.L. ECON. & POL'Y 67 (2019). *See also* LabMD, Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018) (ruling FTC cease and desist order was unenforceable due to vagueness of requirement of "reasonably designed data-security program").

93. *Wyndham Worldwide Corp.*, 799 F.3d at 256.

94. *Id.* at 255.

95. *Id.* at 240.

96. *Id.*

97. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014).

Although not directed at internal vulnerability management and patch management programs, two FTC enforcement actions against software and hardware vendors for their alleged failure to provide proper software updates to their customers demonstrate the FTC's consideration of the importance of software updates. In 2011, the FTC brought an enforcement action against Oracle due in part to software updates to Java, a programming language that Oracle had developed.[98] The FTC alleged that Oracle knew that its consumers were vulnerable to attack due to Java's insufficient update process.[99] The FTC cited internal Oracle documents stating that the "Java update mechanism is not aggressive enough or simply not working."[100] The FTC alleged when Java consumers updated the Java software, unbeknownst to the consumers, prior versions of the software remained on the consumers' computers.[101] The FTC claimed that hackers exploited the flaw and accessed consumers' data through the outdated Java versions.[102] In the consent agreement, the FTC ordered Oracle to improve the Java updating process and conspicuously inform consumers of the versions of Java installed on their devices.[103]

In 2016, the FTC brought a similar action against ASUSTeK Computer, Inc. (ASUS) for its alleged failure to protect users of ASUS's routers from cyberattack.[104] ASUS, a hardware manufacturer, developed software for its routers and was responsible for developing and distributing software updates to patch security vulnerabilities.[105] Many of ASUS's routers included features called AiCloud and AiDisk, which allowed consumers to plug USB hard drives directly into the routers to create an at-home "private personal cloud."[106] In 2014, hackers exploited vulnerabilities in AiCloud and accessed over 12,900 consumers' storage devices.[107] The FTC alleged hackers accessed the users' connected storage devices without credentials by bypassing the AiCloud login screen.[108] Additionally, the FTC alleged the default settings on AiDisk made

98. Oracle Corp., No. 132-3115, 2015 WL 9412609, at *1 (F.T.C. Dec. 21, 2015) (Complaint).
99. *Id.*
100. *Id.* at *2.
101. *Id.*
102. *Id.* at *3.
103. *Id.* at *6–7 (Order).
104. ASUSTeK Comput., Inc., No. 142-3156, 2016 WL 4128217, at *1 (F.T.C. July 18, 2016) (Complaint).
105. *Id.*
106. *Id.* at *2.
107. *Id.*
108. *Id.*

the storage devices accessible to anyone on the internet who had the routers' IP addresses.[109] The FTC alleged that ASUS did not notify consumers about available security updates.[110] Moreover, the tool that informed consumers of available security updates often told consumers their software was up-to-date when, in fact, newer software with "critical security updates" was available.[111] The FTC ordered ASUS to establish a comprehensive security program.[112] Specifically, the FTC ordered ASUS to notify consumers about software updates and to refrain from making misleading statements regarding whether consumers' products were up-to-date.[113]

In recent consent decrees, the FTC has consistently ordered companies to implement patch management programs.[114] In 2020, the number of people who participated in Zoom meetings each day rose from approximately 10 million to 300 million.[115] Within this context, the FTC claimed Zoom undermined the security of its users by engaging in unfair and deceptive trade practices.[116] According to the FTC, Zoom had failed to maintain proper internal network security, despite touting its advanced security practices.[117] Relevant here, the FTC alleged Zoom was a year or more behind in patching software in its commercial environment.[118] As part of its settlement with the FTC—in addition to discontinuing some of the practices alleged in the complaint—Zoom must implement specific security safeguards, including conducting vulnerability scans on at least a quarterly basis and implementing policies and procedures to remediate critical or high vulnerabilities no later than thirty days after detection.[119] Zoom must hire a third party to conduct an

109. *Id.* at *3.
110. *Id.* at *4.
111. *Id.* at *6.
112. *Id.* at *13–15 (Order).
113. *Id.* at *14.
114. Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, FED. TRADE COMM'N: BUS. BLOG (Jan. 6, 2020, 9:46 AM), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance ("We were also mindful of the 11th Circuit's 2018 LabMD decision, which struck down an FTC data security order as unenforceably vague. Based on this learning, in 2019 the FTC made significant improvements to its data security orders.").
115. Zoom Video Commc'ns, Inc., No. 192-3167, 2020 WL 6589815, at *2 (F.T.C. Nov. 9, 2020) (Complaint).
116. *Id.* at *2–3.
117. *Id.* at *3.
118. *Id.*
119. Zoom Video Commc'ns, Inc., No. 192-3167, 2020 WL 6589819, at *1–3 (F.T.C. Nov. 9, 2020) (Analysis of Proposed Consent Order to Aid Public Comment).

independent assessment of the new safeguards once every other year for twenty years.[120]

Moreover, in post-2018 cases, involving SkyMed, D-Link, and InfoTrax, the FTC ordered companies to implement security safeguards that include vulnerability testing.[121] For example, it ordered InfoTrax to scan for vulnerabilities every four months.[122]

The consent agreement in Zoom and agreements in other recent cases exemplify the FTC's recent specific focus on ordering entities to implement vulnerability management programs. The requirement to implement a vulnerability management program is more specific than previous orders, which at times vaguely required companies to implement reasonable security programs "designed to protect the security . . . of personal information . . . ."[123] The more recent orders are still broad and susceptible to a wide range of interpretations, and ultimately, companies face potential legal risk as they try to navigate the logistical and practical challenges of prioritizing which out-of-date software to update.

b. Enforcement Under the GLBA

While the FTC has brought enforcement actions for violation of the GLBA Safeguards Rule, the complaints and consent orders have not explicitly referenced vulnerability management and patch management. The Safeguards Rule, which implements section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions develop a written information security program that contains "administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[124] The Safeguards Rule identifies general requirements. Influenced by the New York Department of Financial Services (NY DFS) Cybersecurity Requirements for Financial Services Companies, the FTC has proposed a revised Safeguards Rule that contains more specific information security requirements.[125] Although the proposed revision does not explicitly reference vulnerability management and patch management, it does reference periodic vulnerability

120. *Id.* at *2–3.

121. Skymed Int'l, Inc., No. 192-3140, 2020 WL 7646326, at *4 (F.T.C. Dec. 16, 2020); FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD (N.D. Cal. Sept. 19, 2017) (Leagle); InfoTrax Sys., L.C., No. 162-3130, 2019 WL 6168270, at *3 (F.T.C. Nov. 12, 2019).

122. *InfoTrax Sys., L.C.*, 2019 WL 6168270, at *3.

123. LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018).

124. 16 C.F.R. § 314.1 (2002).

125. *See* Standards for Safeguarding Customer Information, 84 Fed. Reg. 13,158 (Apr. 4, 2019).

assessments.[126] Neither the proposed revisions nor the NY DFS regulations define vulnerability assessments.

c. FTC Publications

The FTC has issued a number of publications addressing what it considers reasonable for vulnerability management and patch management. In the FTC brochure, *Start with Security*, the FTC explains the need for patch management programs stating:

> [d]epending on the complexity of your network or software, you may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third-party software is an important step to reducing the risk of a compromise.[127]

In 2016, the FTC recommended that entities, as part of their general network security, regularly check with vendors and experts for alerts about vulnerabilities and "implement policies for installing vendor-approved patches to correct problems."[128] Then in 2020, the FTC reiterated its requirement for patch management programs, explaining that its recent consent decrees had ordered companies to implement such programs.[129]

Together, the orders and publication suggest that the FTC believes that patch management programs are fundamental to reasonable cybersecurity but also that the agency understands that it is not a one-size-fits-all process. As explained in Section II, the adequacy of vulnerability management and patch management remains a question of degree. For many companies, it is cost prohibitive to patch every out-of-date software on every system. Instead, companies prioritize based on risk calculations. Thus, vulnerability management and patch management are unlike some other areas of information security, which can be binary, *e.g.*, customer files are encrypted or they are not, default passwords must be changed or they are not. The exceptions to this general observation are when a company has internal policies or makes statements that a third party or the public relies on about its vulnerability management and patch management programs that it fails to follow. Setting

126. *Id.* at 13,176.

127. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 12 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

128. FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 10 (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

129. Smith, *supra* note 114.

these exceptions aside, in the wake of this ambivalent guidance, a company needs to make decisions about what is reasonable, and they may not be the same decisions the FTC would have made.

2. U.S. Department of Health and Human Services Office for Civil Rights (HHS OCR)

Like the FTC, the HHS OCR has also demonstrated an interest in investigating and bringing enforcement actions for vulnerability management and patch management practices.[130] HHS OCR enforces the implementing regulations under HIPAA and the HITECH Act of 2009.[131] The applicable regulations for information security are the Privacy Rule[132] and the Security Rule.[133] Entities subject to the regulations ("covered entities") include certain healthcare providers, health plans, and healthcare clearinghouses.[134] Business associates of covered entities are also subject to certain regulatory oversight by HHS OCR.[135] This includes any person or organization that performs services for a covered entity that includes the use of or disclosure of protected health information (PHI).[136]

The Security Rule requires covered entities and business associates to protect electronic PHI (ePHI) and establishes minimum security requirements to do so.[137] The Security Rule consists of "standards" and "implementation specifications." Some of the standards are required, while others are considered "addressable." Although the Security Rule does not reference vulnerability management or patch management, covered entities and business associates are required under the rule to conduct a "risk analysis," implement a "risk management" process, and ensure "transmission

130. *See* Resolution Agreement between HHS OCR and Anchorage Community Mental Health Services, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 2, 2014), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf.

131. OCR, *About Us*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Oct. 8, 2019), https://www.hhs.gov/ocr/about-us/index.html; OCR, *HITECH Act Rulemaking and Implementation Update*, U.S. DEP'T OF HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/security/guidance/hitech-act-rulemakingimplementation-update/index.html.

132. 45 C.F.R. pt. 160 (2013); 45 C.F.R. §§ 164.102–164.106 (2013); 45 C.F.R. §§ 164.302–164.318 (2013).

133. 45 C.F.R. pt. 160, 164.

134. 45 C.F.R. § 160.103 (2014).

135. *Id.*

136. *Id.*

137. *Id.* ePHI is defined as protected health information that is transmitted by electronic media or maintained in electronic media. *Id.*

security."[138] This process likely will include evaluations of a company's vulnerability and patch management.

A risk analysis is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI a covered entity or business associate holds.[139] Under the Security Rule, the risk management process implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.[140] According to an HHS OCR newsletter from July 2018, a risk analysis includes identifying risks and vulnerabilities that unpatched software poses to an organization's ePHI.[141] In the July 2018 newsletter, HHS OCR stated that implementing security measures can include "installing patches if patches are available and patching is reasonable and appropriate."[142]

Failures to adequately address vulnerabilities have also been explicitly cited in HHS OCR enforcement actions. In a settlement announced in 2014, HHS OCR stated that a covered entity suffered a breach of unsecured ePHI due to the covered entity's failure to regularly update its "IT resources with available patches."[143] The settlement agreement[144] indicated that the failure to update IT resources with available patches was a violation of the transmission security requirement of the Security Rule.[145]

As such, HHS OCR clearly considers vulnerability management and patch management as important requirements for covered entities and business associates. However, the 2018 newsletter indicates that HHS OCR may take a potentially flexible approach to evaluating patch management through an understanding that deployment of a patch may not be appropriate. In those cases, HHS OCR likely expects that entities implement compensating controls

138. 45 C.F.R. §§ 164.308(a)(1)(ii)(A)–(B); *id.* § 164.312(e)(1).

139. *Id.* § 164.308(a)(1)(ii)(A).

140. *Id.* § 164.308(a)(1)(ii)(B).

141. *Guidance on Software Vulnerabilities and Patching*, U.S DEP'T OF HEALTH & HUM. SERVS. OFF. FOR C.R. 1 (June 2018), https://www.hhs.gov/sites/default/files/june-2018-newsletter-software-patches.pdf.

142. *Id.* at 2.

143. *Bulletin: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software*, U.S DEP'T OF HEALTH & HUM. SERVS. OFF. FOR C.R. 1 (Dec. 2014), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf.

144. *See* Resolution Agreement, *supra* note 130.

145. The Security Rule requires "transmission security" which are "technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network." 45 C.F.R. § 164.312(e)(1) (2013).

to reduce the risk of identified vulnerabilities in the unpatched software.[146]

3. The Securities and Exchange Commission

The SEC enforces a variety of different statutes and regulations, including the Safeguards Rule of Regulation S-P, which requires that brokers, dealers, investment companies, and registered investment advisors adopt written policies and procedures reasonably designed to protect customer records and information.[147] In the cases where the SEC has brought enforcement actions for violations of the Safeguards Rule, the SEC has alleged the companies failed to implement policies and procedures related to encrypting customer PII or employing a firewall to protect web servers.[148] It has not yet alleged in an enforcement action that a failure to have written policies and procedures related to vulnerability management and patch management were a violation of the Safeguards Rule.

However, the SEC's Office of Compliance Inspections and Examinations (OCIE) has released several publications that highlight vulnerability management and patch management. In May 2017, following reports of widespread attacks by the malware WannaCry, OCIE released a "risk alert" that, in an examination of seventy-five registered broker-dealers, investment advisors, and investment companies, all broker-dealers and ninety-six percent of investment management firms had a regular process in place to install software patches.[149] However, the risk alert reported that a minority of the inspected entities had a "significant number of critical and high-risk security patches that were missing important updates."[150] In a 2020 report on "Cybersecurity and Resiliency Observations," OCIE reported that inspected organizations used vulnerability scanning to routinely scan systems within the organization and a patch management program to patch software and hardware.[151] OCIE reiterated the importance of patch management and vulnerability management as a way to "enhance cybersecurity

146. Resolution Agreement, *supra* note 130, at 1–2.
147. 17 C.F.R. § 248.30(a) (2005).
148. R.T. Jones Cap. Equities Mgmt., Inc., No. 3-16827 (S.E.C. Sept. 22, 2015).
149. *Cybersecurity: Ransomware Alert*, OFF. COMPLIANCE INSPECTIONS & EXAMINATIONS 1–2 (May 17, 2017), https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf.
150. *Id.* at 2.
151. Off. Compliance Inspections & Examinations, *Cybersecurity and Resiliency Observations*, U.S. SEC. & EXCH. COMM'N 4–5 (Jan. 27, 2020), https://www.sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf.

preparedness and operational resiliency" in a July 10, 2020 risk alert.[152] Specifically, the OCIE risk alert stated, "[i]mplementing proactive vulnerability and patch management programs that take into consideration current risks to the technology environment, and that are conducted frequently and consistently across the technology environment."[153]

These SEC publications indicate that the SEC may consider written policies and procedures for vulnerability management and patch management to be a part of an information security program that is "reasonably designed" to protect customer records and information and in compliance with the Safeguards Rule.

B. State Statutes

Regulators and plaintiffs in private litigation have alleged poor patch management and vulnerability management practices violate certain state statutes. All fifty states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws. In addition to breach notification, half of the states have enacted laws that require certain data security practices. The enforcement mechanism for these laws vary and include private rights of action or enforcement by state regulators. California was the first state to enact both a data breach notification law and a data security practices law. Enacted in 2004, the California data security practices law requires businesses that own or license information about California residents to "implement and maintain reasonable security procedures and practices . . . to protect the personal information . . . ."[154] The law provides a private right of action by an injured party.[155] Many other states have since joined California in requiring reasonable information security. Regulators take the view, as expressed in statements implementing regulations, that these reasonable security practices include patching outdated software.

In a 2016 report, the California Attorney General identified the Center for Internet Security's Critical Security Controls as the minimum level of information security that organizations must meet to have reasonable security.[156] As explained in Section II, CIS Control 3 requires vulnerability management and patch management. In

152. *Cybersecurity: Ransomware Alert*, OFF. COMPLIANCE INSPECTIONS & EXAMINATIONS 2 (July 10, 2020), https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.
153. *Id.* at 3.
154. CAL. CIV. CODE § 1798.81.5(b).
155. CAL. CIV. CODE § 1798.84(b).
156. HARRIS, *supra* note 67, at 30.

the "Message from the Attorney General," then-Attorney General Kamala Harris specifically cited that for the breaches from 2012 to 2015 in California, "nearly all of the exploited vulnerabilities, which enabled these breaches, were compromised more than a year after the solution to patch the vulnerability was publicly available."[157]

Like California, Oregon requires businesses "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information . . . ."[158] The Oregon law also provides examples of reasonable safeguards for companies to use, including "[a]pplying security updates and a reasonable security patch management program to software that might reasonably be at risk of or vulnerable to a breach of security."[159] Massachusetts has a similar requirement in the regulations implementing its data security practices law. Under the regulation, businesses that have systems connected to the internet and containing personal information must have "reasonably up-to-date firewall protection and operating system security patches."[160]

Recently, New York has joined the group of states that requires data security practices. Beginning in March 2020, New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act went into effect. The new law imposes a variety of new information security requirements on companies, including requiring businesses that own or license New York residents' private information "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information . . . ."[161] The law identifies examples of safeguards for companies to adopt to comply with the reasonable security requirement. Included within these safeguards are identifying reasonably foreseeable internal and external risks, assessing risks in network and software design, and regularly testing and monitoring the effectiveness of key controls, systems, and procedures.

C. Common Law Causes of Action

When an attacker successfully breaches a company network and acquires (or in very few states, accesses) PII, state laws may require the company to notify the individuals whose PII has been impacted in certain circumstances. Following the notifications, impacted individuals often file class action lawsuits against the company. The

157. *Id.* at ii.
158. OR. REV. STAT. § 646A.622(1).
159. *Id.* § 646A.622(2)(d)(B)(ii).
160. 201 MASS. CODE REGS. 17.04(6).
161. N.Y. GEN. BUS. LAW § 899-bb(2).

alleged causes of action are varied and can include negligence, negligence per se, gross negligence, and unjust enrichment. Issues related to vulnerability and patch management are emerging as relevant bases for these causes of action.

1. Negligence

In data breach cases, plaintiffs frequently, and often unsuccessfully, allege negligence under a common law tort theory. A claim of negligence requires that a plaintiff allege four elements: duty, breach, causation, and damages.[162] The availability of plaintiffs to successfully allege negligence as a cause of action following a data breach is a contested legal issue. In several jurisdictions, courts have ruled in favor of defendants and have dismissed negligence claims in this context for a variety of reasons.[163] In states where negligence has been an available cause of action in this context, plaintiffs may attempt to allege that a defendant's patch management and vulnerability management procedures are relevant to determining whether the defendant satisfied its duty to use reasonable care to safeguard sensitive personal information. While duty is a question of law, standard of care is a question of fact, established through expert opinion,[164] legislation, regulation, or fixed by the factfinder by applying the facts of the case.[165]

In this context, courts typically have not specified the standard of care required by a defendant, including whether that standard of care requires adequate vulnerability management and patch management. Some courts have referred to the standard in vague

---

162. A general rule of negligence is that "anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act." RESTATEMENT (SECOND) OF TORTS § 302 cmt. a (AM. L. INST. 1965).

163. On a variety of different bases, courts have dismissed data breach cases that allege negligence. *See, e.g.*, *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 977 (N.D. Cal. 2016) (dismissing claims brought under Indiana law for negligence because Indiana law does not provide for a private cause of action for a database owner that fails to adequately protection personal information); *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 477 (D. Md. 2020) (dismissing claims brought under Illinois law for negligence because there is no duty under Illinois law to protect personal information); *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (dismissing claims under Alaska, California, Illinois, Iowa, and Massachusetts law due to the economic loss rule).

164. In medical malpractice cases, determining standard of care "requires expert testimony and presents a question of fact for the jury." K.H. *ex rel.* H.S. v. Kumar, 122 A.3d 1080, 1097 (Pa. Super. Ct. 2015).

165. *See* RESTATEMENT (SECOND) OF TORTS § 285 (AM. L. INST. 1965); *see also* Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017) (explaining that while duty is a legal question, the scope of the duty is a question of foreseeability).

"reasonableness" terms.[166] Others have provided more specific references to whether the company used industry standards,[167] whether the company followed its own written policies,[168] and whether the company was aware of the vulnerability that led to the breach.[169] These three characteristics may be relevant in a case where the plaintiffs allege that a defendant failed to patch a known software vulnerability.

a. Cases Referencing Industry Standards

In the privacy class action filed against Target following the cyberattack that affected more than forty-one-million customer payment card accounts, the plaintiffs claimed Target failed to comply with PCI-DSS.[170] The plaintiffs also claimed Target owed a duty "to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting [Plaintiffs'] personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons."[171] Target did not dispute this element, and some of the negligence claims alleging a failure to comply with PCI-DSS survived Target's motion to dismiss. Similarly, the plaintiffs in *Sackin v. TransPerfect Global, Inc.*

166. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1170 (noting that plaintiffs claimed defendants owed a duty "to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting [Plaintiffs'] personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons") (alteration in original); *see also* Hapka v. Carecentrix, Inc., No. 16-2372-CM, 2016 WL 7336407, at *5 (D. Kan. Dec. 19, 2016) (explaining that plaintiffs sufficiently alleged that employer defendants breached their duty to implement reasonable data security measures in "obtaining, securing, safeguarding, deleting and protecting" plaintiffs' personal information from disclosure).

167. *Sackin*, 278 F. Supp. 3d at 744 ("TransPerfect's cyber-security was not up to industry par . . . ."); Wines, Vines & Corks, LLC v. First Nat'l of Neb., Inc., No. 8:14CV82, 2014 WL 12665802, at *5 (D. Neb. Aug. 20, 2014) (holding that plaintiffs' claim that defendants failed to use "reasonable care and conform to industry standards in securing and protect[ing]" plaintiff's account information survived a motion to dismiss).

168. Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (granting defendant's motion for summary judgment in part because defendant followed its own information security policies).

169. Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *13 (D. Mass. Dec. 31, 2019) ("Because Plaintiffs claim that Defendants failed to employ reasonable security measures, including encryption, which was recommended by the Information Technology Department after two previous data breaches and to adequately train its employees to guard against a phishing scam, the Complaint adequately alleges that Defendants breached their duty of reasonable care."); *see also* Bohannan v. Innovak Int'l, Inc., 318 F.R.D. 525, 527 (M.D. Ala. 2016).

170. Amended Complaint at 121, *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1170 (D. Minn. 2014) (No. 14-2522). Notably, PCI-DSS standards require that companies maintain a vulnerability management program. *See infra* Part III.C.

171. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1170 (alteration in original).

alleged that because TransPerfect's cybersecurity was "not up to industry par," an employee responded to a phishing email and sent copies of W-2 forms and payroll information for all current and former employees to a cybercriminal.[172] The court found that plaintiffs sufficiently alleged "TransPerfect violated its duty to take reasonable steps to protect its employees' PII."[173] Specifically, TransPerfect's cybersecurity was "not up to industry par" because it failed to erect a digital firewall, conduct data security training, or adopt retention and destruction policies.[174] The accepted reliance on industry standards indicates that the industry standards set forth in Section II relating to vulnerability and patch management may be considered in determining the duty of care.

b. Cases Referencing Internal Policies

Courts have found that plaintiffs have sufficiently alleged a breach of duty of reasonable care when plaintiffs have alleged that defendants failed to comply with their own policies.[175] In 2015, a trial court in New York concluded that following a breach of health information, the plaintiffs sufficiently stated a negligence claim because the hospital's privacy policy assured the plaintiffs that the hospital would protect the plaintiffs' information and would not disclose it without consent.[176] Conversely, courts have held that defendants acted reasonably when defendants implemented written information security policies.[177] As such, when companies have internal policies relating to vulnerability and patch management, a failure to comply with those policies may also provide a basis for a plaintiff to allege a duty of care existed.

---

172. Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 744 (S.D.N.Y. 2017).

173. *Id.* at 748.

174. *Id.* at 744, 748.

175. Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *13 (D. Mass. Dec. 31, 2019) ("Because Plaintiffs claim that Defendants failed to employ reasonable security measures, including encryption, which was recommended by the Information Technology Department after two previous data breaches and to adequately train its employees to guard against a phishing scam, the Complaint adequately alleges that Defendants breached their duty of reasonable care."); Abdale v. N. Shore Long Island Jewish Health Sys., Inc., 19 N.Y.S.3d 850, 861 (N.Y. Sup. Ct. 2015) (finding plaintiffs' negligence claim survived a motion to dismiss, the court did not analyze the standard of care and noted defendants allegedly informed plaintiffs their personal information would not be shared with third parties absent consent).

176. *Abdale*, 19 N.Y.S.3d at 861.

177. Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (granting defendant's motion for summary judgment in part because defendant followed its own information security policies).

c. Cases Referencing Knowledge

In 2016, Innovak, a creator of administrative software for school districts, announced users' PII had been comprised in a data breach when hackers infiltrated the internet portal where end users accessed their tax and payroll information.[178] In the privacy class action litigation that followed, the plaintiffs claimed that Innovak knew of the vulnerability since 2014 and "failed to take reasonable steps to prevent a breach."[179] Though neither the court nor the plaintiffs articulated a standard of care, Innovak's alleged awareness of its vulnerabilities and its failure to take affirmative steps led the court to deny Innovak's motion to dismiss.[180]

Although the ability for a plaintiff to allege negligence following a data breach is an undecided issue of law, to reduce the legal risk of a cause of action for negligence, these considerations weigh in favor of a company maintaining and implementing an adequate vulnerability management and patch management program, which includes following the written procedures that apply to the program and staying abreast of industry standards.

2. Negligence Per Se

In the context of data breach litigation, plaintiffs have similarly attempted, with mixed results, to use Section 5 of the FTCA and the failure to use "reasonable measures" to protect personal information as the basis for a claim of negligence per se.[181] In states where courts have held that negligence per se applies, plaintiffs have sought to establish a duty through FTC publications and orders related to vulnerability and patch management.

In 2019, an attack on Capital One affected over 100 million consumers in the United States.[182] The plaintiffs alleged that hackers accessed their data by exploiting a "well-known" vulnerability of the Amazon Web Services cloud where Capital One stored consumers' confidential PII.[183] The court found that the plaintiffs plausibly

178. Bohannan v. Innovak Int'l, Inc., 318 F.R.D. 525, 527 (M.D. Ala. 2016).
179. *Id.* at 530.
180. *Id.*
181. *See In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., No. 19-md-2879, 2020 WL 6290670, at *21 (D. Md. Oct. 27, 2020) (dismissing negligence per se claims brought under Maryland law but denying defendant's motion to dismiss negligence per se claims brought under Connecticut and Georgia law); *In re* Capital One Consumer Data Sec. Breach Litig., No. 1:19md2915 (AJT/JFA), 2020 WL 5629790, at *18 (E.D. Va. Sept. 18, 2020) (dismissing negligence per se claims brought under Virginia law but denying defendant's motion to dismiss negligence per se claims brought under New York law).
182. *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 5629790, at *1.
183. *Id.*

alleged a negligence per se claim under New York law, because the plaintiffs plausibly alleged that the FTCA created an enforceable duty in the data breach context and the plaintiffs were of the class the statute was meant to protect—those whose information was allegedly compromised by a data breach.[184] Further, the plaintiffs imported the standard of care from the FTCA, which, as stated earlier, included provisions related to vulnerability and patch management.[185]

Marriott announced in 2018 that hackers had infiltrated its guest reservation database and had been extricating customers' PII for four years.[186] Plaintiffs sufficiently pled negligence per se predicated on violations of Section 5 of the FTCA under Connecticut law and Georgia law, but not under Maryland law.[187] In its opinion, the court rejected defendants' argument that the "FTC Act cannot serve as the predicate for a negligence claim based on the violation of a statute because it does not 'proscribe a particular standard of care.'"[188] The court explained that several courts had rejected similar arguments by "finding that data breach plaintiffs adequately had pleaded claims of negligence *per se* based on alleged violations of Section 5 of the FTC [A]ct."[189] Because a violation of Section 5 of the FTCA can serve as a predicate for a negligence per se claim, the vulnerability management and patch management considerations within that Act may be considered as part of the risk of civil liability in a class action.

V. CONCLUSION

Though adequate cybersecurity is in many ways viewed as a subjective metric that can be based on factors specific to a company's size, industry, and risk profile, objective measures applicable to general categories of security functions continue to come into focus. Developing caselaw and language relating to regulatory enforcement are making it apparent that vulnerability and patch management are widely becoming recognized as essential functions of an adequate cybersecurity program. Thus, vulnerability and patch

184. *Id.*

185. *Id.* The court found defendants' alleged violations of Section 5 of the FTC did not predicate a negligence per se claim under Virginia law, because only statutes "enacted for public safety" may give rise to negligence per se claims. *Id.* at *18.

186. *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., No. 19-md-2879, 2020 WL 6290670, at *1 (D. Md. Oct. 27, 2020).

187. *Id.* at *24. The court dismissed the negligence per se action under Maryland law because it does not recognize an independent cause of action. *Id.* at *21.

188. *Id.* at *10.

189. *Id.*

management are no longer purely technical functions which concern only a company's IT department, because their existence and sufficiency within a company's cybersecurity program have likewise become the subject of scrutiny of regulators and plaintiffs alike. As such, legal departments are increasingly having to take notice of their company's vulnerability management and patch management programs and evaluate the potential legal risk they pose to the company, even before a data breach occurs.

The Future of Our Fingerprints: The Importance of Instituting Biometric Data Protections in Pennsylvania

*Julia M. Siracuse**

* J.D. Candidate, Duquesne University School of Law, 2021. The author received her Bachelor of Arts with a double major in Chinese and Sociology from the University of Pittsburgh in 2018. She thanks her parents and brothers for their constant support and Professor Ann L. Schiavone for her invaluable guidance and encouragement.

I. INTRODUCTION

Only a few years ago, people would not have thought about using fingerprints or facial recognition to operate a cell phone.[1] Today, these are common features of smartphones that make our lives more efficient and straightforward.[2] These fingerprints and facial recognition features used on smartphones are two examples of a specific type of sensitive data known as biometric data: data that uniquely identifies an individual according to their own physical and behavioral attributes.[3] The scope of biometric data technology is rapidly expanding, resulting in an accumulation of more aspects of daily life revolving around data.[4] Institutions and services that people interact with daily—including social media, banking, retail, and government—now involve the collection and analysis of biometric data.[5] While the implementation of biometric data across these industries has benefits, it comes with substantial risks as well, which must be effectively managed.[6] Individuals, companies, and other entities must understand that biometric data can be hacked by cyber criminals.[7] Today, if an individual's credit card or social security number is stolen, they have the ability to set up a new one.[8] One cannot, however, replace a stolen fingerprint or DNA sample.[9]

---

1. *See* Vindu Goel, *That Fingerprint Sensor on Your Phone Is Not as Safe as You Think*, N.Y. TIMES (Apr. 10, 2017), https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html (stating that fingerprint scanners have turned today's smartphones into miracles of convenience).

2. Riley v. California, 573 U.S. 373, 395 (2014) ("Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower . . . . Today . . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

3. *See* Maria Korolov, *What Is Biometrics? 10 Physical and Behavioral Identifiers That Can Be Used for Authentication*, CSO (Feb. 12, 2019, 3:00 AM), https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html.

4. Leonardo Sam Waterson, *10 Ways Biometric Technology Is Implemented in Today's Business World*, M2SYS (Nov. 29, 2018), http://www.m2sys.com/blog/biometric-technology/10-ways-biometric-technology-implemented-business/.

5. Danny Palmer, *What Is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZDNET (May 17, 2019, 6:33 AM), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

6. *See* Scott Sayce, *Cyber Security: The Future Risk of Biometric Data Theft*, CNA HARDY, https://www.cnahardy.com/news-and-insight/insights/english/cyber-securit-the-future-risk-of-biometric-data-theft (last visited Jan. 16, 2020).

7. *Id.*

8. *Id.*

9. *See id.*; *see also* AnnaMaria Andriotis, *Cash, Plastic or Hand? Amazon Envisions Paying with a Wave*, WALL ST. J., https://www.wsj.com/articles/cash-plastic-or-hand-amazon-

In the United States, there are four states with statutes specifically providing safeguards for biometric data privacy, but with the development of biometric data technology resulting in increasing security risks, more states must enact legislation in order to fully protect citizens' biometric data.[10] Pennsylvania currently does not have a statute regulating the protection and use of its citizens' biometric data, nor do Pennsylvania's data breach notification laws—dictating how Pennsylvania businesses must notify affected Pennsylvania residents when a business experiences a harmful data breach[11]—provide protection for biometric data as personal information.[12] The lack of regulation is surprising given the sensitivity, permanence, and inherently unique features of biometric data.[13] It is imperative to protect Pennsylvania citizens' biometric identities from the risks that come with evolving biometric data practices.[14]

This article will first lay out the background of biometric data and the ways in which it is implemented.[15] Next, it will outline the current framework of U.S. state laws and the European Union's General Data Protection Regulation related to biometric data privacy.[16] Finally, this article will explain why Pennsylvania must enact a statute regulating the collection, retention, and use of the biometric data of its citizens.[17] This section will illuminate the need for state legislation over federal legislation and why a biometric data protection statute would best align with Pennsylvania's interests.[18] It will also discuss how Pennsylvania should approach statutory construction by incorporating a broad definition of "biometric data," affording biometric data protection as a fundamental right, and providing effective remedies for parties harmed by violations, including a private right of action and statutory penalties.[19]

---

envisions-paying-with-a-wave-11579352401 (Jan. 19, 2020, 11:58 AM) (discussing Amazon's vision of implementing the usage of palm prints for customer purchases).

10. *See* Blake Benson, *Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy*, 19 N.C. J.L. & TECH. ON. 161, 161 (2018) (advocating for a federal biometric privacy law).

11. *See generally* Breach of Personal Information Notification Act, 73 PA. STAT. AND CONS. STAT. ANN. §§ 2301–2329.

12. *Id.*

13. Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 KAN. L. REV. 637, 638 (2018).

14. *See infra* Section II.B.

15. *See infra* Section II.

16. *See infra* Section III.

17. *See infra* Section IV.

18. *See infra* Section IV.

19. *See infra* Section IV.

II. BACKGROUND INFORMATION

A. What Is Biometric Data?

In 2014, a group of hackers, suspected of working for the Chinese government, breached the United States Office of Personnel Management, stealing the personal data of an estimated 21 million Americans.[20] The stolen data contained the fingerprint information of 5.6 million people.[21] While federal experts concluded the ability to misuse the fingerprint data was limited in this event,[22] the potential for harm remains.[23] Increased implementation of biometric authentication systems, which compare biometric data to data that is already stored and confirmed in a database,[24] means more opportunities for hackers to use stolen biometric information to bypass or trick supposedly secure authentication systems.[25] Cybercriminals are rapidly finding new ways to profit and benefit from illegal activities, like identity theft, hacking of personal and corporate computer systems, and cyber stalking.[26] They can sell stolen biometric information to third parties, use it to board airplanes,[27] and to recreate fingerprints.[28] Through a tactic called spoofing, cyber hackers take photographs of latent fingerprints—from a surface like a drinking glass—and recreate them in a gelatin mold or artificial

---

20. *See* Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015, 2:00 PM), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.

21. *Id.* Many companies using biometrics do not store your actual fingerprints. *See* Anna Myers, *Can the U.S. Legal System Adapt to Biometric Technology?*, IAAP: PRIV. TECH (Aug. 12, 2016), https://iapp.org/news/a/can-the-u-s-legal-system-can-adapt-to-biometric-technology/. Instead, they convert fingerprint information into authentication codes, which are long numerical sequences that are hard to predict. *Id.* These authentication codes are then stored by the company as fingerprint information. *Id.*

22. Peterson, *supra* note 20.

23. *See generally* Jeremy Bergsman, *Biometrics Are Less Secure than Passwords—This Is Why*, BETANEWS, https://betanews.com/2016/08/24/unsafe-biometrics/ (last visited Oct. 30, 2019).

24. Dean Nicolls, *What Is Biometric Authentication?*, JUMIO (July 17, 2019), https://www.jumio.com/what-is-biometric-authentication/.

25. Marc Goodman, *You Can't Replace Your Fingerprints*, SLATE (Feb. 24, 2015, 10:05 AM), https://slate.com/technology/2015/02/future-crimes-excerpt-how-hackers-can-steal-fingerprints-and-more.html.

26. Danny Thakkar, *Fighting Crime and Tackling Terrorism with the Help of Biometric Technology*, BAYOMETRIC, https://www.bayometric.com/fighting-crime-with-the-help-of-biometric-technology/ (last visited Oct. 29, 2019).

27. Steve Symanovich, *Biometric Data Breach: Database Exposes Fingerprints, Facial Recognition Data of 1 Million People*, NORTONLIFELOCK, https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html (last visited Oct. 30, 2019).

28. Sayce, *supra* note 6.

silicon finger.[29] This technique is good enough to fool fingerprint scanners eighty percent of the time.[30] Even Play-Doh can be used to create fingerprint molds, which are able to trick ninety percent of fingerprint scanners.[31] Facial recognition systems, another common biometric security device, are also known to be vulnerable to cyber hacking when simply shown a photograph of an individual to unlock the individual's device.[32] Thus, when biometric information is collected and stored in a database, that information can be stolen and subsequently used for criminal activity.[33]

To fully appreciate the need for robust laws and regulations designed to prevent biometric data from falling into the wrong hands, it is important to have a basic understanding of what biometric data is and how it functions.[34] Although there is no universally accepted definition of biometrics,[35] it usually refers to either: "[m]easurable human biological and behavioral characteristics that can be used for identification," or "[t]he automated methods of recognizing or analyzing an individual based on those characteristics."[36] Simply stated, biometrics is the measurement of a person's physical being.[37] Biometric data generally refers to data that captures unique physical or behavioral characteristics as a means of verifying personal identity.[38] This data is derived from physiological and

29. *Id.*; *see also* Goodman, *supra* note 25.

30. Goodman, *supra* note 25.

31. *Id.*

32. Aside from traditional identity theft concerns, now any users of facial recognition programs must be concerned about other data weaponizations. *See* Sayce, *supra* note 6; *see also* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (Feb. 10, 2020) (discussing a groundbreaking facial recognition app, allowing a single picture taken of an individual to be matched with public photos across millions of websites, can make searching someone by face as easy as using Google to search a name: "There's always going to be a community of bad people who will misuse it[.]").

33. *See* Zimmerman, *supra* note 13, at 657.

34. *See generally Biometric Data and Data Protection Regulations (GDPR and CCPA)*, THALES, https://www.gemalto.com/govt/biometrics/biometric-data (Nov. 4, 2020).

35. Michael P. Daly et al., *Biometrics Litigation: An Evolving Landscape*, DRINKER BIDDLE & REATH LLP (Apr. 2, 2018), https://1.next.westlaw.com/w-001-8264?transitionType=Default&contextData=(sc.Default)&__lrTS=20171228100058671&firstPage=true&bhcp=1.

36. Peter A. Steinmeyer, *Expert Q&A on Biometrics in the Workplace: Recent Developments and Trends*, PRACTICAL L., https://www.ebglaw.com/content/uploads/2018/02/Sholinsky-Steinmeyer-Reuters-Expert-QA-Biometrics-February-2018.pdf (last visited Jan. 14, 2020).

37. Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. L. TODAY, May 2016, at 1.

38. *Biometrics*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/biometrics (last visited Oct. 28, 2019); *see also Biometrics*, HOMELAND SEC. (July 13, 2020), https://www.dhs.gov/biometrics.

behavioral identifiers.[39] Physiological identifiers include facial structure, retinal color and design, fingerprint readings, heat signatures, and DNA readings.[40] Behavioral identifiers include handwriting samples and signatures, voice recognition, and keyboard stroke and typing habits.[41] These identifiers allow for a person to be both authenticated, meaning to verify their identity, and identified, meaning to determine their identity.[42]

The character and value of biometric data can differ drastically from other, traditional forms of personal data. Biometric data is inherently permanent and unique to each individual, making it extremely sensitive information.[43] An individual's biometric information is exceedingly difficult to replace or change because it is unique to that person: "[I]t is very difficult, if not impossible, for any individual to disassociate oneself from one's biometric [information]."[44] Losing biometrics may not be a matter of replacement.[45] Passwords, credit cards, and even social security numbers can be replaced, but a person cannot get a new fingerprint.[46] Although choosing not to partake in biometric-facilitated transactions does not seem to be as drastic of a decision with few transactions involving the use of biometric data nowadays, biometric-facilitated transactions will one day become commonplace to consumers and retailers.[47] The personal effects of a breach could dissuade individuals from participating in such a transaction again in the future, which may lead to an overall chilling effect on the national economy.[48]

---

39. *See* Phil Ross, *Biometrics: A Developing Regulatory Landscape for a New Era of Technology*, ROBINSON & BRADSHAW (May 21, 2014), https://theprivacyreport.com/2014/05/21/biometrics-a-developing-regulatory-landscape-for-a-new-era-of-technology/.

40. *Id.*

41. *Id.*

42. *Biometrics: Definition, Trends, Use Cases, Laws and Latest News*, THALES, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (Dec. 4, 2020).

43. Benson, *supra* note 10, at 165.

44. Rigoberto Chinchilla, *Ethical and Social Consequences of Biometric Technologies*, AM. SOC'Y FOR ENG'G EDUC., 2012, at 1, 5–6.

45. *Id.* at 5.

46. Kaya Yurieff, *Why Are We Still Using Social Security Numbers as ID?*, CNN BUS. (Sept. 13, 2017, 8:40 AM), https://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html.

47. Recent studies show that mobile biometrics will "authenticate $2 trillion worth of in-store and remote mobile payment transactions annually by 2023." *See* Lynne Jeffery, *Biometrics and the Future of Payment Transactions*, BIOMETRICUPDATE.COM (Dec. 2, 2019), https://www.biometricupdate.com/201912/biometrics-and-the-future-of-payment-transactions. This not only demonstrates "a shift in consumer adoption of biometric authentication, but also rapid advancements in the technology being used to present these opportunities for biometric authenticated" transactions. *Id.*

48. Several studies indicate data security and privacy are essential in order to maintain customers: PwC reported 85% of consumers will not shop at a business if there are concerns about a business's security practices; Verizon reported that 69% of consumers would avoid a

B. Industries Implementing Biometric Data

Biometric data is used currently in a variety of different applications, and that list of uses grows longer every day.[49] From opening up your smartphone with your fingerprint or facial recognition to unlocking your car to paying for groceries, biometric data is becoming a go-to method for many everyday tasks.[50] While biometrics are still predominately used for law enforcement purposes,[51] biometric data is also being deployed across the following industries: automotive, financial services and banking, healthcare, food and beverage, hospitality, retail, and education.[52]

In the automotive industry, biometrics are increasingly developed for security and driver safety features.[53] Devices such as iris or fingerprint scanners may become the standard security feature to lock, unlock, and start a vehicle, and automotive suppliers are leveraging biometric facial recognition and retina tracking to prevent driver distraction and fatigue.[54] In the financial services and banking industry, banking fraud is becoming more widespread.[55] Banks are adopting stricter identification protocols, including opting for fingerprint biometrics, to combat fraud and increase transaction security, as biometrics can help reduce fraudulent payments.[56] Various sectors of the healthcare industry are also using

---

company that had suffered a data breach and 29% of consumers surveyed would never visit that business again. *See* WORLDPAY ED. TEAM, *How the Consequences of a Data Breach Threaten Small Businesses*, FIS (July 10, 2019), https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses.

49. Catherine R. Tucciarello, *Rapid Increase in Biometric Data in Airports Raises Privacy Concerns*, JACKSON LEWIS (Mar. 1, 2019), https://www.workplaceprivacyreport.com/2019/03/articles/consumer-privacy/rapid-increase-in-biometric-data-in-airports-raises-privacy-concerns/.

50. *9 Industries Biometrics Technology Could Transform*, CB INSIGHTS (Dec. 12, 2019), https://www.cbinsights.com/research/biometrics-transforming-industries/.

51. *Id.* Biometrics have long been used by law enforcement with the use of DNA and fingerprints for reliable types of evidence in criminal cases. *Id.* There is a growing trend of law enforcement using facial recognition for identification purposes. *Id.* For example, facial recognition plays a big part in helping law enforcement to identify victims of sex trafficking between the US-Mexico border. *Id.*

52. *Id.*

53. "Other companies are developing in-vehicle biometrics for automotive security. For example, Porsche has partnered with edge computing software developer FogHorn to develop a multi-factor authentication prototype that uses real-time facial recognition plus additional authentication via smartphone, which allows drivers to enter into their cars without key fobs." *Id.* (noting the global market for automotive biometric identification is expected to reach $303M by 2024).

54. *Id.*

55. *Id.*

56. *Id.*; *see also* Alan S. Wernick, *Biometric Information—Permanent Personally Identifiable Information Risk*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/.

measures, including facial recognition, and iris or fingerprint scanning, to advance telemedicine to make patient identification more accurate.[57] The food and beverage industries are increasingly using biometric technology to allow remote monitoring of employees and granting area access permissions, which minimizes cross-contamination.[58] In the hospitality industry, facial recognition is growing as a new way to provide better personalized services for customers.[59] Large retail companies are experimenting with biometric identification systems for payments and promotional targeting and the implementation of facial recognition to reduce theft.[60] Lastly, biometrics are applied to different aspects of education systems, including lunch programs, dorm access, security purposes, and preserving academic integrity for examinations.[61]

With each of these industries' investments in biometric data technology comes genuine security concerns.[62] Data breaches are growing more common.[63] In fact, more than half of U.S. businesses have experienced a cyberattack in the past year.[64] Just as companies must implement and update safeguards, legislatures and regulators must respond with legal efforts to protect biometric data privacy.[65]

III. CURRENT BIOMETRIC DATA PROTECTION LAWS

As the use of biometric data becomes more prevalent, a handful of legislatures across the nation have taken note.[66] Despite the popularity of biometrics and the unique issues they pose, there is no single, comprehensive federal law in the United States regulating

57. *9 Industries Biometrics Technology Could Transform*, *supra* note 50.

58. *Id.* (noting Coca-Cola uses a biometric fingerprint system to track the activity of independent truck drivers entering certain canning sites).

59. *Id.*

60. *Id.* (noting Amazon is leading the way in terms of biometric payment systems for retail and is currently testing a scanner that uses computer vision and depth geometry to identify an individual's hand as a way to ring up a store purchase).

61. *Id.* (discussing facial recognition may be used to quickly identify any unauthorized presence within school grounds).

62. *See generally* April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.

63. Joseph Cox, *Are Data Breaches Becoming More Common?*, VICE (July 28, 2016, 12:58 PM), https://www.vice.com/en_us/article/xygvgk/data-breaches-vigilante-pw.

64. According to CB Insights' Industry Analyst Consensus, the biometric technology industry is projected to be worth approximately $59 billion by 2025. *Cyber Attacks Infographic*, MUNICH RE (2017), https://www.munichre.com/HSB/cyber-risk-infographic/index.html.

65. *See* Kelly A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, 20 J. HIGH TECH. L. 229, 230 (2020).

66. *See* Wernick, *supra* note 56.

the collection and use of biometric information.[67] In the United States, four states, Illinois, Texas, Washington,[68] and California, have biometric data privacy statutes, and several others are debating enacting biometric privacy laws.[69] Additionally, the General Data Protection Regulation (GDPR), adopted by the European Union,[70] specifically addresses the protection of biometric data, representing a true international impact for data protection and privacy.[71] The increasing enactment of laws and regulations demonstrates a strong interest in protecting against threats and regulating the collection of biometric data.[72]

A. Illinois's Biometric Information Privacy Act (BIPA)

In October 2008, Illinois enacted the first state law governing the collection, use, safeguarding, and storage of biometric data known as the Illinois Biometric Information Privacy Act (BIPA).[73] BIPA was enacted in response to the bankruptcy of a startup called Pay By Touch: a biometrics firm that enabled customers to make payments by connecting their financial accounts to their fingerprints.[74] Pay By Touch's bankruptcy and dissolution left customers with no information as to what would become of the biometric data and financial information they provided.[75] This event was the catalyst for the Illinois General Assembly to enact BIPA.[76] The Illinois General Assembly further reasoned that "[t]he use of biometrics is growing in the business and security screening sectors . . . ."[77] The General Assembly also reasoned that an affected individual "has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions" when their biometrics are compromised.[78] Thus, "[t]he public welfare, security,

67. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.
68. Wernick, *supra* note 56.
69. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.
70. *See generally* Council Directive 2016/679, 2016 O.J. (L 119) 1 (EU).
71. Council Directive 2016/679, art. 4, 2016 O.J. (L 119) 1, 34 (EU).
72. Chris Burt, *Biometrics Regulations Are Coming, Firm Warns as BIPA Lawsuits Pile Up*, BIOMETRICUPDATE.COM (Sept. 6, 2019), https://www.biometricupdate.com/201909/biometrics-regulations-are-coming-firm-warns-as-bipa-lawsuits-pile-up.
73. Ryan S. Higgins et al., *Biometric Privacy Update—Actual Harm Not Required*, MCDERMOTT WILL & EMERY (Feb. 7, 2019), https://www.mwe.com/insights/biometric-privacy-update-actual-harm-not-required/.
74. Justin O. Kay, *The Illinois Biometric Information Privacy Act*, DRINKER BIDDLE & REATH LLP, https://www.acc.com/sites/default/files/2019-02/Drinker-Biddle-2017-1-BIPA-Article-2.pdf (last visited Nov. 2, 2019).
75. *Id.*
76. *Id.*
77. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/5.
78. *Id.*

and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[79]

BIPA limits the private sector's collection, use, and retention of "biometric identifiers," such as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry.[80] The law also applies to "biometric information," which is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[81] The law requires private entities to provide individuals with notice, to obtain an individual's signed written release stating informed consent before collecting their biometric data,[82] to disclose both the lawful purpose for the collection of data and the amount of time the data will be kept, and to destroy the information within a certain timeframe.[83] Furthermore, BIPA prohibits private entities from using a consumer's biometric information for profit and requires written policies concerning biometric data retention and destruction that are accessible to the public.[84]

Unlike data privacy statutes in other states, BIPA creates a private right of action against private entities that fail to satisfy BIPA's requirements with respect to the collection and use of biometric information.[85] This means that individuals, either on their own or via class actions, may seek enforcement through civil litigation claiming monetary relief.[86] BIPA also entitles a prevailing party to the following statutory damages: for each negligent violation of BIPA equal to the greater of $1,000 or actual damages, or for

79. *Id.*

80. 740 ILL. COMP. STAT. ANN. 14/10.

81. *Id.*

82. *See* Carley Daye Andrews et al., *Litigation Under Illinois Biometric Information Privacy Act Highlights Biometric Data Risks*, K&L GATES (Nov. 7, 2017), http://www.klgates.com/litigation-under-illinois-biometric-information-privacy-act-highlights-biometric-data-risks-11-07-2017/.

83. 740 ILL. COMP. STAT. ANN. 14/15.

84. *Id.* BIPA explicitly prohibits private entities from selling, leasing, trading, or "otherwise profit[ing] from" an individual's biometric data. Michael Bahar et al., *Biometrics Beware—Compliance and the Biometric Information Privacy Act*, JD SUPRA (Apr. 12, 2019), https://www.jdsupra.com/legalnews/biometrics-beware-compliance-and-the-66757/ (alteration in original). There are currently no BIPA class actions based on this provision, which raises questions regarding how courts will interpret the phrase "otherwise profit." *Id.*

85. Ronald J. Hedges & Gail L. Gottehrer, *Beyond HIPAA: Examining Data Privacy Laws at the State Level*, J. AHIMA (May 1, 2019, 12:01 AM), https://journal.ahima.org/beyond-hipaa-examining-data-privacy-laws-at-the-state-level/.

86. Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, K&L GATES (Mar. 25, 2019), http://www.klgates.com/the-biometric-bandwagon-rolls-on-biometric-legislation-proposed-across-the-united-states-03-25-2019/.

each intentional or reckless violation of BIPA the greater of $5,000 or actual damages.[87] Additionally, in January 2019, the Illinois Supreme Court held that plaintiffs need not "plead and prove that they sustained some actual injury or damage beyond infringement of the rights afforded them under the [BIPA]" in order to have a cause of action.[88] BIPA has been said to be the "the archetype . . . of biometric privacy law,"[89] and it appears to be one of the biometric data protection statutes to emulate.[90]

B. Texas's Capture or Use of Biometric Identifier (CUBI) and Washington's House Bill 1493 (H.B. 1493)

Shortly after Illinois passed BIPA, Texas enacted a biometric data protection statute in 2009.[91] The Capture or Use of Biometric Identifier Act (CUBI) is similar to BIPA in that it contains similar substantive provisions to that of BIPA, particularly regarding prohibiting private entities from collecting biometric information before giving notice and obtaining an individual's consent,[92] making profits off of the sale of biometric data, and requiring certain security and retention measures.[93] However, CUBI differs from BIPA in that it does not create a private right of action, but instead permits the Texas Attorney General to bring a civil action and provides for a penalty cap of $25,000 per violation.[94] The CUBI also defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[95]

Washington became the third state to enact a biometric privacy statute in 2017 with House Bill 1493 (H.B. 1493), which is similar to CUBI.[96] The Annotated Revised Code of Washington defines a

87. Claypoole & Stoll, *supra* note 37, at 2.

88. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019); *see also* Molly K. McGinley et al., *"No Harm, Still Foul": Actual Harm Not Required for Plaintiffs Under Illinois Biometric Privacy Act*, NAT'L L. REV. (Jan. 26, 2019), https://www.natlawreview.com/article/no-harm-still-foul-actual-harm-not-required-plaintiffs-under-illinois-biometric.

89. Jane Bambauer, *Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal*, PROGRAM ON ECON. AND PRIV., https://pep.gmu.edu/wp-content/uploads/sites/28/2017/06/Biometric-Privacy-Laws-FINAL_really_6.20-.pdf (last visited Dec. 19, 2020).

90. *See* Claypoole & Stoll, *supra* note 37.

91. *See generally* Capture or Use of Biometric Identifier, TEX. BUS. & COM. CODE ANN. § 503.001.

92. TEX. BUS. & COM. CODE ANN. § 503.001(b)–(c); *see also* Claypoole & Stoll, *supra* note 37, at 2.

93. TEX. BUS. & COM. CODE ANN. § 503.001(c).

94. *Id.* § 503.001(d).

95. *Id.* § 503.001(a).

96. *See generally* H.B. 1493, 2017 Leg., Reg. Sess. (Wash. 2017).

"biometric identifier" as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[97] H.B. 1493 broadly regulates the collection, retention, and use of "biometric identifiers," and like CUBI, permits the state's Attorney General to bring a civil action with a penalty cap of $25,000.[98]

C. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

The California Consumer Privacy Act (CCPA) of 2018 similarly provides protections for consumer data, including biometric data.[99] The CCPA recently went into effect on January 1, 2020.[100] It defines "biometric information" as "an individual's physiological, biological, or behavioral characteristics, including an individual's [DNA], that can be used, singly or in combination with each other or with identifying data, to establish individual identity."[101] The CCPA establishes a narrow private right of action for certain data breaches involving a subset of personal information, and consumers may seek actual damages or statutory damages ranging from $100 to $750 per intentional violation.[102] The act also provides a maximum penalty of $7,500 for intentional violations, while other violations lacking intent remain subject to a preset fine of $2,500.[103] One hotly contested part of the CCPA is its "notice and cure" provision, which provides an avenue for a company to avoid individual statutory damages if a company cures its violations within thirty days.[104] This provision ultimately compels a company to implement and maintain reasonable security procedures and practices.[105]

---

97. WASH. REV. CODE ANN. § 19.375.010.
98. *Id.* § 19.86.140.
99. *See generally* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.
100. *Id.*
101. *See id.* § 1798.140(b) (stating "[b]iometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that can contain identifying information.").
102. *Id.* § 1798.150; *see also* Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKERHOSTETLER LLP, https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf (last visited Nov. 1, 2019).
103. CAL. CIV. CODE § 1798.155.
104. *Id.* § 1798.150(b).
105. *Id.*

Most notably, the CCPA empowers California consumers with fundamental privacy rights to control their own personal information,[106] providing many similar protections as the European Union's GDPR.[107] The CCPA follows in the footsteps of the GDPR by allowing individuals to have greater control over their personal data.[108] The CCPA offers California consumers new statutory rights, including the Consumer Right to Delete, Consumer Opt-Out from Sale of Personal Information, Consumer Opt-In for the Sale of Personal Information of Minors, and Non-Discrimination for Exercise of Consumer Rights.[109] These provisions in the CCPA afford consumers with individual rights to learn what personal information covered businesses have collected, sold and disclosed, opportunities to opt-out of the sale of their personal information, and the unique protection from discrimination in the form of reduced service or functionality for exercising those rights.[110] With strong similarities to the GDPR, the CCPA is frequently presented as a model for future legal framework of U.S. data privacy law.[111]

Although the CCPA currently provides comprehensive data protections for its citizens, recent events demonstrate that privacy regulation in the state of California will not stop with the CCPA.[112] On November 3, 2020, Californians voted to approve a ballot initiative known as Proposition 24, which enacted the California Privacy Rights Act (CPRA).[113] Taking effect on January 1, 2023, the CPRA

106. *See* Xavier Becerra, *California Consumer Privacy Act (CCPA)*, CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa (last visited Dec. 19, 2020).

107. CAL. CIV. CODE §§ 1798.100–1798.199. The CCPA provides the following rights to consumers: to know all data collected on a consumer by a business, twice a year, free of charge; to say no to the sale of a consumer's information; to delete the data posted; to sue companies who collect their data, where that data was stolen or disclosed pursuant to an unauthorized data breach, if the company was careless or negligent about how it protected one's data; not to be discriminated against for telling a company not to sell one's personal information; to be informed of what categories of data will be collected about one prior to its collection or at point of collection, and of any charges made to this collection; mandated opt-in before sale of children's information; to know the categories of third parties with whom your data is shared; to know the business or commercial purpose of collecting one's information. *See infra* Section III.D.

108. Palmer, *supra* note 5.

109. John Stephens, *California Consumer Privacy Act*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

110. *Id.*

111. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.

112. Cynthia Cole et al., *Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now*, BLOOMBERG L. (Nov. 16, 2020, 4:00 AM), https://news.bloomberglaw.com/privacy-and-data-security/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now.

113. The California Privacy Rights Act of 2020, Cal. Proposition 24 (2020), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

is not intended to replace the CCPA; rather, the CPRA incorporates the CCPA and includes a number of amendments and modifications to the CCPA.[114] The CPRA amends and expands upon the CCPA by creating additional consumer rights, modifying existing CCPA rights, establishing a new privacy enforcement agency, and mandating a new subcategory of consumer personal information known as "sensitive personal information."[115] Biometric data is included as an identifier that qualifies as sensitive personal information.[116] While the CCPA implicitly includes the regulation of sensitive personal information in broader terms, the CPRA imposes distinct requirements and restrictions on regulating sensitive personal information, including disclosure requirements, opt-out requirements for use and disclosure, opt-in consent standard for use and disclosure, and purpose limitation requirements.[117] Ultimately, the enactment of the CPRA represents a significant shift in the U.S. privacy landscape and will likely energize efforts to pass other data privacy acts throughout the nation.[118]

D. General Data Protection Regulation (GDPR)

Aside from the biometric data protection laws in the United States, the General Data Protection Regulation serves as an exemplary international standard for data protection.[119] The GDPR was passed in April of 2016 and went into effect on May 25, 2018.[120] Not only does the GDPR apply to organizations located within the European Union, but it also applies to all companies, anywhere in the world, processing and holding the personal data of those that reside in the European Union.[121] It defines "biometric data" as "personal data resulting from specific technical processing relating to the physical, physiological or [behavioral] characteristics of a natural person, which allow or confirm the unique identification of that

114. Matthew A. Diaz & Kurt R. Hunt, *California Approves the CPRA, a Major Shift in U.S. Privacy Regulation*, NAT'L L. REV. (Nov. 17, 2020), https://www.natlawreview.com/article/california-approves-cpra-major-shift-us-privacy-regulation.

115. Cole et al., *supra* note 112.

116. *Id.*

117. Brandon P. Reilly & Scott T. Lashway, *The California Privacy Rights Act Has Passed: What's in It?*, MANATT (Nov. 11, 2020), https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed.

118. Diaz & Hunt, *supra* note 114.

119. *See generally* Laurent Barthelemy, *One Year on, EU's GDPR Sets Global Standard for Data Protection*, PHYS.ORG (May 24, 2019), https://phys.org/news/2019-05-year-eu-gdpr-global-standard.html.

120. Palmer, *supra* note 5.

121. Ben Wolford, *Does the GDPR Apply to Companies Outside of the EU?*, GDPR.EU, https://gdpr.eu/companies-outside-of-europe/ (last visited Feb. 16, 2020).

natural person, such as facial images or dactyloscopic [fingerprint] data."[122] The GDPR also establishes a private right of action for material or non-material damages caused by a data controller or data processors breach.[123] Material damage involves actual damage that is quantifiable, while non-material damage involves any damage that is not financial, such as pain and suffering.[124] The GDPR imposes penalties of up to four percent of an organization's annual global turnover, or a company's total revenues,[125] or twenty million euros, whichever is greater.[126]

Most notably, the GDPR affords the following rights to its citizens: right to breach notification; right to access; right to be forgotten; right to data portability; right to know whether or not personal data is being processed, where, and for what purpose; a free copy of personal data in electronic format; the right to have the data controller erase his or her data, cease further dissemination of the data, and potentially have third parties halt processing of the data; the right to obtain personal data in a commonly used and machine readable format; and the right to transfer that data to another controller.[127]

Not only has the GDPR enhanced data protection for citizens in the European Union, but it has become globally influential, being referred to as the new "gold-standard" for the protection of data worldwide.[128] At its core, the GDPR is designed to give citizens of the European Union more control over their personal data.[129] Countries and regions around the world appear to be taking cues from

122. *See* Council Directive 2016/679, *supra* note 70, at art. 4.

123. *Id.* at art. 82.

124. Deirdre Kilroy, *Data Protection Litigation—An Irish Perspective*, MATHESON (Sept. 12, 2018), https://www.matheson.com/news-and-insights/article/data-protection-litigation-an-irish-perspective.

125. Adam Hayes, *Overall Turnover*, INVESTOPEDIA (July 2, 2019), https://www.investopedia.com/terms/o/overall-turnover.asp.

126. *See generally* Council Directive 2016/679, *supra* note 70, at art. 12–23.

127. *See generally id.*

128. Maeva Kpadonou, *With the GDPR, Europe Shows the World the Way*, LEADERS LEAGUE (Nov. 4, 2019), https://www.leadersleague.com/en/news/with-the-gdpr-europe-shows-the-world-the-way.

129. Some scholars argue this European value of privacy is largely due to Europe's past experiences, particularly with the Nazis in the twentieth century, with fascism and communism. *See* David Meyer, *Opinion: How Europe Is Better at Protecting Data than the U.S.—and What the Stasi and Nazis Have to Do with It*, MKT. WATCH (Mar. 21, 2018, 1:34 PM), https://www.marketwatch.com/story/why-europe-does-a-better-job-of-protecting-online-privacy-than-the-us-does-2018-03-20; *see also* Jeffrey Toobin, *The Solace of Oblivion: In Europe, the Right to Be Forgotten Trumps the Internet*, NEW YORKER (Sept. 22, 2014), https://www.newyorker.com/magazine/2014/09/29/solace-oblivion. *But see* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004) (stating scholars have alternatively theorized that European Union views privacy as an aspect of dignity based on ancient European practices for defending reputation).

the GDPR by introducing or modifying data protection legislation, as demonstrated with the enactment of the CCPA.[130] The GDPR is an exemplary demonstration of the importance of building a foundation of trust in a digital future, thus ensuring citizens that they are in control of their personal information, and their information is always protected.[131]

IV. ANALYSIS: IMPLEMENTING BIOMETRIC DATA PROTECTIONS IN PENNSYLVANIA

A. State Legislation over Federal Legislation

Although scholars argue that enacting federal legislation would be a more appropriate solution to solve biometric privacy concerns, biometric data legislation will likely be more successful at the state level.[132] Companies conducting business across multiple states allege that compliance with biometric data protections would be easier if there was one uniform standard to follow.[133] However, there are issues regarding the lengthy deliberation process of creating federal legislation.[134] Congress passes far fewer bills, both as a percentage of those introduced and as a raw number, than state legislatures.[135] Legislation moves faster and is passed with greater frequency at the state level.[136] State legislatures pass about a quarter of the bills that are offered.[137] This allows for states to act as "laboratories of democracy," serving as proper testing grounds for biometric data protection laws and ultimately influencing an appropriate federal law protecting citizens' biometric data nationwide.[138]

---

130. Whitman, *supra* note 129; Meyer, *supra* note 129; Toobin, *supra* note 129.

131. Whitman, *supra* note 129; Meyer, *supra* note 129; Toobin, *supra* note 129.

132. *See generally* Daniel C. Vock, *State Labs: Congress Can Learn a Lot from State Legislatures*, GOVERNING (Sept. 2019), https://www.governing.com/topics/politics/gov-state-labs.html.

133. Fiona Q. Nguyen, Article, *The Standard for Biometric Data Protection*, 7 J.L. & CYBER WARFARE 61, 71 (2018).

134. Vock, *supra* note 132 (noting that during the last Congress, members introduced nearly 11,200 bills over two years, and only 416 of them became law, and even including those, less than four percent of bills introduced became law).

135. *Id.*

136. *State Legislatures vs. Congress: Which Is More Productive?*, QUORUM, https://www.quorum.us/data-driven-insights/state-legislatures-versus-congress-which-is-more-productive/176/ (last visited Nov. 2, 2019) ("[S]tate legislatures introduce [twenty-three] times more bills than Congress does, totaling an average 128,145 bills per year and 3.1 million words per day in session.").

137. Vock, *supra* note 132.

138. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("[A] single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

Rather than facing a Congressional gridlock and continue to delay the enactment of an ideal uniform federal standard, enacting biometric data protections through state legislation is the best option for quickly and efficiently regulating this information.[139] As technology continues to develop, consumers' privacy interests continue to be urgent and outweigh the arguments against biometric legislation, and waiting for Congress to draft the perfect uniform federal biometric data protection law.[140] Protections for Pennsylvania citizens' biometric information could be implemented more quickly and efficiently if the Pennsylvania legislature enacted its own statute.[141]

B. Why Pennsylvania?

As more states propose and enact legislation protecting the collection, retention, and use of biometric data,[142] Pennsylvania must consider these proposals and enactments and its own biometric privacy law to encourage similar standards of compliance for the protection of its own citizens, consumers, and companies.[143] There is currently no statute that specifically protects citizens' biometric data in Pennsylvania, and Pennsylvania's data breach notification law also does not contain "biometric information" under its protected "personal information."[144] Although it would improve biometric data privacy protections to an extent, it is not enough for Pennsylvania to simply amend its data security breach notification laws to include "biometric data" as a type of "personal information."[145] A comprehensive statute will provide Pennsylvania consumers more protection because, like the other biometric data protection statutes in place, it will recognize that biometric information is distinct from other types of personal information and

139. *See generally State Legislatures vs. Congress*, *supra* note 136.

140. *See* Carra Pope, Note and Comment, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 799 (2018).

141. *See generally State Legislatures vs. Congress*, *supra* note 136.

142. *See* McGinley, *supra* note 86 (Arizona, Florida, and Massachusetts are the latest states to propose legislation addressing biometric information protections).

143. *See generally* Nguyen, *supra* note 133.

144. *See* Breach of Personal Information Notification Act, 73 PA. STAT. AND CONS. STAT. ANN. § 2302 (defining "personal information" as "(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number; (ii) Driver's license number or a State identification card number issued in lieu of a driver's license; (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.").

145. *See generally id.*

acknowledge that the potential harms are not limited to data security breaches.[146]

There are several features specific to the state of Pennsylvania which make enacting state legislation the best choice for furthering biometric data protections. One of the most significant factors to consider for enacting a statute for biometric data protection is Pennsylvania's economy.[147] With two major metropolitan areas facilitating a tremendous amount of business throughout the state, Pennsylvania has the sixth largest economy in the United States by GDP.[148] If Pennsylvania does not protect these consumers, Pennsylvania puts its consumers at a greater risk as biometric data becomes increasingly relevant in various industries.[149] Furthermore, if Pennsylvania does not provide guidelines for companies to protect consumers' biometric data, it would ultimately fail its citizens by not protecting their biometric data.[150] Legislators all across the nation are making data privacy a top priority, resulting in a domino effect as the number of laws proposed for proactive and reactive data security measures are spiking.[151] If Pennsylvania neglects to pass this legislation, it would disturb this domino effect and would not influence other states to implement similar protections.[152] This ultimately discourages the expansion of biometric data protection laws throughout the nation.[153] Thus, it is logical for the Pennsylvania General Assembly to implement a statute to establish a sense of trust in consumers that their sensitive data will be protected, which allows consumers to feel more comfortable turning their data over, and in turn, allows for a more prosperous economy.[154]

---

146. Zimmerman, *supra* note 13, at 648.

147. *See Gross Domestic Product by State, 2nd Quarter 2020*, BUREAU OF ECON. ANALYSIS, (Oct. 2, 2020, 8:30 AM), https://www.bea.gov/sites/default/files/2020-10/qgdpstate1020_0.pdf.

148. *Id.*

149. *See infra* Section IV.B.

150. *See* NAT'L RSCH. COUNCIL, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 85 (Joseph N. Pato & Lynette I. Millett eds., 2010).

151. *See* Mark S. Goldstein et al., *The Sword Behind the SHIELD: Implications of New York's Expanded Data Security Law for Employers and the Broader Biometric Landscape*, REED SMITH (Oct. 23, 2019), https://www.reedsmith.com/en/perspectives/2019/10/the-sword-behind-the-shield.

152. The CCPA's impact on privacy regulation across the United States is discussed as starting a new wave of privacy focused standards in the U.S. *See generally* Lindsey O'Donnell, *California's Domino Effect on U.S. Privacy Regulation*, THREATPOST (Nov. 14, 2019, 10:32 AM), https://threatpost.com/ccpas-domino-effect-us-privacy-regulation/150246/.

153. *See* Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

154. *See generally* Sam Saltis, *GDPR Fines: Everything You Need to Know*, CORE DNA (Nov. 5, 2020), https://www.coredna.com/blogs/gdpr-fines.

Additionally, Pennsylvania's Constitution demonstrates strong values placed on individual privacy rights and consumer protection.[155] The Pennsylvania Supreme Court has interpreted both Article 1, Section 1 and Article 1, Section 8 of the Pennsylvania Constitution as being tied to the implicit right to privacy in the Commonwealth of Pennsylvania.[156] In fact, the Commonwealth of Pennsylvania has long embodied a commitment to the protection of individual privacy.[157] Pennsylvania courts have regularly stated that Pennsylvania's right to privacy encompasses freedom from disclosure of personal information.[158] With these privacy interests embedded in the provisions of the Pennsylvania Constitution, the enactment of a statute protecting biometric data privacy would align properly with interests that the Commonwealth of Pennsylvania seeks to continuously protect.[159]

C. Affording Privacy Rights

In order to fully protect its citizens' biometric information, the Pennsylvania legislature must consider affording statutory rights to consumers in its biometric privacy provisions.[160] The inclusion of statutory rights with biometric data protections is demonstrated in the GDPR, BIPA, and CCPA.[161] The rights afforded under these provisions must be considered in the drafting of Pennsylvania's biometric data protection statute: right to breach notification; right to access; right to be forgotten; right to data portability; right to know whether or not personal data is being processed, where, and for what purpose; the right to have the data controller erase his or her data, cease further dissemination of the data, and potentially have third parties halt processing of the data; the right to obtain

155. PA. CONST. art. I, § 1, 8.

156. *See, e.g.*, Commonwealth v. Murray, 223 A.2d 102, 109–10 (Pa. 1966) (Musmanno, J.) (plurality opinion) (stating that the right to privacy is rooted in the Article I, Section I protection of "inherent and indefeasible rights" and in Article I, Section 8); *see* Pa. State Educ. Ass'n v. Commonwealth, 148 A.3d 142, 151 (Pa. 2016); Commonwealth v. Russo, 934 A.2d 1199, 1200 (Pa. 2007); Commonwealth v. Edmunds, 586 A.2d 887, 901 (Pa. 1991).

157. Seth F. Kreimer, *The Right to Privacy in the Pennsylvania Constitution*, 3 WIDENER J. PUB. L. 77, 82 (1993).

158. *Id.* at 102; *see* Denoncourt v. Pennsylvania State Ethics Comm'n, 470 A.2d 945, 948 (Pa. 1983); *see also In re* June 1979 Allegheny Cnty. Investigating Grand Jury, 415 A.2d 73, 77 (Pa. 1980); Fischer v. Commonwealth, Dep't of Pub. Welfare, 482 A.2d 1148, 1159 (Pa. Commw. Ct. 1984) (en banc).

159. *See generally Denoncourt*, 470 A.2d at 948. *See also In re June 1979 Allegheny Cnty. Investigating Grand Jury*, 415 A.2d at 77; *Fischer*, 482 A.2d at 1159.

160. *See generally* CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; Council Directive 2016/679, *supra* note 70, at art. 12–23.

161. CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; Council Directive 2016/679, *supra* note 70, at art. 12–23.

personal data in a common use and machine readable format; and the right to transfer that data to another controller.[162]

Each of the rights afforded under these biometric data privacy laws highlight different protections and needs.[163] The right to be informed, or the right to know whether or not data is being processed, highlights the need for transparency from companies regarding how these companies process an individual's data.[164] The right to be forgotten, or the right to erasure, gives individuals the right to demand that their data be removed or deleted from a database, which obligates companies to erase all data about the individual, unless it must be stored for a legal purpose.[165] The right to restrict processing, or to have third parties halt processing of the data, gives individuals the rights to block or suppress the processing of personal data.[166] The right to data portability ensures that individuals can reuse their personal data for their own purposes across different services.[167] Considering what each of these rights provide for individuals, incorporating statutory rights in Pennsylvania's biometric data protection statute would allow consumers to have control over the collection, aggregation, and retention of their biometric data and shift the burden over to companies to justify their use of and protection of this data.[168]

D. Defining "Biometric Data"

When drafting a biometric data protection statute, the Pennsylvania legislature must construct a definition of "biometric data" that fully protects each aspect of its consumers' biometric information and that makes it simple for other out-of-state companies to abide by.[169] Defining "biometric data" too narrowly would likely fail to encompass certain classifications of biometric data that should rightfully be protected.[170] The legislature must consider a

162. Council Directive 2016/679, *supra* note 70, at art. 12–23.

163. *See generally Consumer Rights and GDPR*, LEADDESK, https://leaddesk.com/gdpr-consumer-rights-2/ (last visited Dec. 19, 2020).

164. *Id.*

165. *Id.*

166. *Id.* Under the GDPR, processing covers a range of operations performed on data, including "the collection, recording, [organization], structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data." *What Constitutes Data Processing?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en (last visited Feb. 14, 2020).

167. *Consumer Rights and GDPR*, *supra* note 163.

168. *See generally id.*

169. *See* Zimmerman, *supra* note 13, at 666.

170. *Id.*

definition for "biometric data" that not only encapsulates as many biological characteristics as possible, but one that also is in line with technological changes in order for the law to keep up with ever-advancing technologies.[171] However, the legislature should consider balancing this broad definition by including a provision to prevent the conversion of biometric data into other formats, similar to the provision included in BIPA: "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[172] This provision will prevent organizations from circumventing the law and converting biometric identifiers into other formats.[173]

Both the GDPR and the CCPA's definitions of "biometric data" and "biometric information," respectively, allow for all potential forms of biometric information to be protected.[174] The GPDR's inclusion of "physical, physiological, and behavioral characteristics" as biometric identifiers appears to be an implicit acknowledgement that biometric technology is relatively nascent and will continue to evolve beyond our current understanding.[175] The CCPA's definition of "biometric information" extends to unique biological characteristics and the data generated by measuring them.[176] The CCPA's definition includes elements of the GDPR's definition of special categories of data, but it broadly incorporates the idea that biometric data "can be used, singly or in combination with each other or with other identifying data, to establish individual identity."[177] With both the GDPR and CCPA's inclusive definitions serving as model laws, the Pennsylvania legislature should also set out a broad definition of "biometric data," using a technology-neutral definition focusing on the *type* of data that is collected by biometric technologies, ultimately allowing the statute to provide a flexible standard that can be applied to new and evolving technologies in the future.[178]

---

171. *Id.*
172. 740 ILL. COMP. STAT. ANN. 14/10.
173. QUINN EMANUEL URQUHART & SULLIVAN, LLP, *June 2019: The Rise of Biometric Laws and Litigation*, JD SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/june-2019-the-rise-of-biometrics-laws-82168/.
174. *See* CAL. CIV. CODE §§ 1798.100–1798.199; Council Directive 2016/679, *supra* note 70, at art. 4.
175. Danny Ross, *Processing Biometric Data? Be Careful, Under the GDPR*, INT'L ASS'N OF PRIV. PROF'LS (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/.
176. *See* Jonathan (Yoni) Schenker & Craig A. Newman, *Part I: A Closer Look at California's New Privacy Regime: The Definition of "Personal Information,"* PATTERSON BELKNAP (Apr. 9, 2019), https://www.pbwt.com/data-security-law-blog/part-i-a-closer-look-at-californias-new-privacy-regime-the-definition-of-personal-information.
177. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.
178. Zimmerman, *supra* note 13, at 668.

E. Private Right of Action

Like the GDPR, BIPA, and CCPA, Pennsylvania must offer a mechanism by which parties in violation of the law can be held accountable.[179] The most direct approach to offer effective recourse is for Pennsylvania to include a private right of action in its biometric data protection statute.[180] Offering a private right of action will allow Pennsylvania citizens to enforce protections of their rights and get equal consideration for their claims without relying on the Attorney General.[181] Attorney General offices have limited time and resources to pursue every claim, and cases involving delicate biometric information should not be selectively pursued.[182] Although some scholars argue that adding a private right of action creates a flood of litigation, a clear and comprehensive law balancing privacy and business interests will minimize litigation, and it is a small price to pay for strong protections of Pennsylvanian's biometric information.[183] Creating a private right of action would ultimately provide data breach victims with a right to hold violators accountable.[184]

On the contrary, a statute that does not provide a private right of action for a biometric data breach increases the risks involved in privately suing a compromised entity, leaving the injured party to rely on legal theories independent of specific laws.[185] BIPA's inclusion of a private right of action is one of the most imperative aspects of the statute, as it was created in the aftermath of a private entity dissolving, leaving questions for consumers about what would become of their sensitive biometric data.[186] With biometric authentication technology being used more often by the average adult today, many Americans believe they have lost control of their data and are unsure how to get it back under their control.[187] This is not entirely surprising considering how few data breach victims are able to

179. *See generally* CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; Council Directive 2016/679, *supra* note 70, at art. 82.

180. Michael A. Rivera, Note, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 571, 595 (2019).

181. Benson, *supra* note 10, at 191.

182. *Id.*

183. *Id.*

184. Rivera, *supra* note 180, at 595.

185. *Id.* at 582–83.

186. *See* Kay, *supra* note 74.

187. *See* Mary Louise Kelly, *Most Americans Feel They've Lost Control of Their Online Data*, NPR (Apr. 10, 2018, 7:02 PM), https://www.npr.org/2018/04/10/601148172/most-americans-feel-theyve-lost-control-control-of-their-online-data.

successfully hold private entities legally accountable for failure to protect this sensitive biometric data.[188]

A private right of action also provides a mechanism in which harmed consumers can avoid the class certification challenges present in data breach class action suits.[189] "The private right [of action] can also provide an alternate means to bring suit against private entities with forced arbitration clauses [which] specifically prohibit class action suits."[190] Other jurisdictions have offered a private right of action, demonstrating that it is a workable option for legal recourse.[191] For example, there is little to suggest that Illinois suits brought through this private right of action offered in BIPA have become unduly burdensome on Illinois businesses or courts.[192] A private right of action is an element that ultimately prioritizes the safety of consumer biometric data and empowers consumers to hold private entities accountable.[193] Therefore, a private right of action should be incorporated in Pennsylvania's biometric data protection statute in order to provide proper remedies for its citizens who have been harmed by violators.[194]

F. Penalties for Statutory Violations

Independent of this private right of action, Pennsylvania should consider imposing monetary civil penalties for when its biometric data protection statute is violated.[195] Imposing high penalties like the GDPR—up to four percent of an organization's annual global turnover or twenty million euros, whichever is greater—will deter violation of the statute.[196] Businesses argue the fines outlined under the GDPR are unreasonably high and could extinguish companies' operations if there were a data breach or violation of the standard.[197] However, with over half of businesses experiencing cyberattacks in the United States, legislatures must implement higher standards of protection to combat cyber hackers and reduce the

188. Rivera, *supra* note 180, at 598.
189. *Id.*
190. *Id.*
191. *Id.* at 599.
192. *Id.*
193. *Id.* at 610.
194. *See* Benson, *supra* note 10, at 166.
195. *See generally* CAL. CIV. CODE §§ 1798.150–1798.155; 740 ILL. COMP. STAT. ANN. 14/20; TEX. BUS. & COM. CODE ANN. § 503.001(d); WASH. REV. CODE ANN. § 19.86.140; Council Directive 2016/679, *supra* note 70, at art 83.
196. Nguyen, *supra* note 133, at 81.
197. *See If the Data Breach Doesn't Kill Your Business, the Fine Might*, TRIPWIRE (Apr. 1, 2019), https://www.tripwire.com/state-of-security/security-data-protection/data-breach-fine/.

amount of cyberattacks.[198] Higher penalties can motivate data collectors and companies to invest in increased security measures, which will save companies from the damage of fines, lawsuits, and damage to their reputations.[199] If companies are held to higher standards, this encourages greater compliance with biometric data protection standards and overall security of consumers' sensitive biometric data.[200] Pennsylvania must impose penalties under its biometric data protection statute in order to effectively protect both themselves and their customers.[201]

To ensure that businesses are not financially extinguished by penalties, Pennsylvania can consider implementing a "notice and cure" provision for noticed violations.[202] Under its "notice and cure" provision, the CCPA grants businesses a thirty-day cure period, in the event that a cure is possible, to avoid statutory damages or class-wide damages.[203] A private plaintiff, one who is affected by an unauthorized disclosure or theft of personal information, must provide a business written notice within thirty days identifying the specific provisions of this title and the consumer alleges have been or are being violated prior to filing their lawsuit.[204] The notion of cure is not defined in the CCPA, but it has the flexibility to be interpreted narrowly, meaning a specific incident is cured to the extent possible at the time the business receives notice of the violation, or broadly, meaning the business's reasonable security procedures and practices must be remedied as a whole.[205] While the notice and cure provision will not affect lawsuits for actual damages, it provides an avenue for companies to continue operating and to cure issues relating to data incidents, as well as helping to ensure consumers that companies are compelled to keep security procedures and practices effective and up to date.[206]

Although the CCPA's "notice and cure" provision provides measures to protect both businesses and consumers when violations occur, it also raises many questions as to what constitutes a proper

198. *Cyber Attacks Infographic*, *supra* note 64.
199. Saltis, *supra* note 154.
200. *See* Nguyen, *supra* note 133, at 81.
201. *See* Saltis, *supra* note 154.
202. *See generally* CAL. CIV. CODE § 1798.150.
203. *Id.*
204. James M. Perez & Sheri Porath Rockwell, *Navigating the CCPA's 'Notice and Cure' Provision*, BLOOMBERG L., https://www.sidley.com/-/media/publications/bloomberg-law_navigating-the-ccpas-notice-and-cure-provision.pdf (last visited Jan. 18, 2020).
205. COOLEY LLP, *United States: CCPA FAQs Part 3: Litigation, Regulatory Actions and Liability*, MONDAQ (Oct. 7, 2019), http://www.mondaq.com/unitedstates/x/851552/Data+Protection+Privacy/CCPA+FAQs+Part+3+Litigation+Regulatory+Actions+and+Liability.
206. *See generally* Perez & Rockwell, *supra* note 204.

"cure."[207] The Pennsylvania legislature must draft this provision with clearer standards on what companies must do to cure purported violations.[208] A clearer definition for a "cure" should make clear that the cure must relate to the company's violation of its duty to maintain and provide reasonable security procedures and practices.[209] This would not only avoid confusion in the courts, but it would also allow businesses to consider possible responses in cases of violations and ways to further enhance biometric data security practices, as these decisions must be made quickly within a thirty-day time frame.[210] To ensure the explanation of an appropriate "cure" is not too narrow, the Pennsylvania legislature should consider including that the appropriate "cure" should be informed by the circumstances of each breach and the affected company's existing security program.[211] Incorporating a "notice and cure" provision into its statute is a way the Pennsylvania legislature can balance the protection of consumers' biometric data security and also provide businesses an avenue of relief, while ultimately ensuring the continuous enhancement of reasonable security practices.[212]

V. CONCLUSION

Biometric data technology will become ubiquitous, with its applications increasing across a variety of fields.[213] With these innovative uses of biometrics comes the potential for serious consequences involving cyber hacking and data breaches,[214] sometimes leaving victims of these breaches without proper recourse. It is not only important for individuals, companies, and other entities to keep up with their own reasonable security and compliance measures, but state legislatures must also take on the responsibility of creating biometric data protections for consumers and provide companies with effective guidelines on how to safeguard this sensitive data.

To ensure proper protections of its consumers' biometric data, it is essential for the Pennsylvania legislature to take action and enact state legislation for the protections and benefits of both consumers and companies. The privacy interests of Pennsylvania citizens

---

207. *See* COOLEY LLP, *supra* note 205.
208. *See* Perez & Rockwell, *supra* note 204.
209. *See generally id.*
210. *Id.*
211. *Id.*
212. *Id.*
213. *See* Craig Oliver, *Technology at a Price: Risks with Using Biometric Scanning in the Workplace*, BRADLEY (Feb. 27, 2019), https://www.bradley.com/insights/publications/2019/02/technology-at-a-price-risks-with-using-biometric-scanning-in-the-workplace.
214. Thakkar, *supra* note 26.

outweigh waiting to enact one uniform federal standard, and it may only be a matter of time before a catastrophic data breach occurs leaving victims without proper protections and recourse. Failing to create legislation protecting rights for consumers' biometric data protection with the Pennsylvania Constitution's strong values of privacy would be ignoring these fundamental principles embedded in the Pennsylvania legal system.[215] Pennsylvania has the potential to construct a statute that may serve as a model of its own to the rest of the nation and inspire trust and uniformity in the realm of biometric data protection. Thus, Pennsylvania must seize this opportunity to protect its citizens' biometric data, and it must do so before this data is compromised.

215. *See* PA. CONST. art. I, § 1, 8.

Too Big to Protect: A Dodd-Frank Framework for Protecting 21st Century American Consumer Privacy Rights

Stanley A. Marciniak III[*]

* J.D. Candidate, Duquesne University School of Law, 2021; B.S.B.A., Robert Morris University, 2018. The author extends his heartfelt thanks to Professor Agnieszka McPeak for providing her invaluable suggestions and guidance, as well as to Professor John Rago for inspiring his passion for protecting privacy.

INTRODUCTION

In seemingly every area of one's daily economic interactions, consumers are protected by comprehensive legal frameworks—the Food and Drug Administration (FDA) ensures safe food and drugs are available in grocery stores, the National Highway Traffic Safety Administration (NHTSA) ensures cars have safe designs, the Federal Aviation Administration (FAA) ensures safe airline travel, and the Occupational Safety and Health Administration (OSHA) safeguards workplace conditions.[1] However, when consumers download an app, make an online purchase, or sign-up for a new digital service, it becomes difficult to point to a single comprehensive legal framework that protects consumer privacy in the United States. That is the focus of this article. American privacy law desperately needs wholesale reform to serve the needs of the twenty-first century consumer.

Part I of this article discusses the nature of the present consumer privacy crisis in American industry, examining recent data breaches, the privacy void consumers face, and the current lack of sufficient regulatory enforcement mechanisms.[2] Part II briefly explores the 2008 financial collapse, the origins of which contain numerous parallels to the present privacy crisis.[3] It primarily discusses the reform efforts following the financial crisis—namely the Dodd-Frank Act. Part III analogizes the 2008 financial crisis to the 2020 privacy crisis, highlighting the "Wild West" regulatory environment leading to each crisis, the development of economic bubbles, and tenuous corporate practices.[4] Finally, Part IV proposes a Dodd-Frank approach to comprehensive American consumer privacy legislation to respond to the current privacy crisis—articulating a "Data Fiduciary Rule," the creation of a Consumer Data Protection Bureau, and the promulgation of a Volcker rule for corporate data practices.[5]

---

1. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 89 (2018).
2. *See infra* Part I.
3. *See infra* Part II.
4. *See infra* Part III.
5. *See infra* Part IV.

I. BACKGROUND: PRIVATE INDUSTRY'S PRIVACY CRISIS

In an interview with ABC News, Apple CEO Tim Cook stated that privacy in itself "has become a crisis."[6] The American public broadly shares Cook's sentiment. According to a March 2019 Axios poll, fifty-eight percent of American consumers believe the threat to online privacy is a crisis.[7] In the interview, Cook discussed the expansive amount of personal information available online, noting that "[t]he people who track on the internet know a lot more about you than if somebody's looking in your window . . . ."[8] Though privacy is a crisis, Cook believes it is a crisis that can be addressed—suggesting it is a problem solvable by united action.[9]

In 2013, the Organization for Economic Cooperation and Development (OECD) estimated that in developed nations, an average family of four had ten internet-connected devices in their home.[10] It is not hard to imagine, in the near future, devices that will produce data concerning one's diet, if they are home, and even whether they are having intimate relations.[11] This prospect becomes all the more disturbing when it is likely that these devices will be sharing information with corporate third-party entities. The number of internet-enabled devices—not just tablets and phones, but also things like smart refrigerators—has grown from 12.5 billion to 26.7 billion over the past decade.[12] Ben Zhao, a professor of computer science at the University of Chicago who studies security, privacy, and artificial intelligence,[13] notes that the firms manufacturing smart devices are often so small that "'there is no hope of ensuring that they're responsive' to privacy concerns . . . ."[14] There is no pressure for such firms to protect privacy as they have no public reputation, like industry giants such as Facebook.[15] More firms are now collecting, and possibly losing or abusing, individuals' data than ever

---

6. Lisa Eadicicco, *Apple CEO Tim Cook Says Digital Privacy 'Has Become a Crisis*,' BUS. INSIDER (May 4, 2019, 6:03 PM), https://www.businessinsider.com/apple-ceo-tim-cook-privacy-crisis-2019-5.

7. Kim Hart, *A Growing Majority Now Views Our Online Privacy as a Crisis*, AXIOS (Mar. 9, 2019), https://www.axios.com/a-growing-majority-now-views-our-online-privacy-as-a-crisis-1552080369-94146f05-332d-465d-a136-4414f9cdf9ce.html4.

8. Eadicicco, *supra* note 6.

9. *Id.*

10. HARTZOG, *supra* note 1, at 261.

11. *Id.* at 263–64.

12. Susie Allen, *The New Panopticon: Worried About Online Privacy? Computer Science Experts Worry Too*, U. OF CHI. MAG., Spring 2019, at 12.

13. *Id.*

14. *Id.*

15. *Id.*

before.[16] As an example of how ubiquitous the issue of data mining has become:

> [i]magine a seemingly innocuous retail app asking for permission to access your phone's built-in microphone. Without thinking much about it, you hit "allow." The simple tap of a button allows the app to listen for inaudible, high-pitched beacons emitted from its partner websites in addition to advertisements and storefronts. That means the company can know where you've been and what ads you've seen, online and offline.[17]

In short, "the company that makes your toaster knows you're a lefty who drives a Honda."[18] The fact that a growing number of the objects surrounding us are becoming internet-connected is a "prominent concern" for privacy.[19] More internet devices create a greater potential for data leaks, surveillance, and security vulnerabilities.[20]

Many regard privacy as a human right.[21] In many countries, the right to privacy is not explicitly protected, particularly on the internet.[22] Over the last three decades, there has been an aggressive erosion of privacy.[23] Most things on the internet appear to be "free."[24] But, they are not free. The public pays for them in other ways—via data and attention.[25] This is the price paid to Facebook for social networking and to Google for searches.[26] As individuals move throughout the world around them, they leave a trail of data behind them.[27] This electronic footprint left on the internet "tells a story."[28] The data generated by network-connected smart devices "is almost invariably sent to the cloud where it's carefully aggregated, packaged, and then usually sold."[29] The privacy and attention traded for the existence of "free" services and content is

16. *Id.*
17. *Id.*
18. *Id.*
19. HARTZOG, *supra* note 1, at 261.
20. *Id.*
21. Alasdair Allan, *The Coming Privacy Crisis on the Internet of Things*, MEDIUM (Oct. 8, 2017), https://medium.com/@aallan/has-the-death-of-privacy-been-greatly-exaggerated-f2c4f2423b5.
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*

growing increasingly personal.[30] Now the data being shared, collected, and sold is not just "email[s] or the photographs of your cat, but your location, your heart rate, your respiration rate . . . [n]ot just how you slept last night, but with whom."[31] In short, connecting devices to the internet has resulted in poor privacy controls and poor security.[32] Consumers can avoid the death of privacy only if problems with smart devices continue to be "public relations nightmares for the companies involved."[33] "The loss of privacy may seem inevitable, but the only thing that makes it that way is our own apathy."[34]

Thus, "[t]here is no longer any question that data collection can create privacy harms for individuals: the question is what the law can and should do about it."[35] Currently, the central goal of American privacy law "is to create an environment where industry experiments first and asks questions later . . . ."[36] "Data collection by private entities is governed by a patchwork of state and federal law that applies on a sectoral basis."[37] If no sector-specific law applies, companies are free to collect data and use it at-will.[38]

But, if there is a privacy crisis, this raises the question of how exactly we define privacy. One way of defining privacy is "limited access to the self."[39] As it relates to privacy concerns in industry—primarily the overzealous collection, subsequent sale, and illicit use of personal information—this definition of privacy shall suffice for purposes of this article. After all, preventing exposure of one's personal information limits access to one's most intimate self. As an elaboration, privacy scholar Alan Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[40] The current landscape of privacy law in America, as well as globally, represents a "work in progress" held together by legal "duct tape" that "lacks cohesion."[41]

---

30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.*
34. *Id.*
35. Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1059 (2019).
36. *Id.* This is oddly reminiscent of KGB operatives during the Cold War, who shot first and asked questions later.
37. *Id.*
38. *Id.*
39. HARTZOG, *supra* note 1, at 10.
40. *Id.* at 63.
41. *Id.* at 56.

America's current "patchwork approach to privacy" allows some problems to go unnoticed and unsolved.[42] Exacerbating this issue, "lawmakers focus so intently on the details of complex, sector-specific statutes and regulations that they often fail to see the forest for the trees."[43] In short, America's legislators are not using all of their available tools to confront the privacy crisis.[44] Current disclosure-based regulatory regimes tend to "bury and obscure privacy-relevant information," overwhelming users.[45] One need only look at a single app's privacy policy to understand this. Consumers are most often confronted by:

> a threadbare, formalistic, or meaningless technical legal compliance . . . that overwhelms individuals with information and choices instead of substantively protecting them. It would be impracticable to read even a small fraction of the privacy notices we're asked to consent to or to forgo using the services we rely on . . . .[46]

If ordinary internet users were to read every single privacy policy they came across in the span of a year, it would take the user seventy-six working days to do so.[47] "[M]obile apps can seek over 235 . . . different types of permissions from smartphone users, with the average app asking for around five different permissions to access and use data."[48] Efforts to adapt the privacy torts to modern data collection and uses have failed.[49]

There is an inherent hypocrisy to the modern privacy crisis. "[W]hile powerful businesses, financial institutions, and government agencies hide their actions behind nondisclosure agreements . . . our own lives are increasingly open books. Everything we do online is recorded . . . ."[50] The decline in personal privacy has not been matched by business transparency. Credit agencies, search engines, and banks collect data about individuals, quantifying it into scores, rankings, and risk calculations while simultaneously shielding the details of the mechanisms by which they do so from

---

42. *Id.* at 57. For example, reliance on a web of statutes prevents privacy issues relating to overall technological design from being uniformly regulated.
43. *Id.*
44. *Id.*
45. *Id.* at 59.
46. *Id.* at 61.
47. *Id.* at 64.
48. *Id.* at 66.
49. *Id.* at 67.
50. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3 (2015).

public scrutiny.[51] Corporations "have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how they use this knowledge . . . ."[52]

As the internet has become ubiquitous, "personal data became substantially easier to access and track in ways unimaginable in decades prior."[53] Moreover, advanced algorithms allow utilization of personal data in a variety of fashions, "from predicting social trends to providing personalized financial advice."[54] Processing of personal data can yield social benefits while misuse of personal data can inflict personal harm upon individuals.[55]

A. Recent Data Breaches & the Privacy Void

Recent consumer data breaches provide a helpful illustration of the privacy crisis described above.

1. The Equifax Data Breach

In September 2017, Equifax, one of the three largest consumer credit reporting agencies in the United States, announced that its systems had been compromised.[56] The data breach included "names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers. The credit card numbers of approximately 209,000 consumers were also breached."[57] Federal Trade Commission (FTC) Chairman Joe Simons asserted that Equifax "failed to take basic steps that may have prevented the breach that affected approximately 147 million consumers."[58] The FTC claimed "Equifax failed to patch its network after being alerted in March 2017 to a critical security vulnerability . . . ."[59] Hackers were able to access a staggering amount of data because Equifax failed to implement basic security concerns.[60] The FTC also claimed Equifax stored network credentials and passwords, as well

51. *Id.* at 4.
52. *Id.* at 9.
53. Tyler Stites, *Data Protection on the Doorstep: How the GDPR Impacts American Financial Institutions*, 38 REV. BANKING & FIN. L. 132, 132 (2018).
54. *Id.*
55. *Id.*
56. *Equifax Data Breach*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/data-breach/equifax/ (last visited Sept. 22, 2019).
57. *Id.*
58. Press Release, Fed. Trade Comm'n, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [hereinafter FTC Press Release].
59. *Id.*
60. *Id.*

as Social Security numbers and other sensitive consumer information, in plain text.[61] Ironically, "[d]espite its failure to implement basic security measures, Equifax's privacy policy at the time stated that it limited access to consumers' personal information and implemented 'reasonable physical, technical, and procedural safeguards' to protect consumer data."[62] Unfortunately, Equifax's response to the data breach was not entirely successful. Its response to the breach "raised concerns among security experts and consumer advocates," with security expert Brian Krebs labeling Equifax's response to the breach as a "dumpster fire."[63] Moreover, consumers who contacted Equifax following the breach to freeze their credit were given PINs that corresponded to the date and time of the freeze, making the PINs easier for criminals to guess.[64]

Both the FTC and Consumer Financial Protection Bureau (CFPB) investigated the Equifax Data Breach.[65] As a result of the data breach, Equifax agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement with the FTC, CFPB, and fifty states and territories.[66] After a settlement with Equifax, affected consumers could file a claim for free credit monitoring or accept a cash payment of $125.[67] Moreover, "beginning in January 2020, Equifax will provide all U.S. consumers with six free credit reports each year for seven years . . . ."[68] But, credit monitoring or a few dollars cannot truly compensate the loss of one's privacy, particularly with respect to sensitive information like social security numbers. However, Equifax even botched the management of its settlement. The public response to the settlement has been overwhelming.[69] Because the amount of money set aside for the cash payment option is capped at $31 million, consumers who select that option may not receive the $125 they expected.[70]

61. *Id.*
62. *Id.*
63. *Equifax Data Breach*, *supra* note 56.
64. *Id.*
65. *Id.*
66. *See* FTC Press Release, *supra* note 58.
67. *Equifax Data Breach*, *supra* note 56.
68. FTC Press Release, *supra* note 58.
69. Press Release, Fed. Trade Comm'n, FTC Encourages Consumers to Opt for Free Credit Monitoring, as Part of Equifax Settlement (July 31, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-encourages-consumers-opt-free-credit-monitoring-part-equifax.
70. *Id.*

2. The Capital One Data Breach

In July 2019, a Seattle software engineer hacked into a server holding Capital One's customer information, obtaining the personal data of over 100 million people.[71] The culprit stole 140,000 Social Security numbers and 80,000 bank account numbers in the breach, later boasting online a desire to "distribute" the information.[72] Capital One has suffered prior security breaches. In 2017, the same year as the Equifax breach, Capital One reported that a former employee had access to consumers' personal data for nearly four months, including account numbers, telephone numbers, transaction history, and Social Security numbers.[73] Security breaches are a continuous threat to the financial industry. JPMorgan Chase executive Jamie Dimon has stated that his company spends nearly $600 million per year on security.[74] Similarly, Bank of America has said that its budget for cybersecurity is a blank check.[75]

3. Other Significant Data Breaches

Organizations like Anthem, Blue Cross Blue Shield, T-Mobile, the Internal Revenue Service, and the United States Army National Guard have all experienced data breaches in recent years.[76] Yet, the privacy void we face is not the result of corporate "evil" or malintent. In fact, many business executives expressly state their concerns for the privacy of their consumers and user base;[77] rather, such issues are the result of "overwhelming" economic initiatives to "design technologies in a way that maximizes the collection, use, and disclosure of personal information."[78] Opponents of additional privacy regulations on industry claim that "[w]e already have effective privacy laws that prevent harmful collection, use, and disclosure of personal information . . . ."[79] However, "[a] study by the Pew Research Center found that most adults do not believe online service providers will keep their data private and secure."[80]

---

71. Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of over 100 Million*, N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. HARTZOG, *supra* note 1, at 3.
77. *Id.* at 4.
78. *Id.* at 5.
79. *Id.*
80. *Id.* at 6.

There have been numerous data breaches in recent years. For example, a 2013 breach of Yahoo resulted in the theft of names, birth dates, phone numbers, and passwords impacting nearly three billion users of the site worldwide.[81] A 2015 breach of the federal government's Office of Personnel Management resulted in exposure of the personal data of more than twenty million people, including many with government security clearances.[82] Data breaches of Chipotle, Home Depot, and Target impacted over 100 million individuals, whose credit card numbers were stolen.[83]

Data breaches create considerable problems for consumers stemming from the loss of privacy. One such problem is identity theft.[84] The FTC reported 399,225 cases of identity theft in the United States in 2016.[85] Of that number, twenty-nine percent involved the use of personal data to commit tax fraud.[86] More than thirty-two percent reported that their data was used to commit credit card fraud.[87] Additionally, a 2015 report from the Department of Justice estimated the cost of identity theft to the American economy at $15.4 billion.[88] For an individual consumer, identity theft can result in denial of credit for credit cards and loans, denial of housing, increased interest rates on existing credit cards, and emotional distress and anxiety.[89]

Privacy is being eroded "click by click."[90] Those concerned with privacy most often ask how they can protect themselves in the age of data collection and data breach.[91] But, this begs the question: why must individuals protect themselves in the realm of privacy when the law shields the public for protective purposes in other facets of life, such as operating a motor vehicle, financial services, and criminal justice? This article argues that individuals should not have to.

B. The Lack of Federal Trade Commission Enforcement Power

Given the current state of privacy law in the United States, a private actor not falling under the definition of a narrowly defined,

81. *Equifax Data Breach*, *supra* note 56.
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.*
90. HARTZOG, *supra* note 1, at 6.
91. Allen, *supra* note 12, at 12.

sector-specific privacy statute "can largely do whatever it wants with the data it collects or otherwise obtains, provided it does not lie about its actions and attract the attention of an overstretched FTC."[92] Presently, the FTC is the primary federal agency tasked with protecting individuals from privacy exploitation from commercial entities as it pertains to data privacy, data security, and data misuse.[93]

The FTC asserts that "[w]hen companies tell consumers they will safeguard their personal information," it takes legal action to ensure companies fulfill their promises.[94] One of the only major federal legal frameworks in the United States addressing privacy in the consumer realm is Section 5 of the Federal Trade Commission Act.[95] In many instances of consumer privacy issues, the FTC charges corporations with violation of Section 5 of the FTC Act.[96] Specifically, Section 5(a) of the FTC Act declares unlawful "[u]nfair or deceptive acts or practices in or affecting commerce . . . ."[97]

However, there are substantial limits to the FTC's ability to protect consumer privacy. Any company within the FTC's jurisdiction that uses consumer information in a way that constitutes an unfair or deceptive trade practice is subject to the FTC's oversight.[98] The FTC is essentially the "sole backstop for the weaknesses of the rest of U.S. consumer privacy law . . . ."[99] In short, the FTC can only do so much. Moreover, the FTC's authority does not include common carriers or non-profits.[100] The FTC also lacks the general rulemaking authority of other administrative agencies, policing industry only on a reactive, case-by-case basis.[101] In privacy and data security cases, the FTC typically only utilizes its "deception" authority and rarely relies on its "unfairness" authority.[102] This means that the FTC's monitoring of privacy abuses remains limited to those instances when a company is not forthright about its practices, "regardless of whether the practice itself is inherently abusive . . . ."[103] Because most privacy policies are "difficult to understand" and

92. Barrett, *supra* note 35, at 1061–62.
93. *Id.* at 1073.
94. *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Sept. 22, 2019).
95. *See generally* 15 U.S.C.A. § 45.
96. *Privacy and Security Enforcement*, *supra* note 94.
97. 15 U.S.C.A. § 45(a)(1).
98. Barrett, *supra* note 35, at 1073–74.
99. *Id.* at 1074.
100. *Id.*
101. *Id.*
102. *Id.* at 1075.
103. *Id.*

"rarely read," the FTC's reliance on deception-based enforcement is relatively narrow, allowing corporations to escape legal scrutiny so long as their privacy policies remain truthful, even if exploitative.[104] The FTC's regulatory approach follows no more than an insufficient "do not lie" approach to privacy.[105]

As data breaches become more pervasive and devastating, the FTC is becoming increasingly reluctant to comment on even egregious cases of consumer privacy infractions.[106] The FTC lacks the economic teeth necessary to realistically punish corporations for privacy transgressions. The FTC's powers do not have a "serious deterrent effect" for preventing mishandling of our private information.[107] The largest privacy fine the FTC ever imposed is $5 billion.[108] For comparison, Facebook's 2018 revenue alone was approximately $56 billion, "making the likelihood of a fine that will meaningfully change the company's approach decidedly slim."[109] Overall, the FTC's privacy enforcement mechanisms are "deliberately laissez-faire."[110] This is a fundamental shortcoming because "protecting consumers in a twenty-first century economy where ubiquitous commercial surveillance can both harm consumers and have anticompetitive effects requires an FTC that can *prevent* new kinds of informational harms, not simply *react* to them."[111] As it stands, the nation's largest companies lack a sufficient check on abusive, privacy-invasive practices.[112] In fact, "[t]here is little in current law to prevent companies from selling their profiles of you."[113]

II. THE ADOPTION OF THE DODD-FRANK ACT

The 2008 economic collapse, known as the Great Recession,[114] would be among the worst in American history, rivaling only the

104. *Id.*
105. HARTZOG, *supra* note 1, at 67–68.
106. Barrett, *supra* note 35, at 1075–76; *see, e.g.*, Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests*, WASH. POST (Nov. 30, 2018, 1:03 PM), https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/.
107. PASQUALE, *supra* note 50, at 23.
108. Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FED. TRADE COMM'N (July 24, 2019, 8:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.
109. Barrett, *supra* note 35, at 1076–77.
110. *Id.* at 1077.
111. *Id.* (emphasis added).
112. *Id.*
113. PASQUALE, *supra* note 50, at 32.
114. For a comprehensive overview of the causes and consequences of the 2008 financial crisis, *see* FREDERIC S. MISHKIN, THE ECONOMICS OF MONEY, BANKING, AND FINANCIAL

Great Depression. The Great Recession led to economic despair that was unprecedented in twenty-first century America. Economic growth declined for three straight quarters in late 2008 and early 2009, by 1.3%, 5.4%, and 6.4% respectively.[115] Unemployment rose to over ten percent in the United States.[116]

The Great Recession led to the adoption of several regulatory regimes that changed the landscape of how government entities approached economic regulation in the financial sector. Following the collapse, the government's regulatory focus shifted from monitoring the economic soundness of "individual" financial institutions to the health of the financial "system."[117] One major reform was the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank).[118] Dodd-Frank "is the most comprehensive financial reform legislation since the Great Depression."[119] Its key provisions include consumer protection provisions, resolution authority for oversight entities, systemic risk regulation, the Volcker Rule, and regulation of derivatives.[120]

A. The Consumer Financial Protection Bureau

One of the major provisions of Dodd-Frank was the creation of the Consumer Financial Protection Bureau (CFPB), a "completely independent"[121] agency tasked with examining and enforcing regulations on all businesses with more than $10 billion in assets engaged in issuing residential mortgage products as well as on issuers of financial products targeted at low-income Americans.[122] "For consumer financial services, the centerpiece of the Dodd-Frank Act was the creation of the [CFPB]."[123] Congress vested the CFPB with the consumer financial protection functions of numerous federal agencies and gave the CFPB broad authority over segments of the consumer financial services market not previously subject to federal

---

MARKETS 274–86 (4th ed. 2015). The modern privacy landscape suffers from similar technological and information-based issues that led to the collapse. *See generally* PASQUALE, *supra* note 50, at 4–5. However, the focus of this article is how parallel *reform* efforts can address these parallel *issues*.

115. MISHKIN, *supra* note 114, at 282.
116. *Id.*
117. *Id.* at 283–84.
118. *Id.* at 284; *see also* 12 U.S.C.A. §§ 5301–5641.
119. MISHKIN, *supra* note 114, at 284.
120. *Id.* at 284–85.
121. *Id.* at 284.
122. *Id.*
123. Donald C. Lampe & Ryan J. Richardson, *The Consumer Financial Protection Bureau at Five: A Survey of the Bureau's Activities*, 21 N.C. BANKING INST. 85, 85 (2017).

regulation.[124] The CFPB serves three primary functions: rulemaking, supervision, and enforcement.[125]

Like the Consumer Data Protection Bureau called for later in this article,[126] the CFPB's origins lie in legal academia, as "calls to consolidate federal consumer financial protection functions in a single federal agency predated the financial crisis."[127] In 2005, Professor Heidi Mandanis Schooner of Catholic University argued that banking regulatory agencies' consumer protection responsibilities should be assigned to a single consumer protection agency.[128] In 2007, then-Professor Elizabeth Warren of Harvard University argued in an article entitled "Unsafe at Any Rate" that "streamlined federal consumer protections in the market for tangible goods (like toasters) had successfully balanced the twin goals of protecting consumers and promoting innovation."[129] In contrast, a fragmented regulatory framework in the financial services market had done the exact opposite, failing to protect consumers and limiting innovation.[130] Warren suggested the creation of a Financial Product Safety Commission to create guidelines for consumer disclosure, collect data regarding the uses of financial products, review financial products for consumer safety, and require modification of certain dangerous products before they could be marketed to the public.[131]

Dodd-Frank provides the CFPB with broad rulemaking, supervisory, and enforcement power over the consumer financial services market.[132] Congress gives the CFPB authority over "covered persons," which includes "'any person that engages in offering or providing a consumer financial product or service' and 'any affiliate of [such a person if the] affiliate acts as a service provider to the covered person.'"[133] Under Dodd-Frank, the CFPB can require reports and examinations of "covered persons" and "service providers" to assess their compliance with the law by obtaining information about their activities and compliance systems while detecting risks

124. *Id.*
125. *Id.* at 86.
126. *See infra* Part IV.B.
127. Lampe & Richardson, *supra* note 123, at 90.
128. *Id.* at 91. *See generally* Heidi Mandanis Schooner, *Consuming Debt: Structuring the Federal Response to Abuses in Consumer Credit*, 18 LOY. CONSUMER L. REV. 43, 67–77 (2005).
129. Lampe & Richardson, *supra* note 123, at 91. *See generally* Elizabeth Warren, *Unsafe at Any Rate*, DEMOCRACY J., http://democracyjournal.org/magazine/5/unsafe-at-any-rate/ (last visited Sept. 8, 2020).
130. Lampe & Richardson, *supra* note 123, at 91.
131. *Id.*
132. *Id.* at 97.
133. *Id.* at 95.

to consumers and markets in the realm of consumer financial products and services.[134]

The CFPB also has the power to "enforce" federal consumer financial law, including Title X of Dodd-Frank and rules created under Title X.[135] Dodd-Frank provides the CFPB with three primary enforcement tools: (1) investigation of potential violations of federal consumer financial law; (2) the ability to bring public legal actions in federal court or an administrative forum for violations of federal consumer financial law; and (3) the ability to seek injunctive and monetary relief for violations of federal consumer financial law.[136] The CFPB may demand document production, written responses, and oral testimony if it "has reason to believe that any person may be in possession, custody, or control of any documentary material or tangible things, or may have any information" relevant to a violation of consumer financial law.[137] While the CFPB's rulemaking and supervisory authorities only apply to "covered persons," its broad enforcement authority applies to any "person," resulting in a "sweeping, plenary power."[138]

The CFPB is flexible in its approach, adapting to necessary consumer protection issues as they arise via market developments. But, as much as the CFPB has earned praise from "members of Congress, consumer and community advocates and others," it has also "attracted the attention of policymakers intent on modifying the agency's structure and slimming down its powers," such as the Trump Administration.[139] The impact of the CFPB has been significant in its short history. It has "facilitated approximately $11.7 billion in consumer redress and $440 million in penalties . . . while promulgating thousands of pages of complex, wide-ranging regulations mandated or contemplated by the Dodd-Frank Act," while also conducting over 100 examinations.[140]

B. The Fiduciary Rule

One of Dodd-Frank's major reforms included the "Fiduciary Rule."[141] "The Fiduciary Rule requires financial advisers to act in the best interests of their clients regarding retirement planning

134. *Id.* at 104.
135. *Id.* at 106.
136. *Id.* at 107.
137. *Id.* at 108.
138. *Id.* at 107.
139. *Id.* at 128.
140. *Id.* at 127–28.
141. Corey F. Schechter, *Dodd-Frank and the Fiduciary Rule*, BUTTERFIELD SCHECHTER LLP (Mar. 21, 2017), https://www.bsllp.com/dodd-frank-and-the-fiduciary-rule.

. . . ."[142] The Fiduciary Rule was a package of seven different rules that re-interpreted the term "investment advice fiduciary" to encompass a wider variety of financial transactions.[143]

Beginning in 2010, the Department of Labor set out to overhaul the investment advice fiduciary definition.[144] Monumentally important to the financial services sector, the Fiduciary Rule consisted of 275 pages of regulations.[145] The Fiduciary Rule's definition of "investment advice fiduciary" encompassed "virtually all financial and insurance professionals who do business with ERISA plans and IRA holders."[146] The Fiduciary Rule also included a Best Interest Contract Exemption (BICE), allowing certain financial services providers to be exempt from the penalty provisions of the rule.[147] To qualify for an exemption, financial services providers would need to enter into contracts with clients that affirm their fiduciary status, incorporate impartial conduct standards including the duties of loyalty and prudence, avoiding misleading statements, and that "charge no more than 'reasonable compensation.'"[148]

However, despite its novelty, the reign of the fiduciary rule was short-lived, as its politically charged[149] nature led to its challenge in federal court by business groups.[150] In 2018, the Fifth Circuit vacated the rule,[151] "effectively put[ting] an end" to its operation.[152] Consumer advocates labeled the Fifth Circuit decision as "tragic," noting its implication that consumers would be "on their own" in looking out for their financial interests.[153] However, the Securities and Exchange Commission (SEC), whom Dodd-Frank specifically

142. *Id.*
143. Chamber of Com. v. U.S. Dep't of Lab., 885 F.3d 360, 363 (5th Cir. 2018).
144. *Id.* at 366.
145. *Id.*
146. *Id.*
147. *Id.* at 366–67.
148. *Id.* at 367.
149. *See* Schechter, *supra* note 141. The Fiduciary Rule received significant support from the Obama Administration as well as consumer advocates, hailing its ability to minimize investment advisers' potential conflicts of interest. *Id.* Alternatively, the Trump Administration and financial institutions viewed the rule as a burdensome mechanism that would hurt middle-class investors. *Id.*
150. *Chamber of Com.*, 885 F.3d at 363.
151. *Id.* at 387. In vacating the Fiduciary Rule, the Fifth Circuit characterized it as a backdoor regulation of a significant portion of the American economy. *Id.* at 388.
152. Lorie Konish, *Investor Protection Rule Is Dead*, CNBC (June 21, 2018, 3:30 PM), https://www.cnbc.com/2018/06/21/investor-protection-rule-is-dead.html.
153. *Id.*

authorized to create its fiduciary standard, has plans of proposing its own fiduciary standard.[154]

C. The Volcker Rule

One of Dodd-Frank's key risk management provisions is known as the Volcker Rule.[155] The Volcker Rule consists of a regulatory provision that limits the extent to which banks can trade with depositors' money.[156] This rule also prevents banks from owning more than just a small percentage of shadow entities such as hedge funds and private equity funds.[157] The rule prevents banks from undertaking large trading risks when they benefit from the safety net of federal deposit insurance.[158] As an analogy, the Volcker Rule of Dodd-Frank seeks to limit the moral hazard problem similar to that of a gambler using someone else's money: "I do not care if I lose $20,000 when my friend's money essentially insures me for $40,000." Thus, the Volcker Rule handcuffs banks from "gambling" their depositors' money.

III. ANALOGIZING THE CRISES: TOO BIG TO FAIL VS. TOO BIG TO PROTECT

In many ways, the modern privacy crisis resembles the 2008 financial crisis. In the sections below, these parallels are explored: the "Wild West" regulatory environment present in both realms, the data collection bubble currently arising in twenty-first century life (similar to the housing market bubble), and problems arising from the corporate use and sale of consumer data (similar to the frequent re-sale of mortgages by financial institutions prior to the financial crisis).

A. The "Wild West" Regulatory Environment

Specifically, the regulatory environment for American consumer privacy in 2019 largely parallels the pre-2008 Wall Street regulatory environment in terms of the weakness of the industry protections present in the current law. In the United States, "no comprehensive federal privacy or cybersecurity legislation has been

154. *Id.* The SEC would adopt a best-interest standard for investment advisers and broker dealers that make recommendations to retail investors, covering far more than just retirement accounts. *Id.*

155. MISHKIN, *supra* note 114, at 285.

156. *Id.*

157. *Id.*

158. *Id.*

enacted . . . ."[159] In recent years, there has been a "dramatic increase in devastating cyberattacks" and an increase in the "sophistication of hackers."[160] Even to businesses, "[c]yberattacks can be incredibly costly . . . as the company's data may be temporarily unavailable, destroyed, or even stolen or misused."[161] The 2019 consumer privacy landscape also resembles the Wild West, as "lax enforcement makes perfect sense in an environment where platforms want as many users as possible, as many app purchases as possible, and as many ad clicks as possible."[162] American privacy law "needs a radical course correction, not a mere adjustment."[163]

Corporations are not being entirely forthcoming with how they handle privacy. In 2014, Snapchat "ran afoul of the FTC for lying about how ephemeral its communications were."[164] The current concepts of notice and disclosure are also flawed. "[P]rivacy law still prioritizes technical compliance over meaningful disclosure when demanding notice."[165] Mortgage disclosures prior to 2008, as discussed above were similarly opaque. Woodrow Hartzog, a privacy scholar at Northeastern University School of Law, cautions, however, that "[p]rivate causes of action for privacy violations should be exceptions to the general rule of compliance."[166] Reform must target proactive solutions, rather than reactive panic.

In sum, "[m]ost data privacy laws within the U.S. are fragmented, regulating specific states or industries."[167] FTC regulatory authority derives mostly from enforcing company-issued privacy policies.[168] Dodd-Frank allowed the CFPB to study and regulate data portability in the United States.[169] Yet, the CFPB's current leadership takes a largely "inactive" approach to such regulation.[170] This essentially is a modified self-regulatory scheme, a potential recipe for disaster in the privacy realm. As Johnnie Cochran famously quipped in the O.J. Simpson trial, who is going to "police

159. Daniel Ilan et al., *Data Privacy and Cybersecurity in M&A: A New Era*, 10 LANDSLIDE 48, 50 (2018).
160. *Id.* at 49.
161. *Id.* at 50.
162. Barrett, *supra* note 35, at 1096.
163. *Id.* at 1113.
164. PASQUALE, *supra* note 50, at 123.
165. HARTZOG, *supra* note 1, at 69.
166. *Id.* at 83.
167. Stites, *supra* note 53, at 139.
168. *Id.*
169. *Id.* at 142.
170. *Id.*

the police?"[171] "[S]elf-regulation alone is not going to cut it" in terms of privacy protections in the twenty-first century.[172] Numerous incentives exist for companies to "design consumer technologies in ways that are adversarial" to our privacy interests.[173]

The time is ripe for reform. The business scandals of the late nineteenth century Gilded Age sparked bold legal reforms when the American public demanded business be held accountable to public scrutiny.[174] Such efforts intensified following the Great Depression in the form of the New Deal.[175] Numerous pieces of landmark legislation were passed to peel back the unnerving shroud of secrecy that encapsulated American industry and Wall Street.[176] America saw passage of the Securities Act of 1933 and the Securities and Exchange Act of 1934.[177] Throughout the twentieth century, a push for consumer protection led to the creation of new federal agencies, such as the FDA and the Consumer Product Safety Commission.[178] However, with the rise of the new millennium and the dawn of the age of Google, a cloak of corporate secrecy re-arose.[179] Internet technologies are spreading, "unmonitored and unregulated."[180]

B. The Data Collection Bubble

Privacy issues could be exacerbated if the economy's new "[t]ech [b]ubble" bursts.[181] Just about every company now holds user data.[182] If this data bubble bursts, what will be left of massive companies like Facebook and Twitter? Likely, "the only thing worth salvaging from the shells of former tech companies may be user data."[183] As for what the aftermath of a collapse would look like from a data perspective, consider the bankruptcy of RadioShack. When RadioShack filed for bankruptcy, "one of the assets it put up for sale was its meticulously compiled database of information on

171. David Margolick, *With Tale of Racism and Error, Simpson Lawyers Seek Acquittal*, N.Y. TIMES (Sept. 29, 1995), https://www.nytimes.com/1995/09/29/us/with-tale-of-racism-and-error-simpson-lawyers-seek-acquittal.html.
172. HARTZOG, *supra* note 1, at 72.
173. *Id.*
174. PASQUALE, *supra* note 50, at 11.
175. *Id.*
176. *Id.*
177. *Id.*
178. *Id.* at 12.
179. *Id.* at 13.
180. *Id.* at 14.
181. Kaveh Waddell, *Who Will Own Your Data If the Tech Bubble Bursts?*, THE ATLANTIC (May 13, 2016), https://www.theatlantic.com/technology/archive/2016/05/what-happens-to-your-data-if-the-tech-bubble-bursts/482622/.
182. *Id.*
183. *Id.*

millions of its customers."[184] Soon thereafter, AT&T and Apple claimed to own some of the data, and "officials in a handful of states warned that the sale could violate state laws."[185]

"Corporations, data brokers, and even criminals might buy failed companies just for their users' personal information."[186] Companies may resort to selling user data—"whether it's personally identifiable information, data about preferences, habits, and hobbies, or national-security files."[187] This data could be attractive to both business and criminal buyers.[188] "If contracts and privacy policies prevent a floundering company from selling user data, there's still another way to profit. Most privacy policies that promise not to sell user data include a caveat in case of bankruptcy or sale."[189] A New York Times analysis of 100 of the top web sites in the United States last year found that eighty-five percent of them include clauses in their privacy policies, providing that "[i]f the ownership or control of all or part of our [s]ervices or their assets change[], we may transfer your information to the new owner."[190] This type of transfer of data bears resemblance to the securitization and subsequent sale of packages of mortgage loans in 2008 by failing financial services organizations.[191] If the tech bubble bursts, it is unlikely that the FTC would have appropriate enforcement power to "keep up with the sheer number of previously overvalued data-rich companies offering themselves . . . for sale."[192] Without any other legal remedy in place, "the post-bubble technology industry will take your data down with it . . . ."[193]

IV. THE DODD-FRANK APPROACH FOR AMERICAN PRIVACY

If Americans cannot stop "pervasive" data collection, use, and sale, the question becomes: "[w]hat do we do?"[194] Self-help through privacy-enhancing technologies like "do not track" functions in internet browsers will likely fail "on practical grounds for all but the most skilled (or wealthy) Internet users . . . ."[195] Each day that

184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.*
188. *Id.*
189. *Id.*
190. *Id.*
191. *See generally* MISHKIN, *supra* note 114, at 274–86.
192. Waddell, *supra* note 181.
193. *Id.*
194. PASQUALE, *supra* note 50, at 52.
195. *Id.* at 53–54.

privacy "enhancing" technology emerges, so does privacy "eviscerating" technology.[196] In short, the answer lies in the law. Imposing accountability-based legal structures on corporations that define "fair and unfair uses of information" can catalyze a solution.[197] This article proposes a Dodd-Frank approach to comprehensive American consumer privacy legislation based upon three prongs: (1) fiduciary responsibilities; (2) the creation of a Consumer Data Protection Bureau; and (3) the promulgation of a "Volcker Rule" for data privacy.

A. Mandate of Data Fiduciary Responsibilities

To be effective, comprehensive consumer privacy legislation should include a mandate of fiduciary responsibilities upon certain data-collecting American businesses who share a special relationship to consumers because of consumers' trust in these businesses with their most sensitive information. In short, businesses would be subject to fiduciary responsibilities when holding themselves out as organizations who give consumers reason to believe personal consumer data will not face unreasonable disclosure or misuse. Such an idea is not outlandish or even without legislative support. Senator Brian Schatz, as well as fourteen other Senators, have already proposed the Data Care Act, a comprehensive legislative framework that "sketches out broad duties of loyalty, care, and confidentiality, while providing the FTC with rulemaking authority to determine the details."[198]

Though market forces are often powerful in curbing illicit business behavior, here they are likely to be insufficient. A mandate is necessary because "a voluntary [information fiduciary regulatory] regime shaped by the lobbyists for the companies it would purport to regulate will be subject to the same broad provisions and tepid commitments of other self-regulatory programs that have been largely ineffective."[199] All else being equal, "companies like Facebook or Google would like to maximize the value of the personal data they collect" as "end-user data is one of [a company's] most valuable assets."[200] But, its status as a central component of many companies' business models "creates an inherent potential for

196. *Id.* at 53.
197. *Id.* at 57.
198. Barrett, *supra* note 35, at 1094.
199. *Id.* at 1093.
200. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1226 (2016).

conflicts of interest" between the company and the consumer.[201] Additionally, reliance upon market forces alone to solve these conflict of interest problems is insufficient.[202] Though the market *can* punish companies with bad reputations for mistreating their consumers, "there is no guarantee that this will be enough to effectively police all forms of misbehavior."[203] Personal data is a source of wealth in the digital economy.[204] Because of this, information fiduciaries "should be able to monetize some uses of personal data . . . ."[205] What they should not be able to do is "use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm."[206]

1. The Jack Balkin "Information Fiduciaries" Concept

Privacy is not at odds with business development and innovation. As Professor Jack Balkin of Yale Law School recognizes, "personal privacy in the digital age can co-exist with rights to collect, analyze, and distribute information that are protected under the First Amendment . . . through the concept of an *information fiduciary*."[207] "[M]any online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users."[208] Modern consumer businesses rooted in digital technology possess special power and relationships with others. Accordingly, Balkin argues that information fiduciaries have "special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[209] However, as a responsible basis for a privacy regulatory framework, the duties information fiduciaries owe must be contextually related to both the nature of their business and the expectations of the public.[210]

This begs the question, however, of what a fiduciary is. A fiduciary is "one who has special obligations of loyalty and trustworthiness toward another person," taking care to act in the interests of

201. *Id.*
202. *Id.*
203. *Id.*
204. *Id.* at 1227.
205. *Id.*
206. *Id.*
207. *Id.* at 1186.
208. *Id.*
209. *Id.*
210. *Id.*

the other person—known as the beneficiary or client.[211] At its core, a fiduciary relationship is a relationship of trust.[212] A client puts their trust or confidence in the fiduciary, and the fiduciary must avoid betraying the client's confidence or trust.[213] Fiduciaries may perform professional services or manage property for a client,[214] but they do not necessarily have to. Yet, almost always, fiduciaries "also handle sensitive personal information" as fiduciary relationships "involve the use and exchange of information."[215] Modern consumer interactions are no different.

Generally, fiduciaries have two basic duties to their beneficiaries: a duty of care and a duty of loyalty.[216] First, the duty of care requires the fiduciary to "act competently and diligently so as not to harm the interests" of the beneficiary.[217] Second, the duty of loyalty requires the fiduciary to keep their beneficiaries' interests at heart and act in the beneficiaries' interests.[218] At the heart of these duties are relationships "often centrally concerned with the collection, analysis, use, and disclosure of information."[219] Therefore, a fiduciary also has a duty "not to use information . . . in ways that harm or undermine" the beneficiary.[220] Accordingly, all fiduciaries, at least as Balkin labels them, are "*information fiduciaries*."[221] An information fiduciary is "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."[222] Moreover, people and organizations possessing fiduciary duties arising from the use or exchange of information are fiduciaries regardless of whether they do something on the beneficiary's behalf.[223] The information fiduciary model provides a broad cornerstone by which legislators may shape the coverage scope of twenty-first century consumer privacy law in the United States.

211. *Id.* at 1207.
212. *Id.*
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.* at 1207–08.
217. *Id.*
218. *Id.* at 1208.
219. *Id.*
220. *Id.*
221. *Id.*
222. *Id.* at 1209.
223. *Id.*

2. Data's Fiduciary Rule

The modern digital age has "given rise to new fiduciary relationships created by the explosion of the collection and use of personal data"[224] because there now exists relationships of trust between end-users and online consumer service providers. However, from a regulatory perspective, Balkin argues that these relationships should not be identical to traditional professional fiduciary relationships in all respects because they "may not require the same degree of obligation, loyalty, and protection . . . ."[225] But, these are still fiduciary relationships nonetheless. Balkin notes that "in the digital age, because we trust [consumer entities] with sensitive information," these entities take on fiduciary responsibilities.[226]

Balkin argues we should adopt an information fiduciary regulatory model for twenty-first century consumer privacy protection for four main reasons. First, consumers' relationships with many business entities now involve "significant vulnerability" because these businesses have considerable expertise and knowledge with respect to proprietary online services, and consumers generally lack information about the businesses or what they do with collected information.[227] Second, consumers are "in a position of relative dependence with respect to these companies."[228] Businesses provide many different kinds of services consumers need and consumers must hope that the companies will not misuse their information or abuse their confidence in ways that will harm them.[229] Third, many online service providers and consumer businesses "hold themselves out as experts in providing certain kinds of services in exchange for [consumers'] personal information."[230] Fourth, these entities know they hold valuable data that may be used to consumers' disadvantage, and they understand consumers are aware of this.[231] Thus, these businesses "hold themselves out as trustworthy organizations who act consistent with our interests, even though they also hope to turn a profit."[232] In short, "[b]ecause people understand that they are vulnerable to the collection of personal data, and because they also recognize that the methods used by online service providers are beyond their understanding, they seek reassurance that using these

224. *Id.* at 1221.
225. *Id.*
226. *Id.*
227. *Id.* at 1222.
228. *Id.*
229. *Id.*
230. *Id.*
231. *Id.*
232. *Id.*

services is safe."[233] Unfortunately, most of the details of how companies are utilizing consumers' sensitive information is buried within the "fine print of their privacy policies and in the code of the company's information infrastructure."[234] Therefore, "a changing society generates new kinds of fiduciary relations and fiduciary obligations that the law can and should recognize."[235] Balkin suggests the following formulation for a Data Fiduciary Rule:

> People and business entities act as information fiduciaries (1) when these people or entities hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them; (2) when these people or entities give individuals reason to believe that they will not disclose or misuse their personal information; and (3) when the affected individuals reasonably believe that these people or entities will not disclose or misuse their personal information based on existing social norms of reasonable behavior, existing patterns of practice, or other objective factors that reasonably justify their trust.[236]

Importantly, Balkin notes this formulation of a Data Fiduciary Rule "may require information fiduciaries to protect more things than they have explicitly set out in their privacy policies."[237] Though, this is for the better. As the late Justice Antonin Scalia often noted, "[t]he more speech, the better."[238] Likewise, the more privacy the better. A Data Fiduciary Rule would serve a valuable purpose: "when entities hold themselves out as trustworthy, and when they encourage the disclosure of personal information that places end-users in a vulnerable position, entities should be held accountable . . . ."[239] Also, modern information fiduciaries "may be held to reasonable ethical standards of trust and confidentiality" because of the type of business they engage in.[240]

The Data Fiduciary Rule would also affect third parties. "Fundamentally, a higher legal obligation to users would help shift the

233. *Id.*
234. *Id.*
235. *Id.* at 1223.
236. *Id.* at 1223–24.
237. *Id.* at 1224.
238. Matt Vasilogambros et al., *Scalia Defends* Citizens United *Decision, Reflects on Term in Rare TV Appearance*, THE ATLANTIC (July 18, 2012), https://www.theatlantic.com/politics/archive/2012/07/scalia-defends-citizens-united-decision-reflects-on-term-in-rare-tv-appearance/437268/.
239. Balkin, *supra* note 200, at 1224–25.
240. *Id.* at 1225.

default attitude of data collectors from 'collect everything and ask questions later,' as would holding the service provider responsible for enabling privacy invasions by third parties."[241] Both Balkin and the proposed Data Care Act propose that "fiduciaries should be required to contractually obligate any third parties they share data with to uphold the fiduciary duties they owe their users."[242] Invoking a property concept, "fiduciary obligations must run with the data."[243] "Affirmative legal duties to users, like a prohibition on sharing their information except with entities required to uphold the fiduciary's same duties, would vastly limit incentives to share information" in a reckless fashion.[244]

This model invokes common sense. An information fiduciary model of privacy regulation bears logical resemblance to fiduciary obligations already recognized in American law.[245] For example, consider a doctor, lawyer, or accountant that sold personal information about their clients to a data broker.[246] If these professionals used personal information to manipulate their client's actions for self-interested ends or to gain a business advantage at the expense of their client, they would likely face liability for violating their professional conduct obligations.[247] In essence, the information fiduciary model of privacy regulation merely suggests we extend similar fiduciary principles to those consumer entities which now possess equally sensitive information as professional service providers. Just as in their interactions with doctors, accountants, and lawyers, many consumers assume a sense of personal trust or special confidentiality in their online interactions. Information fiduciaries are no longer just lawyers, doctors, and accountants. In the digital age, they now include our bankers, ride-sharers, social media platforms, digital communications services, and even schools.

"[A]n information fiduciary framework can strike the necessary balance of competing objectives: it is designed to balance commercial prerogatives with meaningful protections for individuals in the way that U.S. privacy law attempts, yet fails, to do."[248] Applying fiduciary duties to data collectors raises the bar of how digital companies are expected to treat user information.[249] "It would help

241. Barrett, *supra* note 35, at 1099.
242. *Id.*
243. *Id.*
244. *Id.*
245. Balkin, *supra* note 200, at 1205.
246. *Id.*
247. *Id.*
248. Barrett, *supra* note 35, at 1087.
249. *Id.* at 1088.

adjust the objective of U.S. privacy law to more heavily prioritize the rights of the user, while still accounting for the commercial prerogatives of the collector."[250] "Duties of loyalty, care, and confidentiality can also prohibit digital harms such as manipulation, discrimination, and other harms that laws exclusively focused on privacy are ill-equipped to prevent, while still permitting non-harmful commercial activity."[251]

Fiduciary rules provide flexibility with respect to professional prerogatives, but they are not "toothless, and they implicate a moral dimension to the regulation of commercial conduct that other consumer protection regulation does not automatically invoke . . . ."[252] Exploiting user information "should not be required for digital products and services to function, and for most of them it is not."[253] Social networks "need not be inherently manipulative, discriminatory, or privacy-invasive—the same is true for an internet service provider, a rideshare company, a medical device company, or a cloud service."[254] Applying fiduciary duties to data collectors requires distinguishing the "kinds of conduct that are inherent to the service—such as a search engine 'discriminating' by sorting through information and only providing the responsive results—from disloyal conduct designed to benefit the data collector to the detriment of the subject."[255]

An information fiduciary framework also solves asymmetric information problems. As in the pre-2008 mortgage markets, modern consumer markets that are reliant on mass data suffer from asymmetric information problems—consumer entities simply possess information with respect to their data practices that consumers do not. Fiduciary concepts may again provide a solution. Fiduciary law assumes that fiduciaries and their beneficiaries are not on "equal footing" because fiduciaries usually possess special skills or knowledge that their beneficiaries lack.[256] The beneficiaries depend upon the fiduciaries to perform certain tasks for them and are often ill-equipped to monitor the behavior of the fiduciaries or prevent them from abusing their relationship of trust, absent any obligations that fiduciary law would supply.[257] Because of information, skill, and knowledge asymmetries, the beneficiaries must trust the

250. *Id.*
251. *Id.*
252. *Id.* at 1091–92.
253. *Id.* at 1092.
254. *Id.*
255. *Id.* at 1089.
256. Balkin, *supra* note 200, at 1216.
257. *Id.*

fiduciaries to act in their best interest.[258] "There are strong asymmetries of information between companies and end users."[259] Company "operations, algorithms, and collection practices are mostly kept secret," most often for sound business reasons.[260] Still, "end-users are not in a very good position to assess how well companies will protect their interests or to decide which company will treat them best in the long run" because "end-users are largely dependent on the good will of these companies not to abuse their personal information."[261] Consequently, these businesses "present the familiar problems that generally give rise to fiduciary obligations."[262] It is difficult for consumers to verify company "representations about data collection, security, use, and dissemination"[263] or to comprehend what companies do with their data.[264] Even if consumers understood these practices, it would be nearly impossible for consumers to monitor them.[265] This situation is analogous to that of financial advisors. Consumers expect that financial advisors will make money from consumers seeking financial advice.[266] However, the fact that consumers expected financial advisors to make money did not prevent the government from attempting to impose fiduciary obligations upon them.[267]

3. Obstacles to Data's Fiduciary Rule, Skepticism, and Supplemental Regulation

Privacy regulations would not be immune to constitutional scrutiny.[268] However, the type of regulation would matter, as privacy regulations concerning the collection and use of data rather than data analysis, disclosure, or sale are less likely to face First Amendment challenges.[269] But, even First Amendment arguments would not doom privacy regulations targeted at data analysis, disclosure, or sale, as when data is "collected, collated, used, and sold in bulk" it is a commodity rather than speech.[270] Specifically, the question arises as to how legislators could keep the information fiduciary

258. *Id.*
259. *Id.* at 1226.
260. *Id.*
261. *Id.* at 1226–27.
262. *Id.* at 1227.
263. *Id.*
264. *Id.*
265. *Id.*
266. *Id.* at 1228.
267. *Id.*
268. *Id.* at 1194.
269. *Id.*
270. *Id.* at 1196.

concept from running afoul of the First Amendment and any right to corporate speech. The answer rests in the law. As Balkin recognized, "when the law prevents a fiduciary from disclosing or selling information about a client—or using information to a client's disadvantage—this does not violate the First Amendment, even though the activity would be protected if there were no fiduciary relationship."[271]

Additional regulation is necessary to supplement any Data Fiduciary Rule. A regulatory framework based exclusively on information fiduciaries would not solve all the problems of "overreaching that will inevitably occur in the age of Big Data."[272] Any consumer privacy fiduciary rule cannot operate in a vacuum if it is to operate successfully. A fiduciary approach is not a replacement for "badly needed structural reforms."[273] Supplemental provisions would also aim to "strengthen existing protections, such as more meaningful obligations to enact reasonable security protocols, and stricter requirements to notify users in the case of breach."[274] For example, opt-in rules could be a helpful supplement to an information fiduciary framework. Such rules can also likely withstand judicial scrutiny, as in 2009 the D.C. Circuit upheld new FCC rules imposing opt-in requirements even in light of a First Amendment challenge.[275]

Also, compliance disasters in the early years of the rule could be an issue. Thus, during a legislative phase-in period, to avoid subjection to penalties under Data's Fiduciary Rule, corporations could be permitted to enter into "best interest contracts" with consumers that affirm fiduciary status and incorporate a duty of loyalty, similar to the BICE the Department of Labor developed following the 2008 financial collapse.[276] The framework proposed by this article is not the only approach to enacting a data fiduciary rule in the consumer privacy realm. For example, there is a more broad and flexible approach that would likely be subject to extensive judicial interpretation and administrative discretion. Ariel Dobkin argues that "informational fiduciary duties should be divided into four categories of behavior: manipulation, discrimination, sharing with

271. *Id.* at 1210; *see id.* at 1211–20 (discussing the difference between speech which is in the public discourse and speech which is removed therefrom and the implications for regulation thereof).

272. *Id.* at 1187.

273. Barrett, *supra* note 35, at 1107.

274. *Id.* at 1097.

275. Balkin, *supra* note 200, at 1203 (citing Nat'l Cable & Telecomms. Ass'n v. FCC, 567 F.3d 659 (D.C. Cir. 2009)).

276. Chamber of Com. v. U.S. Dep't of Lab., 885 F.3d 360, 367 (5th Cir. 2018).

third parties without consent, and violations of a company's privacy policy."[277] "A duty is violated when the fiduciary exceeds a reasonable user's expectations, which those types of conduct will generally do."[278]

But, political conservatives and skeptics need not fear this regulatory framework as being a government overreach, as such a rule would "not apply to everyone. Merely communicating with someone over the Internet does not make [an entity] an information fiduciary."[279] Thus, many business practices concerning consumer data will remain free from regulation.[280] Moreover, the duties legislators may impose on these businesses are likely to be "considerably narrower" than traditional professional fiduciary responsibilities.[281] Also, imposition of fiduciary responsibilities does not mean that all American consumer businesses will suddenly become non-profit entities.[282] The regulatory relationship need not be parasitic or economically harmful; rather, it can be cooperative. "[E]ven though virtual environments are privately owned, governments could create framework statutes that would require platform owners to respect the free speech and privacy rights of end users in return for special legal status and benefits."[283] Ultimately, the legislative process and administrative rulemaking procedures will fashion the precise contours of data's fiduciary rule. Yet, that is beyond the scope of this article.

B. Creation of the Consumer Data Protection Bureau

In the wake of recent data breaches, some have called for the creation of a governmental data protection agency in the United States.[284] Electronic Privacy Information Center (EPIC) suggested that "immediate action" be taken to "address the broader problem of . . . mishandling of consumers' personal data."[285] Reforms should aim to "put consumers back in control of both their credit reports and their personal information."[286] Successful privacy legislation must rely on an enforcement agency that would be given adequate rulemaking authority, civil penalty authority, and sufficient

277. Barrett, *supra* note 35, at 1094.
278. *Id.*
279. Balkin, *supra* note 200, at 1225.
280. *Id.*
281. *Id.*
282. *Id.* at 1227.
283. *Id.* at 1230.
284. *Equifax Data Breach*, *supra* note 56.
285. *Id.*
286. *Id.*

resources and manpower.[287] EPIC notes that with respect to consumer-facing financial institutions, although Dodd-Frank transferred authority over certain privacy provisions to the CFPB, the law did not transfer regulatory authority to establish data security guidelines.[288]

However, the FTC, the federal government's current privacy enforcement arm, is already cooperating with the CFPB.[289] In December 2019, the FTC and CFPB hosted a public workshop to discuss issues affecting the accuracy of traditional credit reports as well as employment and tenant background screening reports. Consequently, the United States should also establish a data protection agency like "virtually every other advanced economy facing the challenges of the digital age."[290] This action is necessary because "[t]he current agencies in the United States tasked with protecting consumers and citizens lack the authority and even the personnel to do what needs to be done."[291]

As to the specific structure and responsibilities of a data protection agency in the United States, one may look to the CFPB for guidance. Accordingly, a Consumer Data Protection Bureau (CDPB) would ideally function as follows. Congress should vest in the CDPB the consumer privacy protection functions of agencies like the FTC, giving the CDPB broad authority in three primary areas—rulemaking, supervision, and enforcement. The CDPB would operate as an independent bureau within the Department of Commerce, not subject to the whim of Congressional appropriations. It would be led by a single director appointed by the President and confirmed by the United States Senate. The CDPB would need adequate manpower to be effective. This enforcement force would likely need to be as large as the CFPB's 1,500 employees,[292] if not larger. The CDPB's authority would be over "covered entities" that, because of their relationship with a consumer, have taken on special duties with respect to the sensitive information they obtain in the course of this relationship.

With respect to rulemaking, the CDPB would have the power to create rules to administer, enforce, and implement federal consumer privacy protection law. Concerning its supervisory

287. Barrett, *supra* note 35, at 1110.
288. *Equifax Data Breach*, *supra* note 56.
289. Press Release, Fed. Trade Comm'n, FTC and CFPB to Host December Workshop on Accuracy in Consumer Reporting (Sept. 19, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/ftc-cfpb-host-december-workshop-accuracy-consumer-reporting.
290. *Equifax Data Breach*, *supra* note 56.
291. *Id.*
292. Lampe & Richardson, *supra* note 123, at 94.

authority, the CDPB would have the power to ensure compliance with the laws and regulations it administers by being able to require reports and examinations of entities to assess their compliance and practices with respect to consumer privacy. To protect start-ups and small businesses, the CDPB's authority could be jurisdictionally-limited to only those entities which meet a certain economic threshold, as Congress would define, focusing upon major companies whose practices implicate consumer privacy—think Google, Facebook, and Equifax. Lastly, an effective CDPB would possess significant authority in the realm of enforcement tools: (1) the power to conduct investigations; (2) the ability to bring public legal actions in federal court or an administrative forum; and (3) the ability to seek injunctive and monetary relief for violations of consumer privacy law by covered entities. Obviously, the CDPB would not be a panacea to all consumer privacy issues. However, it would be a substantial start to bringing the law into alignment with the realities of twenty-first century American life.

C. Data's "Volcker Rule"

Comprehensive consumer privacy legislation in the United States should also include its own version of the Volcker Rule to safeguard consumer data against risky corporate practices. Just as Dodd-Frank's Volcker Rule limited the extent which banks could make risky investments with its depositors' money, a Data Volcker Rule would limit the extent to which businesses could engage in risky practices with consumer data.[293] Third-party data sharing is one possible practice to monitor. Furthermore, the concept of a Data Volcker Rule is not entirely unprecedented. Consider the European Union's General Data Protection Regulation (GDPR). Under the GDPR, institutions that share personal data with third-parties either for storage or processing must ensure the third-party's compliance with the provisions of the GDPR.[294] In the United States, Apple CEO Tim Cook has called for government regulation that would advance two goals: first, increasing the difficulty of data collection by corporate entities; and, second, urging a crackdown on data brokers who transfer consumer data between companies.[295] In sum, comprehensive consumer privacy legislation should guard against "gambling" with consumers' most sensitive information.

293. Ascertaining which specific technological practices are riskier than others with respect to consumer information is beyond the scope of this article; its purpose is to provide a suggestive legislative framework for American consumer privacy law.

294. Stites, *supra* note 53, at 138.

295. Eadicicco, *supra* note 6.

CONCLUSION

Overall, American consumers face a privacy crisis in 2020. The origins of the privacy crisis share numerous parallels to the financial collapse that crippled the American and global economies in 2008. Just as Congress responded to the 2008 financial collapse with comprehensive financial services reform legislation in the form of the Dodd-Frank Act, Congress must respond to the 2020 consumer privacy crisis with comprehensive privacy reform legislation. Congress would be wise to mirror aspects of Dodd-Frank if privacy reform efforts are to succeed, such as including fiduciary obligations, the creation of a new consumer protection agency, and enabling the promulgation of rules designed to limit risky corporate practices. No single piece of legislation will be able to entirely guard against the privacy perils of twenty-first century life, just as no single piece of legislation can entirely prevent economic collapse. Consumers did not lose their privacy in a day; Congress cannot reclaim it instantaneously. However, failing to address the privacy crisis would be an even larger blunder than allowing it to develop in the first place. A Dodd-Frank approach to consumer privacy legislation is a worthy start.

Moving Fast & Breaking Things: An Analysis of Social Media's Revolutionary Effects on Culture and Its Impending Regulation

*Larissa Sapone**

* Larissa Sapone is a 2021 J.D. Candidate at Duquesne University School of Law. She graduated from the University of Pittsburgh, summa cum laude, in 2017 with a B.S. in Psychology and Administration of Justice. The author would like to thank former Duquesne Professor Agnieszka McPeak for her topic suggestion as well as family and friends for their constant support. In loving memory, this article is dedicated to Michael L. Racciato, a dear friend who unexpectedly passed away during production.

INTRODUCTION

If asked how many times a day you check your phone, you would probably answer ten, twenty, at the very greatest thirty times a day. Wrong. In fact, the reality is probably closer to the number of times you think you touch your phone subtracted from one hundred. A study by Asurion found, on average, Americans are checking their phones once every twelve minutes, roughly eighty times a day.[1] Another study found that millennials especially check their phones more than one hundred times a day, totaling five hours.[2] Supposing that individuals utilize their phones for legitimate reasons, such as work and contacting their children, is there really any explanation for spending 144 minutes a day on any given social media platform?[3] Assuming the average user starts at age ten and has a seventy-two year life span, they will spend a whopping six years and eight months on social media in their lifetime.[4]

Whether we like it or not, we now live in a digital era which has very real consequences regarding social media. Sparked by the recently proposed Social Media Addiction Reduction Technology Act (SMART Act), this article outlines the progression of social media and its (hopeful) path toward regulation.

Part I focuses on specific techniques and developments that Big Tech uses when designing their apps. Centered around the neurotransmitter—dopamine—the technology industry prides themselves on their ability to create habit-forming technology, through the use of a tried and tested three-step process.[5] This process is so successful due to its inherent capacity to exploit the psychology of the human brain.[6]

Part II details the societal impacts social media has had on the public at large. There are significant amounts of research and data available which outline the detrimental impact social media has on its user. Ironically, many executives and powerhouses that first opened the floodgates to these platforms refuse to let their children

---

1. SWNS, *Americans Check Their Phones 80 Times a Day*, N.Y. POST (Nov. 8, 2017, 4:08 PM), https://nypost.com/2017/11/08/americans-check-their-phones-80-times-a-day-study/.

2. Kari Paul, *When They're Not Eating Avocado Toast, Millennials Spend Five Hours a Day Doing This*, MKT. WATCH (May 23, 2017, 10:07 AM), https://www.marketwatch.com/story/when-theyre-not-eating-avocado-toast-millennials-spend-five-hours-a-day-doing-this-2017-05-18.

3. *Average Time Spent Daily on Social Media (Latest 2020 Data)*, BROADBAND SEARCH, https://www.broadbandsearch.net/blog/average-daily-time-on-social-media (last visited Oct. 20, 2020).

4. *Id.*

5. Smart & Grundig, *infra* note 26.

6. Allen, *infra* note 10.

use them.[7] We further dive into the manipulative way social media applications spread false information, a prevalent problem in today's political climate. This position is countered by those who believe that an addiction to technology is somewhat of a figment and instead re-direct their energy and time to more "constructive" means.

Part III highlights the regulatory debate and develops the comparison of social media to the tobacco industry. Many think social media is seemingly harmless and claim the comparison to tobacco consumption feels extreme; however, a deeper dive into their targeted cyclic mechanisms, their potential detrimental health effects, and the eerily similar trajectories they both present suggest otherwise.[8] This article concludes that, while perhaps distant, regulation in social media is as imminent as it once was in the tobacco industry.

Lastly, Part IV parses through a recently proposed legislation: the SMART Act.[9] There is a great deal of blame shifting between users and the social media platforms that have them hooked, and there is no "right answer" on how to approach the looming presence of social media in daily living. This section elaborates on the SMART Act's goals, as well as their potential downfalls; however, all hope is not lost as some developers and designers are becoming more cognizant of the products they design and are coming together to take a proactive approach.

I. THE STRATEGIC DEVELOPMENT OF HABIT-FORMING TECHNOLOGY

"How do we consume as much of your time and conscious attention as possible?": the "Kim Kardashian of molecules"—dopamine.[10] Dopamine is responsible for the feelings of pleasure, reinforcement, and activities that "promote our survival," such as eating, drinking, and sexual intercourse.[11]

---

7. *See* discussion *infra* Part II, Section A.
8. *See* MacBride, *infra* note 137; McNamee, *infra* note 148; Ou, *infra* note 135.
9. S. 2314, 116th Cong. (2019).
10. Simon Parkin, *Has Dopamine Got Us Hooked on Tech?*, THE GUARDIAN (Mar. 4, 2018), https://www.theguardian.com/technology/2018/mar/04/has-dopamine-got-us-hooked-on-tech-facebook-apps-addiction; *see* Mike Allen, *Sean Parker Unloads on Facebook: "God Only Knows What It's Doing to Our Children's Brains,"* AXIOS (Nov. 9, 2017), https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html.
11. *Speaking of Psychology: The Molecule of More: Dopamine*, AM. PSYCH. ASS'N (Mar. 2019), https://www.apa.org/research/action/speaking-of-psychology/dopamine.

To the scientific community, dopamine lies at the core of all addiction.[12] Any potentially addictive behavior triggers a release of dopamine within that circuit, thereby strengthening the desire pathway,[13] known as the dopaminergic system.[14] This system is located in the mesolimbic dopamine pathway in the brain.[15] Thus, any substance or behavior that causes this reaction becomes addictive,[16] as people find themselves constantly searching for specific ways to obtain that boost of dopamine. Another neurotransmitter—serotonin—then elicits a sense of happiness and satiates us, which inhibits our need for dopamine.[17] More dopamine equals more happiness, and happiness equals serotonin.[18] However, eventually the body inevitably needs more dopamine to attain more serotonin and create that feeling of happiness.[19] This is the cycle seen in problems of substance abuse, which is also the same cycle Big Tech exploits to attract internet users.[20] Similar to those who struggle with addiction, internet users are compelled to return, perpetually seeking out dopamine to successfully reach the serotonin levels that "tells us we are feeling good."[21]

Dopamine Labs, which has since rebranded as Boundless Mind,[22] is a technology consulting agency previously known for its involvement in creating such "persuasive technology."[23] Particularly, Dopamine Labs boasts its ability to use dopamine to boost the

---

12. *Id.*; Rosen, *infra* note 14.

13. *Speaking of Psychology*, *supra* note 11; *Know Your Brain: Reward System*, NEUROSCIENTIFICALLY CHALLENGED (Jan. 16, 2015), https://www.neuroscientificallychallenged.com/blog/know-your-brain-reward-system.

14. Larry D. Rosen, *Obsessive/Addictive "Tiny Red Dots,"* PSYCH. TODAY (Mar. 11, 2018), https://www.psychologytoday.com/us/blog/rewired-the-psychology-technology/201803/obsessiveaddictive-tiny-red-dots. *See generally Know Your Brain: Reward System*, *supra* note 13.

15. The mesolimbic pathway connects the ventral tegmental area of the brain, the principal dopamine producer, with the nucleus accumbens, an area of the brain strongly correlated with motivation and reward. *Know Your Brain: Reward System*, *supra* note 13.

16. *Speaking of Psychology*, *supra* note 11.

17. Rosen, *supra* note 14.

18. *Id.*

19. *Id.*

20. Jonathan Shieber, *Meet the Tech Company That Wants to Make You Even More Addicted to Your Phone*, TECHCRUNCH (Sept. 8, 2017 2:33 PM), https://techcrunch.com/2017/09/08/meet-the-tech-company-that-wants-to-make-you-even-more-addicted-to-your-phone/.

21. Rosen, *supra* note 14.

22. *Boundless Mind*, WELCOME AI, https://www.welcome.ai/boundless-mind (last visited Sept. 11, 2020).

23. Kyle Langvardt, *Regulating Habit-Forming Technology*, 88 FORDHAM L. REV. 129, 133 (2019) (citing B.J. FOGG, PERSUASIVE TECHNOLOGY: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO 1 (2003)). Persuasive technology is defined as an "interactive computing system designed to change people's attitudes or behaviors." B.J. FOGG, PERSUASIVE TECHNOLOGY: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO 1 (2003).

addictiveness of any given app.[24] The advertisement brags, "Dopamine makes your app addictive. Lift your engagement and revenue up to 167% by giving your users our perfect [hits] of dopamine . . ."[25] The heart of Dopamine Labs' scheme is rooted in the premise of controlling users by giving them small bursts of dopamine,[26] thereby triggering the desire pathway. Sean Parker, the founding president of Facebook, explained that the use of these persuasive technologies creates a "social-validation feedback loop" by specifically exploiting this vulnerability in human psychology.[27]

The brain does not necessarily crave one specific "feel-good" signal as much as a rhythmic pattern.[28] That is why social media platforms like Instagram and Facebook tailor the timing of their notifications in order to expressly dispense dopamine at times determined by an algorithm, which is what keeps the user coming back for more.[29] Users pick up their phones out of a compulsivity that drives them to check any given app simply because they have not checked it in a while.[30] The possibility that there may be a "tiny red dot[]"[31] that they are unaware of generates cortisol and heightens stress and anxiety.[32] Consequently, the user will succumb to their phone simply to displace that anxiety and seek relief from the rising cortisol levels.[33]

The question then becomes, how do Big Tech companies take advantage of social media users? The answer lies in the principles and value systems prioritized by these companies, which means doing everything within their power to track and understand human psychology, in an effort to exploit it and maximize engagement in their products.[34] It is obvious that money is the driving force behind

---

24. Shieber, *supra* note 20.

25. Langvardt, *supra* note 23, at 131 (alteration in original).

26. *See* Allen, *supra* note 10; Alex Hern, '*Never Get High on Your Own Supply*'*—Why Social Media Bosses Don't Use Social Media*, THE GUARDIAN (Jan. 23, 2018), https://www.theguardian.com/media/2018/jan/23/never-get-high-on-your-own-supply-why-social-media-bosses-dont-use-social-media; Virginia Smart & Tyana Grundig, '*We're Designing Minds': Industry Insider Reveals Secrets of Addictive App Trade*, CBC (Nov. 3, 2017, 5:00 AM), https://www.cbc.ca/news/technology/marketplace-phones-1.4384876.

27. Allen, *supra* note 10. Parker is now publicly sounding his alarm with the platform, asserting he does not believe he fully grasped the consequences of what the platform was doing when it first got off the ground. *Id.*

28. Jon Brooks, *Tech Insiders Call Out Facebook for Literally Manipulating Your Brain*, KQED (May 25, 2017), https://www.kqed.org/futureofyou/379828/tech-insiders-call-out-facebook-for-literally-manipulating-your-brain.

29. *Id.*

30. *Id.*

31. Rosen, *supra* note 14.

32. Brooks, *supra* note 28.

33. *Id.*

34. Hern, *supra* note 26.

Big Tech's motive.[35] Companies do not profit unless people are using the app, which is why everyone is in a "technological arms race" to keep users on their app and for the longest period of time.[36] The way to do this is by utilizing one of the most popular techniques called variable rewards, which is comprised of three steps: a trigger, an action, and a reward.[37]

The classic variable reward method can be best understood if taken one step further and broken down into four steps instead of three.[38] The process begins with the ultimate goal of habit forming technology: "[T]o solve the user's pain by creating an association so that the user identifies the company's product or service as the source of relief."[39] Entrepreneur and lecturer at Stanford Graduate School of Business and Design, Nir Eyal,[40] calls the experience of engineering desire through the use of sequential experiences "Hooks," and the more often users participate in this habit-creating cycle, the more likely they will self-trigger.[41]

A. Step One: The Trigger

Step number one is to trigger the user; this comes in two forms—external and internal.[42] An external trigger is, for example, a notification on our phone that prompts us to respond.[43] It will alert its users with an email, an app on a phone's homepage, a notification—something that "triggers" the user and begins forming these so-called "Hooks."[44] By falling victim to these Hooks time after time after time, the user will actualize associations with these internal triggers, which are, in turn, attached to pre-existing behaviors and

35. Smart & Grundig, *supra* note 26.
36. *Id.*
37. *Id.*
38. *See* Nir Eyal, *Hooked Resources & Top Articles on User Behavior*, NIR & FAR, https://www.nirandfar.com/hooked-user-behavior-resources/ (last visited Oct. 28, 2019); *see also* Langvardt, *supra* note 23, at 142. *Compare* discussion *infra* Part I, Sections A–D, *with supra* note 38 and accompanying text.
39. Langvardt, *supra* note 23, at 142 (citing NIR EYAL WITH RYAN HOOVER, HOOKED: HOW TO BUILD HABIT-FORMING PRODUCTS 52 (2014)).
40. Eyal is a graduate of the Stanford School of Business and Emory University. *About Nir Eyal & NirAndFar.com*, NIR & FAR, https://www.nirandfar.com/about-nir-eyal/ (last visited Oct. 29, 2019). He is a self-proclaimed expert in behavioral design, what he calls an intersection of psychology, technology, and business surrounding topics such as user experience and behavioral economics with some neuroscience mixed in. *Id.* An active investor in the booming technology industry, he vows to only invest in habit-forming products that improve lives. *Id.*
41. Eyal, *supra* note 38.
42. *Id.*
43. *Id.*
44. *Id.*

emotions.[45] In very little time, the internal triggers will become part of one's everyday routine, and the habit is formed.[46] The triggers will drive the user to check their phone compulsively, without any intervention.[47] Rewards of dopamine that are released following a like or a retweet are not predictable, nor do they adhere to any particular pattern, which is what drives the obsession.[48]

Every time a user has the thought, "I haven't checked my phone in a while," then reaches and picks it up, this reward system is activated. Individuals have become trained to use their phones as a "quick cure for boredom."[49] Apps such as Snapchat are built on this premise—the internal trigger tells the user to check their phone because there is a possibility that someone "snapped" them. Snapchat keeps track of the user's activity and tallies the number of consecutive snaps, flaunting the "[s]napstreak" between friends.[50] The streak, a technique known as loss aversion,[51] feeds into a well-established psychological human need to bank progress.[52] Therefore, users feel an obligation to check in daily, at the very minimum, to keep the streak.

B. Step Two: The Action

The second step is the intended action.[53] This is the tangible action the user takes by downloading, opening, and using the application.[54] It is maximized by technology companies' careful utilization of two characteristics of human behavior: motivation and ability.[55] Eyal explains that designers strive to maximize the likelihood that users take the intended action, which is done by both heightening motivation and simultaneously making it as easily accessible for the user.[56] The ideal user "should be able to act without stopping

45. *Id.*
46. *Id.*
47. Langvardt, *supra* note 23, at 142–43.
48. Smart & Grundig, *supra* note 26.
49. Langvardt, *supra* note 23, at 143.
50. David Brooks, *How Evil Is Tech?*, N.Y. TIMES (Nov. 20, 2017), https://www.nytimes.com/2017/11/20/opinion/how-evil-is-tech.html?searchResultPosition=1; Langvardt, *supra* note 23, at 143; Smart & Grundig, *supra* note 26.
51. Smart & Grundig, *supra* note 26.
52. Haley Sweetland Edwards, *You're Addicted to Your Smartphone. This Company Thinks It Can Change That*, TIME (Apr. 13, 2018, 10:28 AM), https://time.com/5237434/youre-addicted-to-your-smartphone-this-company-thinks-it-can-change-that/.
53. Eyal, *supra* note 38.
54. Langvardt, *supra* note 23, at 143.
55. Eyal, *supra* note 38.
56. *Id.*

to think before doing so."[57] If a developer is successful in the design, the user-to-action barrier should be as low as possible.[58]

As a result of this process, newsfeeds have now coined the term "bottomless bowls."[59] In a Cornell study, those participants served a "bottomless" bowl of soup neither believed they had consumed more, nor felt that they were satiated.[60] Likewise, this same mechanism corresponds to what occurs as users open their apps—without ever presenting a need to physically click a button, new information will load continuously as the user scrolls,[61] making the user exert the least amount of effort. If there is an infinite bowl of content, users will never think they have seen enough.

C. Step Three: The Reward

Step three is the point at which the user is finally rewarded. The distinctive characteristic of Hooks is that they are based off of a series of unpredictable variable rewards, making it the technology companies' biggest weapon.[62] Simply a reward that varies on a random basis, it is the core behind addictions, such as gambling, gaming, and social media; classic examples are slot machines and the "pull [down] to refresh" feature.[63] The reason this cycle sets itself apart from other loops is the built in unpredictability.[64] The best of app developers will even go so far as using artificial intelligence to predict the best time to reward users based on collected data.[65] It would not be nearly as fun or exciting to open an app, pull down to refresh, and know exactly what you were going to see. As Eyal explains, no one likes boring, and predictability does not create desire.[66]

---

57. Langvardt, *supra* note 23, at 143.
58. *Id.*
59. *Id.*
60. Four participants were instructed to taste-test a new tomato soup recipe. Brian Wansink et al., *Bottomless Bowls: Why Visual Cues of Portion Size May Influence Intake*, 13 OBESITY RSCH. 93, 95 (2005). Two participants received a normal bowl of tomato soup and two participants received a self-refilling bowl of soup. *Id.* The self-refilling bowl consisted of a regular restaurant style bowl connected to a corresponding tube underneath the table linking it to the pot of soup. *Id.* at 95–96. Using a gravity mechanism, as each bite was taken the bowl would refill, unapparent to the diner's eye. *Id.* at 96.
61. Langvardt, *supra* note 23, at 143; Brooks, *supra* note 28.
62. Eyal, *supra* note 38.
63. Langvardt, *supra* note 23, at 144.
64. Eyal, *supra* note 38.
65. Smart & Grundig, *supra* note 26.
66. Eyal, *supra* note 38.

D. Step Four: The Investment

Last, step four is the investment phase, where the user becomes "internally triggered."[67] This is the phase that requires the user to put in some work after obtaining a variable reward.[68] In this phase, Eyal describes two goals the designers are focused on: (1) increasing the odds the user will continue the cycle when presented with the next trigger;[69] and (2) asking the user to contribute something to this cycle when they are the most vulnerable, after receiving heavy doses of dopamine.[70]

The investment phase is what fuels the fire and restarts the cycle.[71] For example, the user will post a picture to Facebook, Instagram, or Snapchat and constantly check and re-check their post multiple times. This act is driven by the compulsive need to see if there is a like—if so, how many—or a comment—if so, what does it say.[72] Examining further, one user's investment can be used as a weapon to entice other users into the cycle.[73] For example, Megan posts a group picture from "Girls Night Out" of herself with Sarah, Jenna, and Allison. Sarah, Jenna, and Allison all get notifications via the "tiny red dot[],"[74] the external trigger, that a picture of them has been posted. Now they will all feel the same compulsion Megan feels that internally triggers them to check that post too.[75] The investment into this process can be viewed as a tool that will improve the users' experience the next time they use the app, like adding new friends or tailoring a profile's features.[76] By strategically designing and implementing these four steps into apps, the developers have created a system to keep users engaged.

The average user most likely does not even realize the aforementioned process is happening. If true, it reinforces the power Big Tech has over its users. The speed at which social media platforms have become such a dominant part of every-day life is alarming. At the very minimum, being cognizant of the process through which it occurs allows the user to regain some of the power that these platforms have over them.

---

67. Langvardt, *supra* note 23, at 145.
68. *Id.*
69. Eyal, *supra* note 38.
70. *Id.*
71. Langvardt, *supra* note 23, at 145.
72. *Id.*
73. *Id.*
74. Rosen, *supra* note 14.
75. *See* Langvardt, *supra* note 23, at 145.
76. Eyal, *supra* note 38.

II. THE IMPACT OF HABIT-FORMING TECHNOLOGY, SPECIFICALLY SOCIAL MEDIA, ON SOCIETY

A. The Detrimental Effects Seen in Society

App developers have accomplished their jobs and continue to thrive. Certain instances have shown that society's increasing use of persuasive technology, specifically social media, is not always negative.[77] A 2018 PEW Research Center study surveyed teens between ages thirteen to seventeen and found 81% felt more connected to their friends, 69% felt social media aided in more diverse social interaction, and 68% felt as though they have people who will support them through tough times.[78]

Since the development of various social media platforms are relatively new, the impact it has on its users is still largely unconfirmed, yet some social media developers are starting to acknowledge the harms social media causes and refuse to use their own carefully crafted technology.[79] Neither Mark Zuckerberg, notorious Facebook creator, nor any of the company's key executives maintain a typical social media presence, if they even maintain one at all.[80] Even as the founding president of Facebook, Sean Parker remains "something of a conscientious objector" to social media.[81] These moguls have recognized that by creating these platforms they were exploiting a vulnerability in humans and deliberately chose to do it anyway;[82] some have even gone as far saying "[they] have created tools that are ripping apart the social fabric of how society works . . . ."[83]

These platforms are largely found to affect mental health most severely.[84] The overwhelming majority of research has generally

---

77. For example, a number of studies have found positive associations with the use of social media as a way to bridge gaps in communication—allowing them to feel more connected to those in their lives, providing a support system in times of difficulty, and giving them a comprehensive outlet to reach out to large and diverse populations. *See generally* Deborah Richards et al., *Impact of Social Media on the Health of Children and Young People*, 51 J. OF PEDIATRICS & CHILD HEALTH 1152, 1154 (2015); Monica Anderson & JingJing Jiang, *Teens' Social Media Habits and Experiences*, PEW RSCH. CTR. (Nov. 28, 2018), https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/.

78. Anderson & Jiang, *supra* note 77.

79. *See* Hern, *supra* note 26.

80. *Id.*

81. *Id.*

82. *Id.*

83. James Vincent, *Former Facebook Exec Says Social Media Is Ripping Apart Society*, THE VERGE (Dec. 11, 2017, 6:07 AM), https://www.theverge.com/2017/12/11/16761016/former-facebook-exec-ripping-apart-society.

84. Holly B. Shakya & Nicholas A. Christakis, *A New, More Rigorous Study Confirms: The More You Use Facebook, the Worse You Feel*, HARV. BUS. REV. (Apr. 10, 2017),

concluded that "daily overuse of various forms of media and technology has a negative effect on the health of all children, preteens and teenagers, which in turn, makes them more prone to psychological disorders like anxiety, depression, and others."[85]

Research studying the relationship between liking content/reacting to posts and well-being showed the two were consistently related to a compromised well-being,[86] ultimately associating overall well-being positively with real-world social networks, and negatively with the networking used in Facebook.[87] This likely stems from a common misconception that social interaction on social media is a replacement for real world interaction, which is certainly not the case.[88]

The dangers associated with social media are not only limited to an adolescent's mental health but also affects other aspects of their lives, such as their academic performances and interpersonal relationships.[89] In addition to a new phenomenon known as "Facebook depression,"[90] these major risks are seen most prominently in cyberbullying,[91] sexting,[92] and improper use of technology.[93]

---

https://hbr.org/2017/04/a-new-more-rigorous-study-confirms-the-more-you-use-facebook-the-worse-you-feel.

85. Richards et al., *supra* note 77, at 1153*; see also* Catriona Morrison & Helen Gore, *The Relationship Between Excessive Internet Use and Depression: A Questionnaire-Based Study of 1,319 Young People and Adults*, 43 J. PSYCHOPATHOLOGY 121, 121 (2010) (linking excessive Internet use to high levels of depressive symptoms); Maarten H.W. Selfhout et al., *Different Types of Internet Use, Depression and Social Anxiety: The Role of Perceived Friendship Quality*, 32 J. ADOLESCENCE 819, 830 (2009) (finding non-communication based Internet use has detrimental effects on adolescents' depression and anxiety).

86. Holly B. Shakya & Nicholas A. Christakis, *Association of Facebook Use with Compromised Well-Being: A Longitudinal Study*, 185 AM. J. EPIDEMIOLOGY 203, 210 (2017).

87. Shakya & Christakis, *supra* note 84. The team included real-world network measures, adjusted for baseline Facebook use and accounted for the participants' level of initial well-being, initial real-world networks, and initial level of Facebook use, ultimately reaching the same conclusion. *Id.*

88. *Id.*

89. Kalika Gupta, *What Is Social Media? How Is It Affecting Adolescent's Mental Health?*, 2 EUR. J. BIOMEDICAL & PHARM. SCI. 410, 410 (2015).

90. Facebook depression is defined as "depression that develops when preteens and teens spend a great deal of time on social media sites, such as Facebook, and then begin to exhibit classic symptoms of depression." Gwenn Schurgin O'Keeffe et al., *The Impact of Social Media on Children, Adolescents, and Families*, 127 AM. ACAD. PEDIATRICS 800, 802 (2011) (citing Gupta, *supra* note 89, at 410).

91. Cyberbullying is defined as "deliberately using digital media to communicate false, embarrassing or hostile information about another person. It is the most common online risk for all young people and is a peer-to-peer risk." Richards et al., *supra* note 77, at 1153.

92. Sexting is defined as "sending, receiving, or forwarding sexually explicit messages, photographs, or images via cell phone, computer, or other digital devices." Schurgin O'Keeffe et al., *supra* note 90, at 802. The rapid distribution of this information can be seen as a form of cyberbullying. *Id.*

93. Gupta, *supra* note 89, at 411.

In fact, privacy can pose one of the greatest threats to adolescents on social media.[94] Young teenagers on social media sites often do not comprehend the repercussions behind what they post online, putting everyone's privacy at risk with complete disregard that "what goes online stays online."[95] These actions, and every action adolescents take on social media sites leave behind a "digital footprint"—an ongoing record of one's web activity.[96] One inappropriate post could jeopardize a user's entire future or career; usually adolescent users are too immature to realize that everything they place on the internet can haunt them.

There have also been severe societal repercussions, such as a new strain on social norms and the degradation of public discourse.[97] The average user's compulsivity to constantly check their phones and their subsequent social media apps has contorted the views of what are now commonly accepted social norms.[98] For example, it is now a commonality for people to eat entire meals together behind their phones, stopping mid-conversation to reply to messages and such.[99] As a result, studies are showing declines in productivity rates, empathy, and intelligence in general when people are around this technology.[100]

Of the societal harms, the effect on the public sphere, is arguably the most severe of all.[101] Today's social media platforms have developed a way to strategically survey the users to constantly adapt the content to the users' emotional needs.[102] Through the use of these algorithms, social media sites are tailoring what information is shown to the user based on their previous history.[103] In essence, the user does not need to find the content they desire—content will find them.[104] This process creates the illusion that the user is molding their own feed; however, in reality, this algorithm uses "revealed preferences" and carves out the interests, values, and opinions of the user.[105] So while you think you are choosing the articles you see on Facebook and the YouTube videos you click on, they are actually already chosen for you.

---

94. *Id.*
95. *Id.*
96. *Id.*
97. Langvardt, *supra* note 23, at 146.
98. *Id.* at 147.
99. *Id.*
100. *Id.* at 148.
101. *Id.*
102. *Id.* at 149.
103. *Id.* at 150.
104. *Id.*
105. *Id.*

Facebook's manipulative platform use is not a new trend, and, in fact, they have been highly scrutinized in the past for a covert study conducted for one week in January 11–18, 2012, in which they either positively or negatively altered the feed of their (unknowing) users and examined how it affected the users emotions, ultimately finding a phenomena called "emotional contagion."[106] Facebook was immensely criticized after it was revealed that they did not receive informed consent from any of the users who participated in the study.[107] In fact, many spoke up arguing that their dirty little experiment had real potential to harm participants.[108] Most importantly, it was highlighted that simply agreeing to Facebook's privacy terms does not give them the type of authorization that translates to informed consent.[109]

1. How Social Media Perpetuates the Spread of False Information: Deep Fakes

Algorithms are now the driving force behind a common political weapon that is utilized by social media users: Deep Fakes. Deep Fakes are a form of digital impersonation that use "machine-learning algorithms to insert faces and voices into video and audio recordings of actual people and enables the creation of realistic impersonations," resulting in videos, audio clips, or pictures making it seem as if that depicted person actually said or did the thing portrayed.[110] In fact, their realistic nature can make it extremely difficult to differentiate fake from reality.[111]

---

106. Charles Arthur, *Facebook Emotion Study Breached Ethical Guidelines, Researchers Say*, THE GUARDIAN (June 30, 2014), https://www.theguardian.com/technology/2014/jun/30/facebook-emotion-study-breached-ethical-guidelines-researchers-say; *see* Kashmir Hill, *Facebook Manipulated 689,003 Users' Emotions for Science*, FORBES (June 28, 2014, 2:00 PM), https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#7d8145ca197c. Users' emotions were measured according to the content of their posts during the time their feed was being altered. Hill, *supra* note 106. Results found that, on average, when positive content was displayed less frequently, people were less likely to post positive statuses. *Id.* Reduced negative content resulted in fewer negative posts. *Id.* Further, a decrease in all emotional content on a user's feed ultimately led to a "less expressive" user who posted less often. *Id.*

107. Arthur, *supra* note 106.

108. *Id.*

109. *Id.* It is an agreed upon tenet within the realm of research that before any research begins, informed consent must be obtained; this was not the case here. *Id.* It is the researcher's ethical obligation to guarantee that informed, voluntary consent has been given from every participant. *Id.* According to others, this standard was largely deviated from by Facebook. *Id.* Agreeing to the website's terms of use does not constitute consent in the same ethical way as would the users' knowing consent to participate in the study. *Id.*

110. Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1758 (2019).

111. *Id.* at 1759.

Social media platforms play a huge role in contributing to "the content of today's angry tribal politics," ultimately cultivating and spreading Deep Fakes.[112] Such a politically charged, fast-acting environment is kindling for a wildfire like a Deep Fake. As explained by the authors of *Deep Fakes*, "the networked environment blends the few-to-many and many-to-many models of content distribution, democratizing access to communication to an unprecedented degree."[113]

The way social media platforms exacerbate the effect of Deep Fakes on the internet is best understood as a snowball effect. It begins with "'information cascade' dynamic[s]," which result when users stop paying attention to their own information and rely on others as a credible source of information.[114] Furthermore, users have a natural urge to perpetuate negative information since that is what tends to catch the eye.[115] This culminates into what users often create and are known as "filter bubbles" which are bubbles of information that confirm preexisting beliefs.[116] Because people share the information they agree with, whether true or not, these bubbles further accelerate the spread of false information .[117]

For example, consider that a user shares a politically fueled Deep Fake. This results in a filter bubble that is continuously shared because not only does the user not check its legitimacy, but they also want to post something that corresponds to their political views. After enough clicks, likes, and shares of similar information, this leads to a personally and emotionally tailored newsfeed. In the presence of the aforementioned algorithms, the only content that the user will see corresponds with their respective political view and emotions behind it. These skillfully crafted mechanisms seamlessly go hand in hand.

112. *See* Langvardt, *supra* note 23, at 149; *see also* Chesney & Citron, *supra* note 110, at 1766.
113. Chesney & Citron, *supra* note 110, at 1764.
114. *Id.* at 1765.
115. *See id.* at 1766.
116. *Id.* at 1768.
117. *Id.*

B. Is "Big Tech" as Addictive as Everyone Says It Is?

For most people, the answer is "yes;"[118] however, a small sample, mainly Nir Eyal,[119] believes it is "ridiculous"[120] that people buy into the theory of social media addiction and instead promotes the foundation of his new book *Indistractable: How to Control Your Attention and Choose Your Life*.[121] Eyal believes "the answer to digital distraction lies in individuals learning to exercise forethought and discipline, not demonizing companies that make products people love."[122]

Accordingly, the best way to approach addictive technology is to confront and understand the psychology of distraction and how to overcome it.[123] The premise behind *Indistractable* is based on the equal and opposing pillars of traction and distraction.[124] As explained earlier, users' actions are prompted by internal and external triggers.[125] Every action either moves us closer toward our goals (traction) or further away from our goals (distraction).[126] A majority of users act out of a desire to escape real life but by using specific techniques, such as consciously stopping themselves from reaching for their phones, and careful planning—this impulsive behavior is avoidable and will allow people to "retrain and regain [their] brains."[127] For example, Eyal has his daily schedule planned and allocated into fifteen to thirty-minute increments.[128] His schedule includes everything from checking certain social media accounts to having dinner with his wife.[129]

---

118. True addiction is applicable to only a relatively small percentage of "problem users" that develop such a serious habit. Langvardt, *supra* note 23, at 146. Those in the Big Tech industry claim they should not be held responsible for those users that struggle with impulse control and are therefore more prone to behavioral addictions. *Id.* However, as discussed above, those in the industry have also made it very clear that those developing persuasive technology do so in a highly exploitative way with a strong incentive to do so. *Id.* at 146–47.

119. *See supra* note 40 and accompanying text.

120. Ezra Klein, *Is Big Tech Addictive? A Debate with Nir Eyal*., VOX (Aug. 7, 2019, 11:00 AM), https://www.vox.com/podcasts/2019/8/7/20750214/nir-eyal-tech-addiction-ezra-klein-smartphones-hooked-indistractable.

121. NIR EYAL WITH JULIE LI, INDISTRACTABLE: HOW TO CONTROL YOUR ATTENTION AND CHOOSE YOUR LIFE (2019).

122. Klein, *supra* note 120.

123. Barnaby Lashbrooke, *Nir Eyal: Instead of Complaining Your Phone Is Addictive, Become 'Indistractable,'* FORBES (Sept. 17, 2019 10:01 AM), https://www.forbes.com/sites/barnabylashbrooke/2019/09/17/nir-eyal-tech-addiction-isnt-real-you-just-need-to-be-indistractable/#617896bb1079.

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*

The goal is to give users the tools to learn how to become "indistractable" and benefit from the ever-present technology.[130] The main theme begins with the distinction between addiction and overuse. Addiction is pathology, overuse is not.[131] Removal of any one of the essential elements required for diagnosis[132] is no longer an addiction; it is simply overuse and referring to it as an addiction is giving Big Tech more credit than is justified.[133]

In a user's mission to becoming "indistractable," these five techniques serve to help "regain control over our attention, our time, and our life": (1) plan your day—not with a to-do list but with a timed schedule devoted to each task; (2) use social media and email at set times; (3) surf the urge—be conscious and notice the sensations you are experiencing, allowing them to peak and feeling the uncomfortableness of the trigger, and then subsequently pass; (4) be aware of liminal moments (i.e., those times transitioning from one task to another); and (5) you are not powerless—do not buy into the "there's nothing we can do" hoax.[134]

III. SOCIAL MEDIA OR BIG TOBACCO: IS SOCIAL MEDIA FOLLOWING THE SAME PATH OF REGULATION SEEN IN THE CIGARETTE INDUSTRY?

If tobacco companies are required to make product disclosures and open their facilities to inspection,[135] then it only seems fitting that Facebook, Twitter, and Instagram must go public with their code. These two creations, social media and tobacco, are not too far removed from each other when considering their potential lasting effects.

A look into the past reveals that in the 1950s and 1960s, nearly fifty percent of all United States adults were habitual smokers.[136] This sharply contrasts the number seen today, less than half that,

130. *See* Klein, *supra* note 120.

131. *Id.*

132. Eyal describes these essential elements as: (1) a predilection for addiction; (2) the product; and (3) a pain that cannot be healthily dealt with otherwise. *Id.*

133. *Id.*

134. Nir Eyal, *5 Ways to Distraction-Train Your Mind*, NIR & FAR, https://www.nirandfar.com/distraction-proof/ (last visited Sept. 13, 2020); *see also* Klein, *supra* note 120.

135. Elaine Ou, *Time to Treat Facebook Like Big Tobacco*, JAPAN TIMES (May 20, 2019), https://www.japantimes.co.jp/opinion/2019/05/20/commentary/world-commentary/time-treat-facebook-like-big-tobacco/#.XYbmSZNKiRt.

136. *See generally* U.S. DEP'T OF HEALTH & HUM. SERVS., THE HEALTH CONSEQUENCES OF SMOKING—50 YEARS OF PROGRESS: A REPORT OF THE SURGEON GENERAL, FIFTY YEARS OF CHANGE 1964–2014 (2014), https://www.ncbi.nlm.nih.gov/books/NBK294310/.

at merely 17.8%.[137] Throughout the early decades of the 1900s, warnings about tobacco and the increased risk of cancer and lung disease were surfacing;[138] however, as these concerns increased, so did the tobacco industry's carefully devised strategies to counter the scientific evidence that was a threat to their empire.[139] This resulted in a decade-long battle in which the tobacco industry tirelessly followed strategies to discredit those threats by "denying the harms of its products, discrediting the scientific evidence that showed these harms, funding research that was intended to divert attention from cigarettes, and marketing new products with implied lower risks than existing products . . . ."[140] Any attempts at regulation were concerned mainly with protecting consumers from misleading advertising and as long as this facet was satisfied, the medical community chose not to engage.[141]

While not entirely unprecedented, the laissez-faire approach to the tobacco industry came to a halt upon the publication of the 1964 Surgeon General's report.[142] The main finding emphasized the causal relationship between smoking and lung cancer for both men and women; the effects of cigarette smoking significantly outweighing all other potential factors.[143] Similarly, it was also determined that cigarette smoking played a substantial role in mortality as it related to specific diseases and overall death rate.[144] In sum, the general consensus from the report concluded, "[c]igarette smoking is a health hazard of sufficient importance in the United States to warrant appropriate remedial action . . . ."[145] Therefore, after decades of a combination of researched evidence, regulation, and numerous lawsuits against the tobacco industry, the smoking rate finally began to wane.[146]

---

137. Elizabeth MacBride, *Is Social Media the Tobacco Industry of the 21st Century?*, FORBES (Dec. 31, 2017, 3:56 PM), https://www.forbes.com/sites/elizabethmacbride/2017/12/31/is-social-media-the-tobacco-industry-of-the-21st-century/#3acd82357011.

138. U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 136.

139. *Id.*

140. *Id.* (citation omitted).

141. *Id.*

142. *See id.* Reports indicate that around thirty million smokers quit following the release of the 1964 Surgeon General's report. *Id.*

143. *Id.*

144. *Id.* This report established a precedential approach not only for the Surgeon General report, but reviews of reports in other fields as well. *Id.* The in-depth analysis and methodology were conducted by carefully selected professionals best considered to be free of any bias. *Id.* The committee evaluated five criteria in distinguishing causation from association: consistency, strength, specificity, temporal relationship, and coherence. *Id.*

145. *Id.* (citation omitted).

146. MacBride, *supra* note 137.

Today, social media is considered "more addictive than cigarettes and alcohol . . . [i]t is no longer possible to ignore it when talking about young people's mental health issues."[147] Placing regulations on social media, just as the tobacco industry has implemented, has become an increasing topic of debate.[148] Cigarettes and social media networks have many parallels; they are both products, they both contain substantial harms,[149] and ultimately, they are both industries comprised of "corporations that make billions of dollars peddling a destructive addiction."[150]

Therefore, it seems appropriate to regulate social media in the same way that cigarettes are regulated.[151] An active executive in the technology industry, Marc Benioff, believes regulation in this industry is unavoidable[152]—comparing the technology industry to others, it is no different from the financial services or food industry,[153] which means utilizing the combination of education and regulation.[154] Yet, just as the tobacco industry was able to rely on its extremely influential lobby to keep it successful in times of desperation,[155] it is not unimaginable that the technology industry, all wrapped up in the Silicon Valley, would not also have similar clout.

A pivotal difference and a key obstacle between regulation of cigarettes and social media lies in the market and its competition.[156] When the tobacco industry was heavily thwarted in the United States, it was able to consolidate, create new technology, and develop growth in other countries that lacked structures able to compete with the tobacco industry.[157] Social media platforms are not as fortunate. In these expansive global markets, social media is countered with "stiff competition and incredibly fluid markets."[158] Consequently, where social media faces regulation in the United States, there will always be another market in which it can thrive that it does not have to face such inconveniences. As a result, these

147. *Id.*
148. *See generally* Roger McNamee, *Why Not Regulate Social Media like Tobacco or Alcohol?*, THE GUARDIAN (Jan. 29, 2018), https://www.theguardian.com/media/2018/jan/29/social-media-tobacco-facebook-google; MacBride, *supra* note 137; Ou, *supra* note 135.
149. Alex Hern, *Facebook Should Be 'Regulated like the Cigarette Industry,' Says Tech CEO*, THE GUARDIAN (Jan. 24, 2018), https://www.theguardian.com/technology/2018/jan/24/facebook-regulated-cigarette-industry-salesforce-marc-benioff-social-media.
150. Brooks, *supra* note 50.
151. Hern, *supra* note 149.
152. *Id.*
153. *Id.*
154. McNamee, *supra* note 148.
155. MacBride, *supra* note 137.
156. *Id.*
157. *Id.*
158. *Id.*

industries will migrate, and technology will develop faster in markets where it does not have to adhere to rigid regulation.[159]

Even those who have braved the challenge of regulation have shown the inadequacies in its capabilities.[160] Some argue that the only solution to this monopolized industry is not creating better competitors but, instead, reducing our dependency on the competitors.[161] It took decades of attempted regulations and public health movements until the government took action against the tobacco industry,[162] making it difficult to predict if, and when, social media will meet a similar fate.

IV. THE SMART ACT

A. Aims and Goals of the SMART Act

Missouri Republican Senator Josh Hawley[163] recently proposed a counter to the "parasite on productive investment"[164] that is social media, the Social Media Addiction Reduction Technology Act (SMART Act). The goal of Hawley's master plan: "[t]o prohibit social media companies from using practices that exploit human psychology or brain physiology to substantially impede freedom of choice, to require social media companies to take measures to mitigate the risks of internet addiction and psychological exploitation, and for other purposes."[165] The Findings section of the SMART Act specifies that (1) internet companies, particularly social media, concern themselves only with capturing as much of their users' attention as possible; (2) they accomplish this by designing their platforms in ways that exploit human psychology and physiology; and (3) as a result of this exploitation, this impedes users' free choice.[166]

Among others, the main tenets of the SMART Act (1) disallow social media companies from implementing design techniques such as infinite scroll, auto play, badges or awards; (2) require platforms to limit available content after a certain amount of time adding

159. *Id.*

160. For example, the European Union, which has implemented the necessary regulations into their political framework, recently issued a judgment against Google for 2.7 billion dollars for "anti-competitive [behavior]," barely leaving a sting to Google. McNamee, *supra* note 148.

161. Ou, *supra* note 135.

162. *Id.*

163. *See infra* notes 168–170 and accompanying text.

164. Emily Stewart, *Josh Hawley's Bill to Limit Your Twitter Time to 30 Minutes a Day, Explained*, VOX (July 31, 2019, 4:20 PM), https://www.vox.com/recode/2019/7/31/20748732/josh-hawley-smart-act-social-media-addiction.

165. S. 2314, 116th Cong. (2019).

166. S. 2314 § 1.

"natural stopping points;" (3) create a neutral process surrounding consent terms to make the accept and deny boxes both identical and easily accessed; and (4) ultimately keep track of time spent on platforms, limiting it to thirty minutes a day.[167]

Hawley can best be described as a self-proclaimed "'anti-tech' crusader."[168] The Senator takes an aggressive standpoint when it comes to social media.[169] In fact, this is not Hawley's first strike at taking down Big Tech.[170] In addition to the SMART Act, he has also proposed legislation attempting to regulate and limit data tracking as well.[171]

B. The Drawbacks

Hawley is eager, but he continues to be met with much disapproval and a heavy pushback. Many are critical that the bill lacks nearly enough statistical data to bridge such a large gap in its attempt at regulation.[172] While this article has elaborately detailed the horrors of social media, it is most important to take everything said lightly; no one should just accept information before gathering their own facts, conducting an analysis, and drawing individual conclusions. Barely thirteen years old, it is important to remember that smartphones, and consequently social media, are an invention of the new age.[173] If and when regulation does occur, it will realistically take much longer than thirteen years for Congress to

---

167. S. 2314 § 3. Do not worry about this requirement. Users can change this in their settings; however, at the beginning of every month it automatically resets back to the thirty-minute limit. Larry D. Rosen, *The SMART Act*, PSYCH. TODAY (Aug. 8, 2019), https://www.psychologytoday.com/us/blog/rewired-the-psychology-technology/201908/the-smart-act; Stewart, *supra* note 164.

168. Visioneer Digital Marketing Agency, *How Hawley's SMART Act May Impact Social Media Companies*, VISIONEERIT (Sept. 6, 2019, 8:54 PM), https://www.visioneerit.com/hawley-smart-act/.

169. *See* Josh Hawley, *We Might Be Better Off if Facebook, Instagram and Twitter Vanished: Sen. Josh Hawley*, USA TODAY (May 23, 2019, 10:52 AM), https://www.usatoday.com/story/opinion/2019/05/22/facebook-instagram-twitter-do-more-harm-than-good-column/3751735002/. Senator Hawley has made various statements illustrating his stance such as, "social media is best understood as a parasite on productive investment . . . ." *Id.* "We are . . . more impoverished, lonely, and despairing." *Id.* "Maybe we'd be better off if Facebook disappeared." *Id.*

170. *See generally* The DASHBOARD Act, S. 1951, 116th Cong. (2019); Do Not Track Act, S. 1578, 116th Cong. (2019). Both legislations are unlikely to pass. *See also* Lauren Feiner, *Two Senators Want Social Media Firms to Tell Users How Much Their Data Is Worth*, CNBC (June 24, 2019, 1:16 PM), https://www.cnbc.com/2019/06/24/sens-hawley-and-warner-take-aim-at-big-tech-with-the-dashboard-act.html.

171. *See generally* S. 1951; S. 1578.

172. Rosen, *supra* note 167; Stewart, *supra* note 164; Adam Thierer & Andrea O'Sullivan, *The Not-So-SMART Act*, THE BRIDGE (July 31, 2019), https://www.mercatus.org/bridge/commentary/not-so-smart-act.

173. Rosen, *supra* note 167.

approve. The data on this relationship rapidly continues to grow; however, there is a substantial difference between causational data and correlational data that cannot be undermined, the former of which Hawley failed to include in his proposal.[174]

Another group of skeptics side with Eyal and take the stance that approaching this as a way to regulate an "addiction" seems perhaps a bit extreme.[175] In fact, some say the "issue may be overblown."[176] The reality of a social media addiction is still largely discussed in the scientific community, and many have different stances.[177] To some academics, the fact that it has not been recognized by the Diagnostic and Statistical Manual of Mental Disorders V (DSM V) is enough to discount it as an applicable theory.[178] Some of the most prominent indicators of addiction include building of tolerance, neglect of other basic aspects of one's life, and dishonesty; however, the research is more suggestive that our reactions to social media stem from anxiety instead.[179] Therefore, FOMO—Fear of Missing Out—makes us check our phones, not an addiction.[180]

Perhaps the most disfavored aspect of the SMART Act is what makes it so different from typically proposed legislation: the impositions of the regulations themselves.[181] The SMART Act aims to force limits on the users themselves, that is, by limiting their time on social media to thirty minutes and reducing their browsing.[182] This is vastly different from other, potentially more successful legislation, which aims at placing limits on the social media platforms and those designers.[183] The opposition to user regulation compared to developer regulation implicates the First Amendment argument that these platforms and content forms are all protected.[184] Therefore, rejections will far exceed any successful attempts at regulation aiming to control the user's choice.

---

174. *Id.*
175. *Id.*; Stewart, *supra* note 164; Thierer & O'Sullivan, *supra* note 172.
176. Thierer & O'Sullivan, *supra* note 172.
177. Stewart, *supra* note 164.
178. *Id.* University of Oxford psychologist, Anthony Przybylski, is one such skeptic and believes the only way we would ever obtain conclusive results regarding social media addiction, would be upon social media companies' participation in "transparent studies with independent scientists . . . ." *Id.*
179. Rosen, *supra* note 167.
180. *Id.*
181. Visioneer Digital Marketing Agency, *supra* note 168.
182. *Id.* However, these are not extremely alarming to the average user since they have the ability and control to eliminate these features in their settings. *See supra* note 168 and accompanying text.
183. Visioneer Digital Marketing Agency, *supra* note 168.
184. Thierer & O'Sullivan, *supra* note 172.

Social media companies have met this proposal with just as much, if not more, pushback than users.[185] If passed, the SMART Act would become a logistical nightmare. In just three short months after its enactment, social media companies would predictably enter into a frenzy of regulatory prep, putting serious work into significantly changing their platforms in ways that comply with regulations.[186] They would also need to continue to be presumably as enticing and aesthetically pleasing to the user. Not only is there risk that this could be financially taxing, but it also would be damaging to their status as a whole, upsetting users for eliminating these coveted features.[187] Eventually, in the quick turnaround time of six months post-enactment, platforms are expected to fully comply with all the listed requirements.[188] Failure to make themselves SMART Act-friendly could leave them answering to the commission, as well as the Attorney General's office.[189]

There are some proponents of social media who claim its risks are not detrimental. There is a reality of people who are not so obsessively and compulsively "addicted" to their social media. So why punish all for the mistakes of one? For example, Duolingo offers the same type of badges the SMART Act is trying to ban;[190] however, Duolingo is a learning platform that teaches and encourages people to learn a particular language.[191] This is most likely not the "parasite on productive investment"[192] Senator Hawley was referring to. Or what about parents letting their children watch kid-friendly shows on auto play on the iPad so that Mom and Dad can actually accomplish some work from the office or chores around the house?[193] Surely, this cannot be what Senator Hawley had in mind when he set out on his anti-tech crusade.[194]

It is clear there are many issues to work through regarding Hawley's logic. And as with every other widely debated issue, everyone holds different stances regarding what is "best." To a degree, some are right. Why does Senator Hawley get to decide what is "socially beneficial" and what is not?[195] With only a twenty-one percent

185. Visioneer Digital Marketing Agency, *supra* note 168.
186. *Id.*
187. *Id.*
188. *Id.*
189. *Id.*
190. Thierer & O'Sullivan, *supra* note 172.
191. *Id.*
192. Hawley, *supra* note 169.
193. Thierer & O'Sullivan, *supra* note 172.
194. Visioneer Digital Marketing Agency, *supra* note 168.
195. Thierer & O'Sullivan, *supra* note 172.

chance of even passing through the first committee hearing,[196] the SMART Act is not the path to regulation for the reasons detailed above. However, it is equally unlikely that social media will remain regulation free forever. Looking at regulation from a different perspective is perhaps a better way to implement change.

C. The Grassroots Movement

It is hard to place all blame on social media companies for the way that they have crafted their product. After all, why would they not want to design a product in the most efficient way. Yet, responsibility needs to be taken to assure that companies are mindful of the evils that the social media industry has tapped into and abused.

Successful attempts at regulation will spearhead through the use of a grassroots movement;[197] those that start at the bottom and work up; those individuals who work to create a sense of mindfulness and responsibility, first and foremost in the app designers. The proposals will be aimed at the creators of Facebook, Instagram, and Twitter, rather than the users of these apps.

In fact, a growing nonprofit now gaining traction is "Time Well Spent," which urges technology companies to put the users' best interests first and their skillfully crafted platforms second.[198] Time Well Spent is fundamentally rooted in the hopeful theory of changing software design.[199] Their mission is clear: "to drive a comprehensive shift toward humane technology that supports our well-being, democracy, and shared information environment."[200]

---

196. *116 Legislative Outlook S. 2314*, LEXIS ADVANCE RES., https://advance.lexis.com/document/documentlink/?pdmfid=1000516&crid=e27b8c86-965b-4bf7-9971-91392180c558&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A5WPM-WB21-F5T5-M2TC-00000-00&pdcontentcomponentid=133053&pddoctitle=Legislative+Outlook+in+detail&pdpurchaseitemtype=loreport&pdiskwicview=false&ecomp=1s39k&prid=9f090d1a-c7a1-48c8-85f4-bebbfd34b7de (last visited Jan. 30, 2020).

197. A grassroots movement is one that mobilizes others to take action and influence an outcome, often politically motivated. Daniel E. Bergan, *Grassroots*, ENCYC. BRITANNICA, https://www.britannica.com/topic/grassroots (last visited Feb. 1, 2020). These efforts can occur in one of two ways: (1) efforts that revolve around voting or (2) efforts to influence policymakers to take a particular stance or take action. *Id.*

198. Catherine Cusick, *Can Apple End Smartphone Addiction?*, LONGREADS (Aug. 16, 2017), https://longreads.com/2017/08/16/can-apple-end-internet-addiction/.

199. Bianca Bosker, *The Binge Breaker*, THE ATLANTIC, https://www.theatlantic.com/magazine/archive/2016/11/the-binge-breaker/501122/?src=longreads (last visited Sept. 15, 2020).

200. *Who We Are*, CTR. FOR HUMANE TECH., https://www.humanetech.com/who-we-are#story (last visited Jan. 1, 2021). This has since been updated from their previous mission statement which was "to reverse human downgrading by inspiring a new race to the top and realigning technology with our humanity." Rachel Lerman, *Putting Humanity First in Tech—That's the Goal of Former Google Executive*, WRAL TECH WIRE (Aug. 11, 2019),

Just as physicians, Time Well Spent is now urging developers to adopt a Hippocratic Oath, but for software.[201] The point is to create accountability in the developers about the psychological influence their designs have on the user.[202] Among others, the main tenets of the Oath serve to remind developers that users are not a "goal" but are people that must be respected.[203] Developers' main purpose is not simply to build platforms, applications and websites, but build connections between human beings.[204] Developers should strive to respect a user's mental health and encourage a healthy relationship with technology.[205] If at any point these values conflict, one should advocate for the benefit of the user and not the product created.[206] Individuals behind the screens are presently showing initiative to implement the aforementioned principles.[207]

The conjunctive efforts of designers' shift in core values to encourage—not demand—users to spend time, wisely, and a sense of conscientiousness to promote responsible platform use will begin to lay down the foundation upon which regulation may stem.

CONCLUSION

Realistically, it is unlikely that there will be a unanimous decision that will benefit everyone equally. Most people are struggling with the idea of regulation. Although Senator Hawley displays regulation as being very definitive, it is not so clear-cut. While there is variance in the way others view social media, nevertheless, society has become a digital era with around seventy-two percent of Americans, of all generations, using some type of social media.[208]

For some, social media use has become a real problem that must be addressed as the Big Tech Companies dig deeper into their box

---

https://www.wraltechwire.com/2019/08/11/putting-humanity-first-in-tech-thats-goal-of-former-google-executive/.

201. Bosker, *supra* note 199.

202. Mariesa Dale, *The Technologist's Hippocratic Oath*, BUILT TO ADAPT (Mar. 9, 2018), https://builttoadapt.io/technologists-hippocratic-oath-94b88d3fe480.

203. *Id.*

204. *Id.*

205. *Id.*

206. *Id.*

207. *See, e.g.*, Mary Meisenzahl, *Here's What Your Instagram Posts Will Look Like Without "Likes,"* BUS. INSIDER (Nov. 11, 2019, 10:03 AM), https://www.businessinsider.com/instagram-removing-likes-what-it-will-look-like-2019-11. Instagram CEO announced a new update of Instagram that will hide likes on posts, claiming "[w]e will make decisions that hurt the business if they help people's well-being and health . . . ." *Id.* Do not worry; it is only for certain users, not the average joes. *Id.*

208. *Social Media Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/social-media/. Compared to 2005, where just five percent of Americans used one of these platforms. *Id.*

of tools. Most significantly, it is not necessarily the existence of social media that is the issue, it is the fine line where existence becomes overuse and where Big Tech exercises too much power over their users' decision-making process. Any success must come from an effort of collaboration. No "one thing" will work in tackling this problem.

Free from the Scourge of War: Defense Contractors Exporting on Behalf of the U.S. Government

*Samantha Cook**

* Samantha Cook is a 2021 J.D. candidate at Duquesne University School of Law. She received her bachelor's degree from George Washington University in international affairs and political science. Samantha would like to thank Professor Patrick Sorek for his guidance.

I. INTRODUCTION

In 1986, Arif Durrani purchased $347,000.00 in Hawk missile parts from an American company.[1] He certified to the American company that he would be responsible for complying with all export obligations, signed a written statement acknowledging that the parts required an export authorization, and knowingly shipped them abroad without appropriate licensing.[2] Durrani was charged with violating the Arms Export Control Act (AECA), which requires Department of State (State Department) licensing for all exports of defense articles.[3] Durrani's defense: the United States government directed him to do it.[4]

Shortly preceding Durrani's indictment, the now notorious Iran-Contra Affair was well underway,[5] and Durrani claimed that he had met with Col. Oliver North, who "assured him 'not to worry about the paperwork' because President Reagan would shortly authorize arms shipments to Iran."[6] The court examined as an affirmative defense a statutory exemption to the licensing requirement, which would permit defense exports without a license if for official use by the United States government (U.S. government), or as part of a foreign assistance program.[7] In its analysis, the court described the AECA's legislative history as "sparse"[8] and turned to the AECA's implementing regulations, the International Traffic in Arms Regulations (ITAR), to guide its interpretation of the government exemption (Section 126.4).[9]

Section 126.4 of the ITAR implements a statutory exemption to the AECA's hard and fast licensing rule.[10] The statute sets forth what appears to be a straightforward rule: unless otherwise noted, a license is not required for the export of defense articles "for official use by a department or agency of the United States Government, or . . . for carrying out any foreign assistance or sales program

1. United States v. Durrani, 835 F.2d 410, 413 (2d Cir. 1987).
2. *Id.* at 414.
3. *Id.* at 415.
4. *Id.* at 416.
5. *Id.*
6. *Id.* at 417. For more information on the Iran-Contra Affair, *see* Executive Summary, S. REP NO. 100-216, at 7 (1987) (Executive Summary).
7. *Durrani*, 835 F.2d at 417.
8. *Id.* at 420.
9. *Id.* at 418–19.
10. *Id.* at 419.

authorized by law and subject to the control of the President by other means."[11] Despite the plain language of the statute and the assistance of its implementing regulation Section 126.4, evolving circumstances and the increasing role of contractors in military operations has driven certain exporters and contractors to understand the limits of the exemption.[12]

Despite the shoddiness of Durrani's claim and doubtfulness of his credibility, his case presents a fascinating—and extremely rare[13]—glimpse into a court's interpretation of a regulatory loophole that allows exporters to ship the most highly-controlled military technology around the world with fairly limited governmental oversight. The rule attempts to answer the question, "when can a private entity ship military equipment at the direction of the government without prior approval by the State Department?"—but it often creates more questions than it answers. In 2019, the State Department amended the language in an attempt to clarify contractors' responsibilities under the ITAR.[14] This article will explore this amendment in light of the increasing need for contractor support.

Contractors play an ever-increasing role in supporting the United States military.[15] An American contractor was killed in December 2019 in a rocket attack in Kirkuk, Iraq, one of many recent military actions involved in the escalation of tensions with Iran.[16] Little information about this contractor has been made public,[17] but unfortunately, their plight is not uncommon. During President Barack Obama's presidency, more civilian contractors were killed in Iraq and Afghanistan than American troops.[18] These overseas contingency operations create numerous legal complexities: what are

11. *Id.* at 418 (citing 22 U.S.C. § 2778(b)(2)).

12. *See infra* Section III(A)(1)–(2).

13. Only two cases have interpreted Section 126.4. *See generally Durrani*, 835 F.2d 410. *See also* United States v. Modarressi, 690 F. Supp. 87, 91 (D. Mass. 1988) ("These exceptions are applicable, however, only in specific, narrow circumstances. They require, among other things, that a transaction be effected solely by a United States government agency (22 C.F.R. § 126.4) or that an article be transferred by the Department of Defense to a representative of a foreign government in the United States (22 C.F.R. § 126.6).").

14. International Traffic in Arms Regulations: Transfers Made by or for a Department or Agency of the U.S. Government, 84 Fed. Reg. 16,398, 16,399 (Apr. 19, 2019) (to be codified at 22 C.F.R. § 126.4 (2019)) [hereinafter Final Rule].

15. *See infra* Section III(A).

16. Barbara Starr, *US Civilian Contractor Killed in Rocket Attack in Iraq*, CNN (Dec. 27, 2019, 9:47 PM), https://www.cnn.com/2019/12/27/politics/iraq-rocket-attack-contractor-killed/index.html.

17. *Id.*

18. Micah Zenko, *Mercenaries Are the Silent Majority of Obama's Military*, FOREIGN POL'Y (May 18, 2016, 4:58 PM), https://foreignpolicy.com/2016/05/18/private-contractors-are-the-silent-majority-of-obamas-military-mercenaries-iraq-afghanistan/.

contractors' rights under the Geneva Convention?[19] What are their authority and obligations under military law?[20] How are civilians overseas held accountable for their actions?[21] One overlooked problem of the growing policy of maintaining a heavily civilian-based military force is seemingly inconsequential, but can in fact be a significant threat to national security: how are the United States' export laws—and their implementing agencies' procedures—adapting to give contractors greater flexibility while holding them accountable?

This article will begin by discussing the background of the AECA and the ITAR, describing their purpose, authority, licensing requirements, and license exemption framework. It will then analyze the recently amended "government exemption," Section 126.4, whose vague language has historically plagued contractors and administrative agencies alike. Section III(A) will discuss the increasing role of private contractors in conducting military operations and illustrate how these contractor-exporters will ultimately benefit from this amended exemption, while Section III(B) will argue that this rule reflects a trend of allowing such contractors increased control over activities that are inherently or closely associated with inherently governmental functions.

The exemption regime of the ITAR acknowledges the need for private individuals to export defense articles overseas in support of U.S. government operations, and the 2019 amendment to Section 126.4 illustrates the State Department's recognition of the military's need for increased contractor mobility. With this increased deference to contractors, however, comes a heightened need for oversight.

II. THE ARMS EXPORT CONTROL ACT, ITAR AUTHORIZATIONS, AND THE SECTION 126.4 EXEMPTION

A. Arms Export Control Act

The federal government controls the proliferation of military equipment and technology primarily via the AECA.[22] The stated goals of the AECA are "a world which is free from the scourge of war and the dangers and burdens of armaments" and "to facilitate

19. *See, e.g.*, Gordon L. Campbell, Contractors on the Battlefield: The Ethics of Paying Civilians to Enter Harm's Way and Requiring Soldiers to Depend upon Them, Presentation to the Joint Services Conference on Professional Ethics (Jan. 27–28, 2000).

20. *Id.*

21. *Id.*

22. Arms Export Control Act, 22 U.S.C. §§ 2751–2799.

the common defense by entering into international arrangements with friendly countries which further the objective of applying agreed resources of each country to programs and projects of cooperative exchange of data, research, development, production, procurement, and logistics support to achieve specific national defense requirements and objectives."[23] The government attempts to strike a balance between its interest in keeping military equipment out of enemies' hands and being competitive in the international defense market. One former Assistant Secretary for Political-Military Affairs, John Hillen, stated the purpose of export controls very concisely, when describing a very expensive effort to destroy 24,000 MANPADS (man-portable air defense systems): "[h]ow much more effective—in terms not only of dollars, pounds sterling or euros, but also in terms of human lives—would it have been to have exercised responsible export controls in the first place and kept these weapons out of the hands of our enemies?"[24]

Generally, the AECA provides that, in furtherance of Congress's stated goals, the State Department, under the direction of the President, is responsible for supervising and monitoring sales and exports of defense articles and defense services in coordination with economic and political factors.[25] Exports of defense articles must be in accordance with United States foreign policy, and strict end-user requirements are set forth to ensure that defense articles and technology are truly for the use of the named recipient and for the stated purpose.[26] Such purposes include the foreign country's self-defense, cooperative projects,[27] public works, nuclear non-proliferation, or to allow the country to participate in arrangements consistent with the United Nations Charter, among others.[28] Its implementing regulations, however, contain specific rules and procedures for carrying out the policies in the AECA.[29]

---

23. *Id.* § 2751.

24. John Hillen, Assistant Secretary for Political-Military Affairs, Dep't of State, Address to the 18th Annual Global Trade Controls Conference (Nov. 3, 2005) (transcript available at the U.S. Department of State Website at https://2001-2009.state.gov/t/pm/rls/rm/56557.htm).

25. 22 U.S.C. § 2752(b).

26. *Id.* § 2753(a)(1)–(2).

27. Cooperative projects under the AECA include written agreements "undertaken in order to further the objectives of standardization, rationalization, and interoperability of the armed forces of [NATO]," *id.* § 2767(b)(1), or "a jointly managed arrangement, described in a written agreement among the parties, which is undertaken in order to enhance the ongoing multinational effort of the participants to improve the conventional defense capabilities of the participants . . . ." *Id.* § 2767(b)(2).

28. *Id.* § 2754.

29. *The International Traffic in Arms Regulations (ITAR)*, U.S. DEP'T OF STATE DIRECTORATE OF DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987 (last visited Feb. 11, 2020).

B. International Traffic in Arms Regulations

The President delegated the implementing regulations of the AECA to the State Department.[30] The implementing regulations, the International Traffic in Arms Regulations (ITAR), set forth a complex regulatory regime for the authorization of defense exports.[31] The ITAR controls defense articles, defense services, and technical data.[32] Defense articles are tangible items and technical data subject to the United States Munitions List (USML).[33] However, technical data and defense services somewhat warp the conventional wisdom of what an export is.[34] Technical data is defined as any information, including software, "required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles."[35] Similarly, a defense service is the provisioning to a foreign person of technical data, assistance in the use of a defense article, or military training.[36] Exports, then, are not as straightforward as shipping an item overseas; merely discussing controlled technical data with a non-citizen in the United States could constitute an export.[37] All defense exports must be authorized by the State Department through its regime of licensing, agreements, and exemptions.[38] Failure to comply with the ITAR subjects exporters to civil and criminal penalties, up to $1,000,000.00 per violation or debarment.[39]

1. Licensing and Agreements

The Directorate of Defense Trade Controls (DDTC) reviews and approves export license applications, and different types of exports

30. Exec. Order No. 13,637, 78 Fed. Reg. 16,129 (Mar. 13, 2013).
31. *See* International Traffic in Arms Regulations, 22 C.F.R. §§ 120–130 (2019).
32. *Id.* § 120.2.
33. *Id.*
34. *See, e.g.*, Final Rule, *supra* note 14, at 16,400 (addressing public comments expressing concern with the proposed rule's removal of the term "technical data" from the language of the exemption: "Several commenters noted the removal of the reference to technical data and assumed that this indicated that the exemption would no longer authorize exports of technical data. As noted above, the Department removed the reference to technical data because it was redundant and confusing. Technical data is a form of defense article and is authorized by the language authorizing the export (now export, reexport, retransfer, and temporary import) of defense articles.").
35. 22 C.F.R. § 120.10(a)(1) (2014).
36. *Id.* § 120.9.
37. *Id.*
38. *E.g.*, *id.* §§ 123.1, 123.5.
39. *Id.* §§ 127.1, 127.3, 127.10.

require different types of licenses.[40] Long-term arrangements for the provision of defense services or technical data require a Technical Assistance Agreement (TAA) or Manufacturing License Agreement (MLA),[41] while regular shipments of hardware or software may require only a DSP-5 license for the permanent export of hardware or technical data.[42] Regardless of the method, all exports of defense articles or technical data require review by DDTC unless it falls into one of few exceptions in the ITAR.[43] License and agreement applications require the exporter to disclose details of the sale or contract under which they are exporting to the DDTC, including the end user, the quantity, the USML classification, and the dollar value of the items.[44] The DDTC then reviews the application, in conjunction with other bureaus within the State Department, the Department of Defense (DoD), and other interested agencies, to ensure that it aligns with foreign policy.[45]

While the population of exporters needing authorization to ship controlled military equipment may seem small, the DDTC received roughly 37,000 license applications in 2018.[46] The DDTC takes on average thirty-four days to process an application.[47] This long turnaround time drives exporters, many of whom are private defense contractors, to seek exemptions to the strict licensing requirements of the ITAR.[48]

---

40. *Id.* § 123.1(a)(1)–(4).

41. *Id.* § 124.1(a).

42. *Id.* § 123.1(a)(1).

43. *Defense Trade Controls Licensing (DTCL)*, U.S. DEP'T OF STATE DIRECTORATE OF DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=02bbbbc4dbc7bf0044f9ff621f9619ac (last visited Oct. 4, 2019).

44. *Guidelines for Completion of a Form DSP-5 Application/License for Permanent Export of Unclassified Defense Articles and Related Unclassified Technical Data*, U.S. DEP'T OF STATE DIRECTORATE OF DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=cfd37af0db199f00d0a370131f96199d (last visited Oct. 26, 2019).

45. Jonathan Dennis, *Complying with ITAR Controls: License Review Process*, U.S. DEP'T OF STATE 6–12 (Sept. 19, 2016), https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=29acd359db9ddf00d0a370131f961942.

46. *Defense Trade Controls Licensing (DTCL)*, *supra* note 43.

47. *Id.*

48. *See* Clinton Long, *An Imperfect Balance: ITAR Exemptions, National Security, and U.S. Competitiveness*, 2 NAT'L SEC. L.J. 43, 62 (2013) ("Loosening the restrictions of ITAR has been welcomed by U.S. industries because it provides them with additional opportunities to sell their defense products with less bureaucracy.").

2. Exemptions

Interspersed throughout the regulatory labyrinth of the ITAR are various exemptions to the "ask first, export later"[49] principle.[50] Under very specific circumstances, exporters may be able to export or temporarily import hardware or software, share technical data, or perform defense services without the need for separate licensing.[51] Though an exporter still needs to be registered with the DDTC in order to be eligible to use an exemption,[52] as well as maintain records of all exemptions,[53] it is typically a much more expeditious process than to apply for a license or agreement.[54]

Exemptions are available for a variety of purposes, but each of them represents a carefully calculated foreign policy consideration.[55] Some exemptions are based on the close relationship with the end-user country; for example, exemptions exist for shipping hardware and data to certain friendly countries, like Canada.[56] Similarly, pursuant to Defense Trade Cooperation Treaties, the ITAR sets forth exemptions for Australia[57] and the United Kingdom.[58] The North Atlantic Treaty Organization (NATO) partners also receive special treatment under the ITAR through exemptions that permit American exporters to maintain equipment for NATO, Japan, and Sweden without a TAA[59] and to share technical data for NATO countries' bid proposals.[60] There are dozens of other exemptions throughout the ITAR, organized in no intuitive manner.[61] Frequenters of license exemptions include defense contractors, university laboratories, and federally funded research and

49. MARK K. NEVILLE, JR., INTERNATIONAL TRADE LAWS OF THE UNITED STATES: STATUTES AND STRATEGIES ¶ 16.03 (2019).

50. JOHN R. LIEBMAN ET AL., CONG. RSCH. SERV., R41916, THE U.S. EXPORT CONTROL SYSTEM AND THE EXPORT CONTROL REFORM INITIATIVE § 4.05[1] (2014).

51. *Id.*

52. *Id.*

53. 22 C.F.R. § 123.26 (2012).

54. *See* Tom Reynolds, *Stop, Read and Apply ITAR Exemptions*, EXP. SOLS., https://www.exportsolutionsinc.com/resources/blog/stop-read-and-apply-itar-exemptions/ (Jan. 14, 2019).

55. Long, *supra* note 48, at 63 ("Either national security is compromised or economic interests suffer, and whichever is the priority for lawmakers at any given time when ITAR is modified will win at the end of the day.").

56. 22 C.F.R. § 126.5 (2012).

57. *Id.* § 126.16.

58. *Id.* § 126.17.

59. *Id.* § 124.2(c).

60. *Id.* § 125.4(c).

61. LIEBMAN ET AL., *supra* note 50 ("There are approximately seventy-five frequently amended exemptions scattered throughout the ITAR, but because the official version of the ITAR contains no index, ITAR readers may be unaware that an exemption is available.").

development centers.[62] Strikingly, between the period of 2004 and 2006, four defense contractors alone comprised twenty-five percent of the exemption certification letters issued by the DoD.[63] One long-questioned ITAR exemption, and the subject of this article, is the license exemption for transfers to or on behalf of the United States government.[64]

C. The United States Government Exemption

1. Prior Language of the Exemption

The revision of Section 126.4 was "long-awaited" by defense contractors[65] as the previous language of the exemption proved to be "complex and difficult to use."[66] Prior to the 2019 amendment, the Section 126.4 exemption authorized the "temporary import, or temporary export, of any defense article, including technical data or the performance of a defense service, *by or for* any agency of the U.S. Government for official use by such an agency, or for carrying out any foreign assistance, cooperative project, or sales program . . . ."[67]

On its face, this exemption seemed to allow the government, in its official capacity, to temporarily import, or temporarily export, defense articles, technical data, or defense services.[68] However, the phrase "by or for" insinuated that the exemption was also open to other non-government entities. The rule went on to specify that the exemption:

> applies only when all aspects of a transaction (export, carriage, and delivery abroad) are affected by a United States Government agency or when the export is covered by a United States Government Bill of Lading. This exemption, however, does not apply when a U.S. Government agency acts as a transmittal

62. U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-1103, CLARIFICATION AND MORE COMPREHENSIVE OVERSIGHT OF EXPORT EXEMPTIONS CERTIFIED BY DOD ARE NEEDED (2007).

63. *Id.*

64. 22 C.F.R § 126.4 (2019 Amended Rule).

65. *See, e.g.*, Williams Mullen & Thomas McVey, *ITAR Amendment Expands License Exemption for Transfers by or for the U.S. Government*, JD SUPRA (Sept. 10, 2019), https://www.jdsupra.com/legalnews/itar-amendment-expands-license-71842; John R. Shane & Lori E. Scheetz, *DDTC Makes Long-Awaited Clarification to the ITAR 126.4 Exemption*, WILEY (Apr. 19, 2019), https://www.wiley.law/alert-DDTC-Makes-Long-Awaited-Clarification-to-the-ITAR-1264-Exemption.

66. Mullen & McVey, *supra* note 65.

67. 22 C.F.R. § 126.4(a) (2019 Pre-Amended Rule) (emphasis added).

68. *Id.*

> agent on behalf of a private individual or firm, either as a convenience or in satisfaction of security requirements.[69]

This provision provides some insight as to how this rule is used by contractors and government agencies alike. It suggests that private individuals and firms could, in fact, ship defense articles abroad without prior DDTC authorization, but only when the entire transaction is carried out by the government.[70] It also hints at how some exporters have tried to abuse it in the past. By specifying that the rule does not apply when the government agency acts merely as a transmittal agent, the State Department prohibits agencies from circumventing the export control process by simply loading contractors' materiel into a government jet and expediting its shipment abroad. The government is also not authorized to make any export that is otherwise prohibited by law.[71]

The final portion of the former version of the rule provided some guidance on shipments, not *by* the government, but *for end-use* by the government, suggesting that this carve-out is intended for private entities. The rule provided:

> (c) A license is not required for the temporary import, or temporary or permanent export, of any classified or unclassified defense articles, including technical data or the performance of a defense service, for end-use by a U.S. Government Agency in a foreign country under the following circumstances:
>
> (1) The export or temporary import is pursuant to a contract with, or written direction by, an agency of the U.S. Government; and
>
> (2) The end-user in the foreign country is a U.S. Government agency or facility, and the defense articles or technical data will not be transferred to any foreign person; and
>
> (3) The urgency of the U.S. Government requirement is such that the appropriate export license or U.S.

69. 22 C.F.R. § 126.4(a) (2019 Pre-Amended Rule).

70. The exemption also applied when the shipment was authorized by a United States Government Bill of Lading. A Government Bill of Lading is an official contract of carriage document setting forth terms with the transporter. 41 C.F.R. § 102-117.85 (2019).

71. 22 C.F.R. § 126.4(b) (2019 Pre-Amended Rule).

> Government Bill of Lading could not have been obtained in a timely manner.[72]

This provision opened significant opportunity and risk for contractors, particularly those under contract with the U.S. government to provide defense articles and services abroad. It drew a seemingly narrow boundary around when Section 126.4 may be used. Applying all three of its elements, it only authorized those private entities that are under contract or written direction from the U.S. government to ship defense articles abroad on very short notice.

The exemption in its prior state was vague, causing confusion among exporters (and their lawyers) as to how and when the provision could be invoked.[73] The rule also drove a wedge between the State Department and the DoD as to the authorization authority and recordkeeping requirements for such exports.[74] In May 2015, the State Department proposed a rule change to clarify the contentious language,[75] and in April 2019, the final rule went into effect.[76]

2. Significant Changes in the Amended Rule

The most significant change in the 2019 amendment is the separation of Sections 126.4(a) and (b), which divides the authorization cleanly between exports by the government and exports for or on behalf of the government.[77] The prior rule chaotically lumped in Section 126.4(a) a cluster of circumstances where an exporter, whether it be the government or a private entity, could temporarily export, import, or perform a defense service.[78] The prior paragraph of Section 126.4(c), on the other hand, seemed to be, but was not expressly directed at parties other than the United States government, and gave loose guidance about how that exemption could be used.[79] The new language of the exemption carves out Section 126.4(a) specifically for use by the government agency with very limited applicability to private entities.[80]

---

72. *Id.* § 126.4(c) (2019 Pre-Amended Rule).
73. Shane & Scheetz, *supra* note 65.
74. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 62.
75. Exports and Temporary Imports Made to or on Behalf of a Department or Agency of the U.S. Government, 80 Fed. Reg. 29,565, 29,565 (proposed May 22, 2015).
76. Final Rule, *supra* note 14, at 16,398.
77. *Id.*
78. 22 C.F.R. § 126.4(a)–(c) (2019 Pre-Amended Rule).
79. *Id.* § 126.4(c) (2019 Pre-Amended Rule).
80. 22 C.F.R. § 126.4 (2019 Amended Rule).

The public comments to the proposed rule "specifically asked the Department to state that any use by a U.S. Government contractor in the course of contract is within the scope of official use by the U.S. Government."[81] The department accepted this recommendation in the new rule and provided clearer criteria for when use by a contractor qualifies as "official use."[82] Section 126.4(b) now belongs to contractors: it omits the need for a license when shipping to a department of the U.S. government or an entity other than the U.S. government at its written direction.[83]

Another significant change is found at Section 126.4(b)(1), which now provides that an entity may export without a license to the U.S. government "at its request."[84] Previously, private contractors shipping to the U.S. government abroad were burdened with additional elements, including being in a contract with or at written direction of the government, verifying that the end-user is the U.S. government, and extreme urgency.[85] The "at its request" standard suggests that there is a lower bar for exporters to ship directly to the U.S. government; notably, the rule implies that the request need not even be in writing, at least for purposes of ITAR compliance.[86] Further, the exemption no longer requires that the government effect the entire transaction.[87] With this change, private entities shipping to the government, or to a foreign person at the written direction of the government, no longer need to question whether they are exporting "by" or "for" the government for one of the approved purposes.

The amended rule also adds a provision to expressly prohibit exports that would otherwise violate the law, such as United Nations Security Council Resolutions and U.S. arms embargoes.[88] This is a seemingly obvious and intuitive catch-all rule to contour the U.S. government exemption. However, like the other changes in the rule, its addition suggests that the broadening of the exemption raised concerns with the DDTC that exporters—and potentially even government agencies themselves—would attempt to export

81. Final Rule, *supra* note 14, at 16,400.
82. *Id.*
83. 22 C.F.R. § 126.4(b) (2019 Amended Rule).
84. *Id.* § 126.4(b)(1) (2019 Amended Rule).
85. 22 C.F.R. § 126.4(c)(1)–(3) (2019 Pre-Amended Rule).
86. 22 C.F.R. § 126.4(c)(1)–(3) (2019 Amended Rule). Section 126.4(c) previously required a contract or written direction for use of the "by or for" exception. 22 C.F.R. § 126.4(c) (2019 Pre-Amended Rule).
87. 22 C.F.R. § 126.4(a) (2019 Amended Rule). This requirement was removed from Section 126.4(a) (2019 Pre-Amended Rule).
88. 22 C.F.R. § 126.4(d) (2019 Amended Rule).

controlled technology to countries with a heightened risk of diversion to enemy nations or terrorist organizations.[89]

Section 126.4(d) now cites another section of the ITAR, Section 126.1, titled, "Prohibited exports, imports, and sales to or from certain countries."[90] This section provides for a near-absolute bar to exports of defense articles and defense services to certain countries[91] and a qualified bar on exports to others, meaning that there is generally a policy of denial to these countries with certain enumerated exceptions.[92] The addition of this section is significant because it involves countries that are likely to be involved in operations warranting the use of the Section 126.4 exemption. Recall that the exemption authorizes exports at the request or written direction of the government, whether for end-use by U.S. persons or not.[93] The United States military carries out foreign assistance in Section 126.1(b) countries, such as Afghanistan and Iraq.[94] Much of this foreign assistance supports peace and security, which is comprised of initiatives such as counter-narcotics, counter-terrorism, transnational crime, combating weapons of mass destruction, and stabilization.[95] Though these programs are funded and monitored by the government,

> [m]ost development and humanitarian assistance activities are not directly implemented by United States government personnel but by private sector entities, such as individual personal service contractors, consulting firms, universities, private

89. The ITAR's purpose is balancing national security with the economic interests of the U.S. defense industry. Exemptions attempt to add nuance to this balance, but they create additional risk to national security. *See, e.g.*, Long, *supra* note 48, at 60 ("There are significant concerns that terrorists or rogue states could acquire these defense articles from other countries—even those friendly to the United States—that import these goods but do not have the same strict export controls as the United States. It is therefore unclear how the State Department will use its exemption authority in the future.").

90. 22 C.F.R. § 126.1 (2019).

91. *See id.* § 126.1(d)(1) (setting forth a policy of license denial to Belarus, Burma, China, Cuba, Iran, North Korea, Syria, and Venezuela).

92. *Id.* § 126.1(d)(2).

93. 22 C.F.R. § 126.4(b) (2019 Amended Rule).

94. In 2018, the United States government spent $999,741,283.00 on assistance to Afghanistan and $452,070,635.00 to Iraq. *Map of Foreign Assistance Worldwide*, U.S. DEP'T OF STATE, https://www.foreignassistance.gov/explore (Nov. 6, 2020) (Select Iraq or Afghanistan, and filter to "2018" and "Spent.").

95. Of the 2018 foreign assistance funding to Afghanistan and Iraq, peace and security projects made up $80,248,924.00 and $53,764,002.00 respectively. *Id.* (Select Iraq or Afghanistan; then filter to "2018," and "Spent," and "Peace and Security.").

voluntary organizations (PVOs), or public international organizations (PIOs).[96]

This arrangement leaves non-governmental parties responsible for carrying out these billion-dollar programs and accountable to ensure that they are done safely and efficiently. The addition of the Section 126.1 provision in the new exemption language is a nod to those contractors whom the prior exemption left wondering if otherwise-prohibited countries was in the scope of Section 126.4. Here, the DDTC affirmatively states that they are not and puts that question to rest.[97]

III. INCREASED CONTRACTOR FLEXIBILITY, DECREASED GOVERNMENT OVERSIGHT: COMPETING ARGUMENTS ON THE SECTION 126 EXEMPTION

A. The Role of Contractors in Defense Administration Has Increased the Need for Less Restrictive Export Controls to Maintain Compliance

The expansion of the government exemption reflects the law's adaptation to the need for contractors to support military operations. Though the military has always employed contractors to conduct wartime operations, "[t]heir support is no longer an adjunct, ad hoc add-on to supplement a capability."[98] In 2007, there were an estimated 100,000 civilian contract workers in Iraq alone.[99] Today, the number of security contractors in Afghanistan is estimated at 5,800, raising concern about concealment of what is really happening "on the ground."[100] Critics against the use of private contractors claim that contractors are employed to give the appearance of de-

96. MARIAN L. LAWSON & EMILY M. MORGENSTERN, CONG. RSCH. SERV., R40213, FOREIGN AID: AN INTRODUCTION TO U.S. PROGRAMS AND POLICY 18 (2019).

97. 22 C.F.R. § 126.4(d) (2019 Amended Rule) ("This section does not authorize any department or agency of the U.S. Government to make or authorize any export that is otherwise prohibited by any other administrative provisions or by any statute that is inconsistent with U.S. arms embargoes or United Nations Security Council Resolutions (*see* § 126.1).").

98. Campbell, *supra* note 19.

99. CARRIE HUNTER & DANIEL GOURE, LEXINGTON INST., CONTRACTORS ON THE BATTLEFIELD 1 (2007).

100. Paul D. Shinkman, *Afghanistan's Hired Guns*, US NEWS (Apr. 26, 2019, 5:00 AM), https://www.usnews.com/news/national-news/articles/2019-04-26/us-employs-unprecedented-number-of-security-contractors-in-afghanistan ("'The main problem with contractors of all sorts is there's just not enough attention to what they're doing. That's not been reported out in a clear way to anybody's satisfaction for all these years,' says Catherine Lutz, a professor at Brown University and a director of its Costs of War project, which documents the use of private contractors in U.S. conflicts. 'The Pentagon should be telling us, the American public, who's funding this, what that means, why this is happening.'").

escalation by withdrawing "troops," as in military personnel, but merely replacing them with "hired guns."[101]

The United States Army (Army) characterizes battlefield contractors as either systems contractors, external support contractors, or theater support contractors.[102] These contractors' roles range from providing support for weapons and other materiel, supporting the combat authority at headquarters, and simply providing goods and services to service members.[103] The Joint Chiefs of Staff Joint Logistics Doctrine states that the "DOD relies on contractors to perform many tasks . . . such as base operating support[,] intra-theater transportation, logistics services, maintenance, storage, construction, security operations, and common-user commodities."[104] The law has adapted with the changing composition of the battlefield to grant privileges to contractors that were previously reserved for the military, and the expansion of the government exemption appears to be one such example.

Another such development is the trend of hybrid Foreign Military Sales (FMS) and Direct Commercial Sales, an arrangement where "the main defense article [is] provided through direct commercial sales and classified systems, weapons, and/or upgrades [are] provided through FMS."[105] This type of contract means that the government carries out one portion of the contract, while the private contractor is responsible for the others; therefore, the export obligations of the government and the contractor are inextricably linked in order to perform the contract, which incentivizes the government to ensure that the contractor can meet its obligations in a timely manner.

Further, the Defense Federal Acquisition Regulations Supplement (DFARS) requires that defense contracts place the burden of export compliance upon the contractor and their subcontractors.[106] This lessens the liability on the contracting agency for mistaken commodity classifications or incorrect interpretations of State

101. *Id.*

102. HUNTER & GOURE, *supra* note 99, at 2.

103. *Id.* at 3.

104. JOINT CHIEFS OF STAFF, DEP'T OF DEF., JOINT LOGISTICS, at xi (2019).

105. Derek Gilman et al., *Foreign Military Sales & Direct Commercial Sales*, DEP'T OF DEF. & DEF. SEC. COOP. AGENCY 14 (Sept. 30, 2014), https://www.dsca.mil/sites/default/files/final-fms-dcs_30_sep.pdf.

106. 48 C.F.R. § 252.225-7048(b) (2019) (requiring federal defense contracts to include the following clause: "The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR.").

Department regulations, such as the appropriate use of the exemption at issue here. Because of this heightened regulatory and operational responsibility on private contractors to execute national security and foreign assistance activities, these entities must receive specific guidance to improve their compliance programs and operate more efficiently with their government partners. The 2019 amendment to Section 126.4 is one such regulatory change.

The use of civilian contractors in battlefield operations raises numerous legal questions related to international and military law,[107] but the focus here is whether the expansion of the ITAR to allow civilians to carry out defense exports at the request of the United States government goes a step too far in authorizing contractors to conduct inherently governmental functions. Below is an examination of potential scenarios where contractors who would previously have been limited in their use of the government exemption may find new opportunity with the amended rule.

1. Application of the Section 126.4 Exemption

One scenario where the revisions to Section 126.4 may benefit exporters and the DoD alike is during the performance of an Indefinite-Delivery/Indefinite-Quantity (IDIQ) contract. IDIQ contracts arise when "the Government cannot predetermine, above a specified minimum, the precise quantities of supplies or services that the Government will require during the contract period . . . ."[108] IDIQ's are a more convenient contract arrangement for the government, where the contract is awarded to multiple contractors and the competition lies at the task order level.[109] Between 2011 and 2015, the DoD accounted for sixty-eight percent of all of the federal government's IDIQ contracts.[110] The Government Accountability Office (GAO) investigated the DoD's use of IDIQ contracts in 2017, reporting:

> [i]n addition, [DoD] officials told us that the contracts they used served a broader customer base, for example, multiple commands, other federal agencies, and foreign military sales. By not needing to specify an exact quantity or timing of

107. *See supra* text accompanying notes 19–21.

108. 48 C.F.R. § 16.504(b) (2019).

109. Gregory R. Hallmark, *2019 NDAA Analysis: Enhancing IDIQs and Other Provisions*, HOLLAND & KNIGHT GOV'T CONTS. BLOG (May 15, 2019), https://www.hklaw.com/en/insights/publications/2019/05/2019-ndaa-analysis-enhancing-idiqs-and-other-provisions.

110. U.S. GOV'T ACCOUNTABILITY OFF., GAO-17-329, AGENCIES WIDELY USED INDEFINITE CONTRACTS TO PROVIDE FLEXIBILITY TO MEET MISSION NEEDS (2017).

> delivery at the time of contract award, program offices can accommodate unforeseen needs on an ongoing basis through issuance of orders. For example, an Army contract for Aerial Target Systems training and testing is intended for use by all military departments as well as foreign military partners. Since the need for testing and training varies depending on the customer, these requirements were less defined at contract award, and will be more clearly specified at the time of order.[111]

The IDIQ arrangement requires the contractor to be agile in its ability to support operations, which presumably creates an increased burden to ship supplies on very short notice.

The GAO's report also discussed two contracts for Unmanned Aircraft Systems (UAS), which provided "support for overseas contingency operations."[112] UAS operations often require "[c]ontractors [to be] deployed for weapon systems maintenance operate out of established overseas military installations or highly secured forward operating bases."[113] If the exporter was obligated under the contract to transport the equipment to contractors overseas, then prior to the 2019 amendment, it would not have qualified for the "for official use"[114] element of Section 126.4(a) or the "for end-use by" provision of Section 126.4(c),[115] even though it was supporting American military operations.

One illustrative DoD contract opportunity calls for Requests for Information from industry for procurement of supplies and services "related to integration of a [counter-UAS Family of Systems]."[116] Under this contract, the "systems integration partner" will be responsible for integrating sensors and systems to provide "layered defense for [Special Operations Forces] Operators in a variety of . . . environments [outside of the continental United States (OCONUS)]."[117] The contractor will need to "[c]oordinate with the

---

111. *Id.* at 14.
112. *Id.* at 18–19.
113. Keric D. Clanahan, *Wielding a "Very Long, People-Intensive Spear": Inherently Governmental Functions and the Role of Contractors in U.S. Department of Defense Unmanned Aircraft Systems Missions*, 70 A.F. L. REV. 119, 173 (2013).
114. 22 C.F.R. § 126.4(a) (2019 Pre-Amended Rule).
115. *Id.* § 126.4(c) (2019 Pre-Amended Rule).
116. *Contract Opportunity: Counter Unmanned Systems (CUxS), Systems Integration Partner (SIP)*, BETA SYS. FOR AWARD MGMT., https://beta.sam.gov/opp/65fa7d2fd0984bed9cb6f2187afd07e3/view?keywords=unmanned&sort=relevance&index=opp&is_active=true&page=1&inactive_filter_values=false&opp_publish_date_filter_model=%7B%22dateRange%22:%7B%22startDate%22:%222020-05-06%22,%22endDate%22:%222020-05- (last visited Nov. 19, 2020).
117. *Id.*

Government logistics team in the fielding of packaged solutions."[118] The contract will also require contractors to be able to "staff and support 24x7 work week . . . including . . . OCONUS deployments to active armed conflict areas."[119] This solicitation exemplifies the integrated nature of the contractor-military relationship in UAS operations and illustrates the contractor's need—and government's expectation—of flexibility to provide overseas support "in the event of an immediate surge or a reduction in requirements."[120]

In the absence of an advisory opinion from DDTC, a risk-averse company would err on the side of first seeking authorization from DDTC rather than relying on direction from the DoD. The 2019 amendment, however, provides clearer guidance for exporters in this position and expressly answers the looming question of whether the exemption applies to private entities.[121] The exemption now provides for entities in a contractual relationship with the government to export without a license in specific circumstances,[122] or for any person or entity to ship to the government without a license as long as it is at its written direction.[123]

B. The Exemption May Continue to Exacerbate Agencies' Oversight Challenges

1. A Note on Department of Commerce's GOV Exemption

Though the focus of this article is the ITAR exemption for government use, the Department of Commerce's Bureau of Industry and Security's (BIS) role in regulating sensitive exports cannot be understated. While the State Department has jurisdiction over the export of defense articles on the munitions list, the Commerce Department's jurisdiction covers the export of quite literally everything else. BIS regulates exports through the Export Administration Regulations (EAR) Commerce Control List (CCL), the scope of which covers the export of everything from nuts and bolts to commercial aircraft. As a result, contractors involved in defense exports often juggle both the ITAR and the EAR when shipments include both military equipment and commercial products. The CCL also regulates "dual-use" items, also known as "600-series" items, which are items that moved from the USML to the CCL during the

118. *Id.*
119. *Id.*
120. *Id.*
121. 22 C.F.R. § 126.4(a)(1)(ii)(A)–(D) (2019 Amended Rule).
122. *Id.* (2019 Amended Rule).
123. *Id.* § 126.4(b) (2019 Amended Rule).

Export Control Reform Initiative, an administrative attempt at harmonizing the multiple export control regimes.

The EAR contains a number of exceptions, as the ITAR does exemptions, which allow exporters to ship without a license. Notably, the EAR contains an exception called GOV.[124] This regulation generally authorizes exporters to ship products (excluding 600-series items) when they are "for personal use by personnel and agencies of the U.S. Government,"[125] when they are "made by or consigned to a department or agency of the U.S. Government,"[126] or when they are "made for or on behalf of a department or agency of the U.S. Government."[127]

This third option somewhat mirrors the contentious language of the §126.4 exemption, but it sheds some additional light. The regulation goes on to authorize exports that are "for use by a department or agency of the U.S. Government, when: [t]he items are destined to a U.S. person; and [t]he item is exported . . . pursuant to a contract between the exporter and . . . the U.S. Government."[128] The exception further applies to exports to "support . . . cooperative program[s] . . . or arrangement[s] with a foreign government or international organization,"[129] much like the ITAR exemption. Finally, the exception explicitly authorizes exports without a license "pursuant to an official written request or directive from the U.S. Department of Defense,"[130] again raising the question of what constitutes a written request or directive.

This exception may also be used to ship to cooperating governments or NATO members, again excluding 600-series items and a number of other exclusions.[131] The use of this exception does not appear to require a contract, written direction, or even consent of the U.S. Government.

EAR compliance is extremely important for exporters. Not only is the jurisdiction incredibly broad, but the regulations are more complex, and the enforcement actions for violations tend to be even more severe than those imposed upon ITAR violators. Though the goal to completely harmonize the export control regimes into one set of regulations never came to fruition, defense contractors with ITAR-controlled products must also understand their obligations

124. 15 C.F.R. § 740.11 (2020).
125. *Id.* § 740.11(b)(2)(i).
126. *Id.* § 740.11(b)(2)(ii).
127. *Id.* § 740.11(b)(2)(iii).
128. *Id.* § 740.11(b)(2)(iii)(A)(1)–(2).
129. *Id.* § 740.11(b)(2)(iii)(B).
130. *Id.* § 740.11(b)(2)(iv).
131. *Id.* § 740.11(c).

under the Commerce Department's EAR when it comes to carrying out military contracts, as more and more formerly ITAR-controlled products shift under the watchful eye of BIS.

2. Improved Alignment Between the State Department and the DoD: Two Arms of American Foreign Policy

Though defense contractors generally see this rule as a triumph,[132] it illustrates a more widespread concern related to administrative oversight of national security and foreign policy. Section III(A) discussed the increasing role of contractors in overseas military operations, a necessity for the DoD to augment its personnel, but a bane for government accountability.

If export controls pose a question of balance of powers, it does not fall within the traditional debate of legislative versus executive powers. Considering all the governmental actions that plague legal analysts as to the federal balance of powers, the authority over arms controls historically, and mostly uncontestably, bends toward the executive branch. Dating back to *United States v. Curtiss-Wright Export Corp.*,[133] the president has had broad discretion over decisions concerning national security. The Court held that "the President alone has the power to speak or listen as a representative of the nation."[134] The more pressing struggle over authority to administer the AECA is between the administrative agencies with a stake in foreign policy.[135]

The AECA delegates the authority and the duty to control arms exports to the State Department.[136] The role that arms exports play in foreign policy, however, extends beyond the State Department into the realm of national defense, necessarily implicating the DoD and other national security agencies. Though these agencies fall under the control of the executive, each agency has a distinct charter with regard to the execution of foreign policy.

The DDTC's mission is, "[e]nsuring commercial exports of defense articles and defense services advance U.S. national security and foreign policy objectives."[137] Generally, the State Department's role in arms administration can be broken into three prongs: policy,

132. *See, e.g.*, Shane & Scheetz, *supra* note 65.
133. 299 U.S. 304 (1936).
134. *Id.* at 319.
135. *See, e.g.*, IAN F. FERGUSSON & PAUL K. KERR, CONG. RSCH. SERV., R41916, THE U.S. EXPORT CONTROL SYSTEM AND THE EXPORT CONTROL REFORM INITIATIVE 3–4 (2019).
136. 22 U.S.C. § 2752(b).
137. *The Directorate of Defense Trade Controls (DDTC)*, U.S. DEP'T OF STATE DIRECTORATE OF DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_about_us_landing (last visited Jan. 10, 2020).

licensing, and enforcement.[138] In its capacity for determining defense trade policy, the DDTC is primarily responsible for maintaining the ITAR, developing technology policy, and analysis of end-users and countries to establish export eligibility.[139] The licensing arm coordinates review and approval of all export licenses and agreements, as well as provides guidance and advisory opinions to exporters.[140] Finally, the enforcement arm of the DDTC "is tasked with ensuring compliance with the AECA and ITAR through civil enforcement of the regulations and coordination with law enforcement regarding criminal violations."[141]

Meanwhile, the DoD's primary agency concerned with arms controls is the Defense Security Cooperation Agency (DSCA), whose mission is to "advance U.S. national security and foreign policy interests by building the capacity of foreign security forces to respond to shared challenges. DSCA leads the broader U.S. security cooperation enterprise in its efforts to train, educate, advise, and equip foreign partners."[142] DSCA administers cooperation programs and FMS transactions with the goal of bolstering allies' military and institutional capabilities in alignment with U.S. interests.[143]

Although the federal agencies are aligned to a unified policy as to the proscribed end-users, locations, and purposes of arms exports, the DoD is in a unique and potentially conflicted position as both a regulator of defense trade as well as a party to the transaction. On one hand, the interest of national security would warrant a full and thorough investigation of each transaction, down to each shipment and email concerning controlled defense articles. On the other hand, the DoD's realistic need for expeditious overseas support for itself and its allies poses a dichotomous stake in export controls.

The application of many of these ITAR exemptions concerning official use by the U.S. government requires the execution of an exemption letter.[144] In calendar years 2004 to 2006, the DoD and its various components certified 1,900 letters for more than 270

138. *Id.*

139. *Defense Trade Controls Policy (DTCP)*, U.S. DEP'T OF STATE DIRECTORATE OF DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=47ee3b08dbc7bf0044f9ff621f9619d7 (last visited Jan. 10, 2020).

140. *Defense Trade Controls Licensing (DTCL)*, *supra* note 43.

141. *Defense Trade Controls Compliance (DTCC)*, U.S. DEP'T OF STATE DIRECTORATE OF DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=000d7b84dbc7bf0044f9ff621f9619a3 (last visited Jan. 19, 2020).

142. *Mission, Vision, and Values*, DEF. SEC. COOP. AGENCY, https://www.dsca.mil/about-us/mission-vison-values (last visited Jan. 19, 2020).

143. *Id.*

144. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 62.

exporters.[145] The State Department has no prior review of any transactions authorized certified under these exemption letters, which has caused friction amongst the agencies.[146] Generally, the process is as follows:

> [s]ome ITAR exemptions apply to exports that directly benefit [DoD] activities, ranging from support of defense cooperative programs, such as the Joint Strike Fighter, to providing equipment and technical services necessary to support U.S. forces in foreign locations. For such exemptions, [DoD] confirms whether the export activity appropriately qualifies for the use of an exemption and typically documents this confirmation in a written letter directly to the exporter or sometimes to the cognizant [DoD] program office that the exemption will benefit.[147]

Certification guidelines were drafted but never issued department-wide.[148] DoD Instruction 2040.02 provides that the Director of the Defense Technology Security Administration is responsible for developing policy of how the DoD uses ITAR exemptions, but this directive does not explain exactly what that policy is.[149] The Foreign Military Sales Handbook provides some, but very limited guidance on how the DoD should handle this exemption.[150] Agencies may authorize the use of the exemption "by submitting a written request through the Technology Security Directorate of the Defense Threat Reduction Agency."[151] One 2004 memo from the Under-Secretary of Defense offered some guidance on how the Section 124.6 exemption should be invoked by military departments, but this guidance appears to have expired in 2006.[152] Similarly, the National Security Administration, which is under the oversight of the Department of Homeland Security, appears to have its own, disparate process for authorizing ITAR exemption/exception letters

145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. DEP'T OF DEF., INSTRUCTION NO. 2040.02, Enclosure 2, ¶ 3.a, 3.p (Mar. 27, 2014), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/204002p.pdf?ver=2019-01-28-141235-830.
150. ANTHONY J. PERFILIO, FOREIGN MILITARY SALES HANDBOOK § 10:65: EXPORTS FOR U.S. GOVERNMENT END USE, n.1, Westlaw (2019).
151. *Id.*
152. Memorandum from Lisa Bronson, Deputy Under Secretary of Defense, Technology Security Policy and Counterproliferation, to Deputy Assistant Secretary of the Army for Defense Exports and Cooperation; Director, Navy International Programs Office; Deputy Under Secretary of the Air Force for International Programs, at 6 (Mar. 8, 2004) (on file with author).

via its Technology Security and Export Control Office.[153] As such, there is no standard protocol for how government officials should certify the use of ITAR exemptions, and limited confidence in the reliability of the data for the State Department to validate.

One of the most significant concerns raised by the State Department was that the DoD was improperly certifying the use of the former Section 126.4(a) to authorize contractors, asserting that the use of that exemption was reserved for United States government personnel only.[154] Guidelines issued to the military departments set forth the circumstances under which they are authorized to certify the use of Section 126.4.[155] Paragraph (d) provides that Sections 126.4(a) and (c) may be used:

> when the services of US persons (e.g., US industry) are required pursuant to the following USG activities: 1. USG sales, loans, leases or grants of defense articles, services and technical data to foreign governments . . . . 2. International cooperative armaments research, development and acquisition agreements. 3. Government-to-government military and civilian personnel exchange agreements. 4. Combined military operations and training. 5. Unilateral US military operations abroad.[156]

Thus, the memo concedes that U.S. industry is needed to support these types of missions and represents the DoD's policy of when private entities may export their services, though this interpretation was exactly what State had previously disagreed with.[157] Paragraphs (i) and (j) explain the standard for authorizing the export of hardware using Section 126.4.[158] The two paragraphs distinguish between the former Sections 126.4(a) and (c), both of which authorize temporary imports and temporary or permanent exports of defense articles, services, and technical data, but the significant distinctions between the two are that Section 126.4(a) was reserved for transfers "for official use by the Military Department, or pursuant to a USG sale, . . . or international cooperative armaments research, development or acquisition agreement administered by the Military Department"[159] and Section 126.4(j) was for transfers "for end use

153. *Technology Security and Export Control*, NAT'L SEC. AGENCY CENT. SEC. SERV., https://www.nsa.gov/business/programs/export-control-policy/ (last visited Jan. 20, 2020).
154. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 62.
155. Memorandum from Lisa Bronson, *supra* note 152, at 3 ¶ d(1)–(5).
156. *Id.*
157. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 62.
158. Memorandum from Lisa Bronson, *supra* note 152, at 4 ¶ i, j.
159. *Id.* at 4 ¶ i.

by the Military Department in a foreign country pursuant to a contract with, or pursuant to the written direction of, that Department."[160] The memo further specifies that the "[u]se of exemptions will not be certified solely for the benefit of the exporter, . . . or for exports to prohibited/embargoed/sanctioned/denied persons, destinations[,] or entities."[161]

The 2019 amendment appears to be a sign of progress in resolving this dispute among the State Department and the DoD by carving into the exemption specific circumstances under which a contractor's export is "for official use by" or "on behalf of" the government. However, in making such progress, this policy change can be interpreted as a concession by the State Department to allow contractors to take on a role in foreign policy that was traditionally deemed to be strictly governmental in nature.

3. DoD and Underreported Inherently Governmental Functions

National security operations require a long, interconnected chain of expert engineers, operators, and decision-makers to carry out missions.[162] DoD contractors perform a wide array of functions, including "professional and management support, information technology support, and weapon system support."[163] Contractors are therefore inextricably embedded with the military in ensuring mission success. Congress has acknowledged the military's growing reliance on private contractors and has since tightened the DoD's reporting requirements as to the number of contractors employed and for what types of services.[164] The GAO has found these reports to be insufficient and the volume likely inaccurate.[165]

The concern raised is that DoD contractors are performing activities that cross the line into functions that an ordinary citizen would expect to be reserved for government entities.[166] The Federal Acquisition Regulations (FAR) prohibit the use of federal contracts to private firms for the provision of inherently governmental

160. *Id.* at 4 ¶ j.
161. *Id.* at 4 ¶ k.
162. *See supra* Section III(A).
163. U.S. GOV'T ACCOUNTABILITY OFF., GAO-17-17, DOD INVENTORY OF CONTRACTED SERVICES: TIMELY DECISIONS AND FURTHER ACTIONS NEEDED TO ADDRESS LONG-STANDING ISSUES 1 (2016).
164. 10 U.S.C. § 2330a(c) (approved 2019).
165. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 163, at 10.
166. Clanahan, *supra* note 113, at 140 (citing Interview with James (Ty) Hughes, former Deputy Gen. Counsel, Acquisitions, Office of the Sec'y of the Air Force (SAF/GCQ) (Feb. 13, 2012)).

functions[167] (IGF) and lays out a non-exhaustive list of examples, including commanding military forces,[168] conducting foreign relations,[169] and directing or controlling intelligence and counter-intelligence operations.[170]

The FAR go on to outline functions that are not inherently governmental but "may approach being in that category because of the nature of the function, the manner in which the contractor performs the contract, or the manner in which the Government administers contractor performance."[171] Such functions may include "[c]ontractors participating in any situation where it might be assumed that they are agency employees or representatives."[172] These functions are referred to as "closely associated with inherently governmental functions" (CAIG).[173]

One particular function of the DoD that presents a severe risk of IGF and CAIG is in the administration of UAS programs, also known as drones.[174] The DoD currently operates more than 11,000 UAS,[175] up from 7,000 in just 2010.[176] The human resources needed for the engineering, manufacture, operation, maintenance, support, and logistics related to maintaining a single UAS is astronomical due to the rapid expansion of UAS systems for intelligence, surveillance, and reconnaissance (ISR), and general mission support.[177] UAS operations require contractor support because:

> the medium to large UAS aircraft make up only a single component of a very complex system. It involves U.S. based grounded flight operators, sensor operators, communications technicians, and imagery analysts, it includes fielded forces and personnel directing takeoff, landing and recovery procedures, and also includes forward deployed maintenance and

167. 48 C.F.R. § 7.503(a) (2020).
168. *Id.* § 7.503(c)(3).
169. *Id.* § 7.503(c)(4).
170. *Id.* § 7.503(c)(8).
171. *Id.* § 7.503(d).
172. *Id.* § 7.503(d)(13).
173. DEP'T OF DEF., HANDBOOK OF CONTRACT FUNCTION CHECKLISTS FOR SERVICES ACQUISITION 7 (May 2018), https://www.dau.edu/cop/ace/DAU%20Sponsored%20Documents/DoD_Handbook_for_Contract_Function_Checklists.pdf.
174. Clanahan, *supra* note 113, at 121.
175. *Unmanned Aircraft Systems (UAS): DoD Purpose and Operational Use*, U.S. DEP'T OF DEF., https://dod.defense.gov/UAS/ (last visited Jan. 19, 2020).
176. Peter Singer, *Unmanned Systems and Robotic Warfare*, BROOKINGS INST. (Mar. 23, 2010), https://www.brookings.edu/testimonies/unmanned-systems-and-robotic-warfare/.
177. Clanahan, *supra* note 113, at 138.

> logistics crews who keep the aircraft and payload . . . mission ready.[178]

The FAR's superficial description of inherently governmental functions fails to encapsulate the assembly line of activities that contractors perform in the operation of UAS, but given the nature of ISR missions, it could be argued that any control that a private individual has over a UAS conducting an ISR mission could be violative of Section 7.503(d). The first step in this supply chain is the transportation of the equipment, which now, due to Section 126.4(b), can be more leniently applied by the contractor. The GAO warns that "the government can become overly reliant on contractors in some situations, such as when a contractor performs functions that put an agency at risk of losing control over functions that are core to its mission and operations."[179]

The carving out of Section 126.4(b) to allow for contractors to execute the export of defense articles without a license at the mere request of the DoD is an extension of the trend toward increased contractor control over certain military functions and, as a result, diminished governmental oversight.

IV. CONCLUSION

If the goal of defense export controls is, as the AECA purports "a world which is free from the scourge of war and the dangers and burdens of armaments,"[180] then regulatory exemptions reflect instances where the need for exporters under contract with the military to act quickly and stealthily outweighs the State Department's need for oversight. Often, the policy behind the ITAR exemption hinges on the parties involved. The State Department's concession of Section 126.4 seems to rely upon its trust in its fellow federal agencies to appropriately certify and monitor the actions of its contractors exporting controlled military technology overseas. There is some cause for concern in the State Department's reliance on the DoD. GAO's findings that the DoD failed to properly report and track the use of ITAR exemptions[181] coupled with the DoD's questionable oversight of contractors performing activities closely associated with inherently governmental functions[182] call into question

178. *Id.* at 137–38.
179. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 163, at 1.
180. 22 U.S.C. § 2751.
181. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 62.
182. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 163 ("What GAO Found").

the national security risks associated with giving defense contractors greater deference in ensuring the legitimacy of their export.

It is not uncommon for weapons bought by the United States military to find themselves in the hands of those whom they were purchased to defend against.[183] An independent organization "committed to working towards understanding the landscape of illicit weapon flows"[184] found that an anti-tank missile was diverted to the Islamic State within fifty-nine days, suggesting that "that there are not many intermediaries in this chain of custody."[185]

As the global War on Terror continues and tensions escalate with Iran, the military's reliance on contractors to operate and maintain advanced weapons systems is only likely to grow. With the existence of contractor logistics support contracts, the DoD relies upon timely shipment of hardware and spares to support active weapons systems. State Department export controls apparently did not contemplate these time-sensitive and high-stakes contractual arrangements. The amendment of Section 126.4 of the ITAR is evidence of a trend toward reforming export laws to contemplate scenarios where contractors are operating less like international arms brokers and more like an extension of the DoD. The DoD must improve its oversight of private contractors in light of the State Department's increased leniency in order to minimize national security risks.

183. *E.g.*, Gabe Joselow, *ISIS Weapons Arsenal Included Some Purchased by U.S. Government*, NBC NEWS (Dec. 14, 2017, 10:51 AM), https://www.nbcnews.com/news/world/isis-weapons-arsenal-included-some-purchased-u-s-government-n829201.

184. *About Us*, CONFLICT ARMAMENT RSCH., https://www.conflictarm.com/about-us/ (last visited Jan. 20, 2020).

185. Joselow, *supra* note 183 (citing an interview with Damien Spleeters).

SCHOOL OF LAW

Volume 59 Number 2 DUQUESNE LAW REVIEW Pages 224-413 SUMMER 2021