Journal of Technology Law & Policy

Volume XXI—2020-2021

ISSN 2164-800X (online)

DOI 10.5195/tlp.2021.241

http://tlp.law.pitt.edu

Babyproofing the House Before the Hurricane: Where We Are Missing the Mark

Anokhy Desai

Abstract

Americans have felt the impacts of data breaches annually for over a decade. In the past few years, the impact and number of those breaches have increased, compromising millions of Americans' informational privacy. This Article examines the privacy protections available to Americans and the issues arising from the lack of regulations that specifically protect data privacy. Section I of this Article offers an overview of privacy in American legal history and case law, global regulatory models, and some notable privacy regulations. Section II explores where those regulatory models and the consumer experience are lacking. Section III takes lessons learned from existing privacy regulations and proposes a suggested mitigation for the national data privacy problem. Finally, Section IV provides concluding thoughts.

Babyproofing the House Before the Hurricane: Where We Are Missing the Mark

Anokhy Desai*

INTRODUCTION

This Article will examine the privacy protections offered to Americans and the issues arising from the lack of regulations that specifically protect data privacy. Americans have felt the impacts of data breaches annually for over a decade.[1] In the

* Anokhy Desai is a J.D. Candidate for the Class of 2022 at the University of Pittsburgh School of Law, and M.S. Candidate for the Class of 2022 at Carnegie Mellon University's Heinz College of Information Systems and Public Policy. She is the Executive Editor of the *Pittsburgh Journal of Technology Law and Policy*, and worked in cybersecurity and privacy prior to law school. Special thanks to Professor Jacqueline Lipton, Professor Aleecia McDonald, Erin McCarthy Holliday, Sima Lotfi, and Chris Grijalva, for all the feedback and support.

[1] David Stout, *AOL Engineer Sold 92 Million Names to Spammer, U.S. Says*, N.Y. TIMES (June 23, 2004), https://www.nytimes.com/2004/06/23/technology/aol-engineer-sold-92-million-names-to-spammer- us-says.html; Bob Sullivan, *Ameritrade Warns 200,000 Clients of Lost Data*, NBC NEWS (Apr. 19, 2005, 3:16 PM), www.nbcnews.com/id/7561268#.X0FoIZNKi8o; E. Scott Reckard & Joseph Menn, *Insider Stole Countrywide Applicants' Data, FBI Alleges*, L.A. TIMES (Aug. 2, 2008, 12:00 AM), https://www.latimes.com/archives/la-xpm-2008-aug-02-fi-arrest2-story.html; Parija B. Kavilanz, *Gap: Stolen Laptop Has Data of Job Applicants*, CNN MONEY (Sept. 28, 2007, 5:46 PM), https://money.cnn.com/2007/09/28/news/companies/gap/; *Monster Attack Steals User Data*, BBC NEWS, news.bbc.co.uk/2/hi/6956349.stm (last updated Aug. 21, 2007); Jan Libbenga, *Norway Sends Entire Citizenry's ID Info to Media*, THE REGISTER (Sept. 18, 2008), https://www.theregister.com/2008/09/18/tax_office_blooper_shocks_norway/; Robert McMillan, *Data Theft Creates Notification Nightmare for BlueCross*, COMPUTERWORLD (Mar. 1, 2010, 8:23 PM), https://www.computerworld.com/article/2520155/data-theft-creates-notification-nightmare-for-bluecross.html; Miguel Helft, *AT&T Said to Expose iPad Users' Addresses*, N.Y. TIMES (June 9, 2010), https://www.nytimes.com/2010/06/10/technology/10apple.html; Ilana Greene, *Citigroup Data Breach: A Lesson and Warning For All*, FORBES (June 13, 2011, 10:04 PM), https://www.forbes.com/sites/ilanagreene/2011/06/13/citigroup-data-breach-a-lesson-and-warning-for-all/#7e822fc24817; *Blizzard Battle.Net Hack Attack Hits Millions*, BBC NEWS (Aug. 10, 2012), https://www.bbc.com/news/technology-19207276; Greg Kumparak, *Apple Confirms That Its Dev Center Has Been Breached By Hackers*, TECHCRUNCH (July 21, 2013, 6:43 PM), https://techcrunch.com/2013/07/21/apple-confirms-that-the-dev-center-has-potentially-been-breached-by-hackers/; Brian Fung, *A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix?*, WASH. POST (Jan. 1, 2014, 11:16 AM), https://www.washingtonpost.com/news/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/; Kate Vinton, *With 56 Million Cards Compromised, Home Depot's Breach Is Bigger Than Target's*, FORBES (Sept. 18, 2014, 8:21 PM), https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/; Kate Vinton, *CVS Investigates Credit Card Breach At Its Online Photo Service*, FORBES (July 17, 2015, 2:41 PM), https://www.forbes.com/sites/katevinton/2015/07/17/cvs-investigates-credit-card-breach-at-its-online-photo-service/; Eric Lichtblau, *Hackers Get Employee Records at Justice and Homeland Security Depts.*, N.Y. TIMES (Feb. 8, 2016), https://www.nytimes.com/2016/02/09/us/hackers-access-employee-records-at-

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

past few years, the impact and number of those breaches have increased, compromising millions of Americans' informational privacy.[2] The right to privacy

justice-and-homeland-security-depts.html; Lily Hay Newman, *Security News This Week: The Deloitte Breach Was Worse Than We Thought*, WIRED (Sept. 30, 2017, 8:00 AM), https://www.wired.com/story/security-news-of-the-week-deloitte-sonic-whole-foods-breach/; Sarah Perez & Zack Whittaker, *Everything You Need To Know About Facebook's Data Breach Affecting 50M Users*, TECHCRUNCH (Sept. 28, 2018, 4:48 PM), https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/; Rob McLean, *A Hacker Gained Access To 100 Million Capital One Credit Card Applications And Accounts*, CNN, https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html (last updated July 30, 2019, 5:17 PM); Anthony Spadafora, *Hundreds of millions of Instagram, TikTok, YouTube accounts compromised by data breach*, TECHRADAR (Aug. 21, 2020), https://www.techradar.com/news/hundreds-of-millions-of-instagram-tiktok-youtube-accounts-compromised-by-data-breach.

[2] David Stout, *AOL Engineer Sold 92 Million Names to Spammer, U.S. Says*, N.Y. TIMES (June 23, 2004), https://www.nytimes.com/2004/06/23/technology/aol-engineer-sold-92-million-names-to-spammer-us-says.html; Bob Sullivan, *Ameritrade Warns 200,000 Clients of Lost Data*, NBC NEWS (Apr. 19, 2005, 3:16 PM), www.nbcnews.com/id/7561268#.X0FoIZNKi8o; E. Scott Reckard & Joseph Menn, *Insider Stole Countrywide Applicants' Data, FBI Alleges*, L.A. TIMES (Aug. 2, 2008, 12:00 AM), https://www.latimes.com/archives/la-xpm-2008-aug-02-fi-arrest2-story.html; Parija B. Kavilanz, *Gap: Stolen Laptop Has Data of Job Applicants*, CNN MONEY (Sept. 28, 2007, 5:46 PM), https://money.cnn.com/2007/09/28/news/companies/gap/; *Monster Attack Steals User Data*, BBC NEWS, news.bbc.co.uk/2/hi/6956349.stm (last updated Aug. 21, 2007); Jan Libbenga, *Norway Sends Entire Citizenry's ID Info to Media*, THE REGISTER (Sept. 18, 2008), https://www.theregister.com/2008/09/18/tax_office_blooper_shocks_norway/; Robert McMillan, *Data Theft Creates Notification Nightmare For BlueCross*, COMPUTERWORLD (Mar. 1, 2010, 8:23 PM), https://www.computerworld.com/article/2520155/data-theft-creates-notification-nightmare-for-bluecross.html; Miguel Helft, *AT&T Said to Expose iPad Users' Addresses*, N.Y. TIMES (June 9, 2010), https://www.nytimes.com/2010/06/10/technology/10apple.html; Ilana Greene, *Citigroup Data Breach: A Lesson and Warning For All*, FORBES (June 13, 2011, 10:04 PM), https://www.forbes.com/sites/ilanagreene/2011/06/13/citigroup-data-breach-a-lesson-and-warning-for-all/#7e822fc24817; *Blizzard Battle.Net Hack Attack Hits Millions*, BBC NEWS (Aug. 10, 2012), https://www.bbc.com/news/technology-19207276; Greg Kumparak, *Apple Confirms That Its Dev Center Has Been Breached By Hackers*, TECHCRUNCH (July 21, 2013, 6:43 PM), https://techcrunch.com/2013/07/21/apple-confirms-that-the-dev-center-has-potentially-been-breached-by-hackers/; Brian Fung, *A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix?*, WASH. POST (Jan. 1, 2014, 11:16 AM), https://www.washingtonpost.com/news/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/; Kate Vinton, *With 56 Million Cards Compromised, Home Depot's Breach Is Bigger Than Target's*, FORBES (Sept. 18, 2014, 8:21 PM), https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/; Kate Vinton, *CVS Investigates Credit Card Breach At Its Online Photo Service*, FORBES (July 17, 2015, 2:41 PM), https://www.forbes.com/sites/katevinton/2015/07/17/cvs-investigates-credit-card-breach-at-its-online-photo-service/; Eric Lichtblau, *Hackers Get Employee Records at Justice and Homeland Security Depts.*, N.Y. TIMES (Feb. 8, 2016), https://www.nytimes.com/2016/02/09/us/hackers-access-employee-records-at-justice-and-homeland-security-depts.html; Lily Hay Newman, *Security News This Week: The Deloitte Breach Was Worse Than We Thought*, WIRED (Sept. 30, 2017, 8:00 AM), https://www.wired.com/story/security-news-of-the-week-deloitte-sonic-whole-foods-breach/; Sarah Perez & Zack Whittaker, *Everything You Need To Know About Facebook's Data Breach Affecting 50M Users*, TECHCRUNCH (Sept. 28, 2018, 4:48 PM), https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/; Rob McLean, *A Hacker Gained Access To 100 Million Capital One Credit Card Applications And Accounts*, CNN, https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html (last updated July 30, 2019, 5:17 PM); Anthony Spadafora, *Hundreds of millions of Instagram, TikTok, YouTube accounts compromised by data breach*, TECHRADAR (Aug. 21, 2020), https://www.techradar.com/news/hundreds-of-millions-of-instagram-tiktok-youtube-accounts-compromised-by-data-breach.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

feels fundamentally American and has been repeatedly defended in our legal history, yet nowhere in our Constitution does it explicitly say all Americans have such a right. To combat this conflict between the amount of privacy we expect and the amount we experience, the United States should enact data privacy legislation similar to the European Union's General Data Protection Regulation (GDPR). Congress must provide an agency, such as the FTC, the power to create and maintain an enforceable comprehensive model data privacy regulation. A codified national regulation would allow the American public to hold the private sector accountable for misusing their data and breaching their informational privacy. Section I of this Article offers an overview of privacy in American legal history and case law, global regulatory models, and some notable privacy regulations. Section II explores where those regulatory models and the consumer experience are lacking. In Section III, I take lessons learned from existing privacy regulations and propose a suggested mitigation for the national data privacy problem. Finally, Section IV provides concluding thoughts.

I. PRIVACY LAW

A. In American Legal History

Privacy has long existed as a legal concept in torts, property law, and, arguably, the Constitution. Over the last century, the Supreme Court has considered a progression of cases which expanded individual privacy rights protected by certain constitutional amendments.[3] While the Court has relied on frameworks, like Justice Rehnquist's "history and traditions" test to determine whether specific liberty rights are afforded by the Fourteenth Amendment's Due Process Clause, the Court in *Lawrence* indicated that the list of privacy issues protected by the Constitution may grow as an outcome of changing times and the growth associated with each generation.[4] History and traditions should be treated merely as "the starting point but not in all cases the ending point of the substantive due process inquiry."[5]

1. The Legal Notion of Privacy

The legal notion of privacy protections can be found in multiple legal subject areas, including torts and property law. Noted torts scholar William Prosser

[3] *See infra* note 10.

[4] Larry J. Pittman, *The Elusive Constitutional Right to Informational Privacy*, 19 NEV. L.J. 135, 142. (2018).

[5] Lawrence v. Texas, 539 U.S. 558, 572 (2003) (citing Sacramento v. Lewis, 523 U.S. 833, 857 (1998)).

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

originally categorized invasion of privacy into four groups within tort law.[6] These include: intrusion upon a plaintiff's seclusion, solitude, or private affairs; public disclosure of private facts; publicity that places a plaintiff in false light; and appropriation of a plaintiff's name or likeness.[7] Within this categorization, a breach of informational privacy would fall under public disclosure of private facts. "Unlike libel or slander, truth is not a defense for invasion of privacy."[8] If this is interpreted to include modern technology, it would inculpate firms whose databases of personal information, like home addresses and health information, are breached, and just because that published or leaked information about individuals is true does not absolve the firm from invading those individuals' personal privacy.

In property law, the castle doctrine is the closest analogy to privacy protections. *Black's Law Dictionary* defines the castle doctrine as an "exception to the [rule to withdraw from a dangerous situation] allowing the use of deadly force to protect one's own home and its inhabitants from attack, especially from a trespasser who intends to commit a felony or inflict serious bodily harm."[9] The doctrine allows an individual to protect their private property from unauthorized entrants. Broadly interpreted to include modern technology, it would give individuals the right to protect their information from attack, placing the responsibility to safeguard individuals' information on firms.

2. The Supreme Court's Holding on Privacy

Though the right to privacy does not appear explicitly in the Constitution, The Supreme Court has historically interpreted the Bill of Rights and the Fourteenth Amendment to include such protections. A number of 20th and 21st century Supreme Court cases form the foundation for what privacy means in the digital age.[10]

In Samuel Warren and Louis Brandeis' 1890 law review article, "The Right to Privacy," a soon-to-be-appointed Justice Brandeis describes the "right to be let alone" as being able to live one's private life in peace, specifically in the context of

---

[6] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[7] RESTATEMENT (SECOND) OF TORTS § 652 (AM. L. INST. 1977).

[8] *The Right to Privacy*, WAY BACK MACHINE—INTERNET ARCHIVE (May 14, 2012), https://web.archive.org/web/20120514050702/http://www.cvc.sunysb.edu/334/ethics/Privacy.html (citing an article from SUNY Stony Brook that is no longer available).

[9] *Castle Doctrine*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[10] *See* Olmstead v. United States, 277 U.S. 438 (1928); Katz v. United States, 389 U.S. 347 (1967); Griswold v. Connecticut, 381 U.S. 479 (1965); Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992); Washington v. Glucksberg, 521 U.S. 702 (1997); Lawrence v. Texas, 539 U.S. 558 (2003); Obergefell v. Hodges, 135 S. Ct. 2584 (2015); Riley v. California, 573 U.S. 373 (2014); Carpenter v. United States, 138 S. Ct. 2206 (2018).

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

protecting individual privacy from becoming publicized.[11] His description of the principle of protecting individual privacy directly aligns with the data privacy regulations called for by this Article. The Fourth Amendment mirrors this principle by providing a "right . . . to be secure" against unreasonable government intrusion.[12] The Fourteenth Amendment's protection of liberty similarly supports the argument that the right to privacy exists in the Constitution.[13] These two Amendments are the primary focus of the following cases.

a. Olmstead v. United States *(1928)*

In *Olmstead*, the petitioners were convicted of conspiracy to violate the National Prohibition Act.[14] Prohibition officers gathered evidence of this illegal activity by wiretapping the phone lines of four of the petitioners.[15] The Court held that because the physical wiretaps were located along phone lines on public property, the evidence was collected without trespassing upon the individuals' properties, and thus the search did not require a warrant and did not violate the Fourth Amendment.[16]

Justice Brandeis dissented, stating that because the government itself conceded that wiretaps constitute a search and seizure, the Fourth Amendment requires warrants for such searches.[17] Additionally, he pointed out that the wiretaps essentially forced the petitioners to act as witnesses against themselves, violating the Fifth Amendment.[18] Despite the "subtler and more far-reaching means of invading privacy . . . available to the Government,"[19] Brandeis continues, the founding fathers intended to protect "the right to be let alone," and thus "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[20]

---

[11] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[12] U.S. CONST. amend. IV.

[13] Pittman, *supra* note 4, at 141–52.

[14] *Olmstead*, 277 U.S. at 455.

[15] *Id.* at 456–57.

[16] *Id.* at 469.

[17] *Id.* at 471–72.

[18] *Id.*

[19] *Id.* at 473.

[20] *Id.* at 478.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

Brandeis' interpretation was soon upheld in *Katz*, which overturned *Olmstead*.[21] In *Katz*, FBI agents placed listening and recording devices outside the public phone booth the petitioner made calls from.[22] The Court held that this wiretapping, though conducted on a public phone booth with "no physical [trespass] to the area occupied by the petitioner,"[23] was unconstitutional and violated the Fourth Amendment, because the Amendment "protects people—and not simply "areas"—against unreasonable search and seizures . . . ."[24]

b. **Griswold v. Connecticut *(1965)***

The defendants, a director of a medical clinic and a doctor, were convicted of violating a state law that prohibited them from dispensing birth control devices to married couples.[25] The Court reversed the convictions, holding that the privacy rights implicit in the Bill of Rights protected the decisions made in one's private life.[26] The Court discussed the privacy protections in the Third Amendment's right to refuse to quarter soldiers without consent, the Fourth Amendment's right to be secure from unreasonable searches and seizures, the Fifth Amendment's protection against self-incrimination, and the Ninth Amendment's right to have rights not enumerated in the Constitution.[27] The majority also touched on the Fourteenth Amendment's protection of liberty and First Amendment's freedom of speech and press as fundamental personal rights, concluding that "the First Amendment has a penumbra where privacy is protected from governmental intrusion."[28]

c. **Planned Parenthood v. Casey *(1992)***

Essentially a rehashing of *Roe v. Wade*,[29] Planned Parenthood asked the question of whether a state's anti-abortion statute violated the Due Process Clause.[30] The Court reaffirmed *Roe*'s main holding, clarifying that this Constitutional protection of a woman's decision over her pregnancy "derives from the Due Process

[21] Katz v. United States, 389 U.S. 347, 347 (1967).

[22] *Id.* at 348.

[23] *Id.* at 359.

[24] *Id.* at 353.

[25] Griswold v. Connecticut, 381 U.S. 479, 480 (1965).

[26] *Id.* at 493.

[27] *Id.* at 479–86.

[28] *Id.* at 483–87.

[29] Roe v. Wade, 410 U.S. 113, 113 (1973) (holding that the Due Process Clause contains an inherent right to privacy that protects a woman's choice to have an abortion).

[30] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 833 (1992).

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

Clause of the Fourteenth Amendment.[31] It declares that no State shall 'deprive any person of life, liberty, or property, without due process of law.' The controlling word in the cases before us is 'liberty.'"[32]

d. Washington v. Glucksberg *(1997)*

The respondents, four physicians who treated terminally ill patients, believed Washington state's classification of assisted suicide as a felony was unconstitutional under the Due Process Clause.[33] The Court disagreed, stating that it "has regularly observed that the [Due Process] Clause specially protects those fundamental rights and liberties which are, objectively, deeply rooted in this Nation's history and tradition."[34]

Though the ruling seemed contrary to the earlier protections of some bodily and decisional autonomy prescribed in *Planned Parenthood*, the focus on the "history and traditions" test showed the Court's consistency in the two decisions. The right to assist another individual's suicide did not track with societal norms, but the privacy rights inherent in bodily and decisional autonomy did.

e. Lawrence v. Texas *(2003)*

The Court considered whether a Texas statute that made it illegal for individuals of the same sex to engage in intimate sexual conduct violated the Due Process Clause.[35] It held that the statute was unconstitutional, a holding consistent with the *Griswold* and *Roe* clarifications of the liberty and personal decision-making protections in the Fourteenth Amendment.[36] While same-sex marriages were not yet legal at the time, the "history and traditions" test indicated that prior holdings had paved the way for Fourteenth Amendment protections for intimate relations between same-sex couples.[37] The majority wrote:

> "Had those who drew and ratified the Due Process Clauses of the Fifth Amendment or the Fourteenth Amendment known the components of liberty in its manifold possibilities, they might have been more specific. . . . They knew times can blind us to certain

[31] *Id.* at 846.

[32] *Id.*

[33] Washington v. Glucksberg, 521 U.S. 702, 707–08 (1997).

[34] *Id.* at 703.

[35] Lawrence v. Texas, 539 U.S. 558, 562 (2003).

[36] *Id.* at 564–67.

[37] *See id.* at 570.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

> truths and later generations can see that laws once thought necessary and proper in fact serve only to oppress. As the Constitution endures, persons in every generation can invoke its principles in their own search for greater freedom."[38]

f. Obergefell v. Hodges *(2015)*

Building on *Glucksberg* and *Lawrence*, the Court in *Obergefell* expanded on the Fourteenth Amendment's liberty interest and held that the Amendment protected same-sex couples' right to marry.[39] Echoing *Lawrence*, the Court stated, "[h]istory and tradition guide and discipline this inquiry but do not set its outer boundaries. . . . That method respects our history and learns from it without allowing the past alone to rule the present."[40]

g. Riley v. California *(2014)*

An officer stopped the petitioner for a traffic violation and searched his person and phone.[41] The officer noticed that the petitioner used certain terminology in his texts linking him with a gang and potentially with a recent shooting.[42] During his trial for multiple convictions resulting from that evidence, the petitioner contended that the search and seizure of his phone were performed without a warrant and that the associated evidence taken from his phone was in violation of the Fourth Amendment and thus inadmissible.[43] The Court agreed and required that police officers must obtain a warrant before searching cell phones and digital devices.[44] While statutes may not account for the vast quantity of sensitive personal information now held on smart phones, the fact that modern day individuals carry around this amount of personal data instead of hiding it at home does not make their privacy "any less worthy of the protection for which the Founders fought."[45]

---

[38] *Id.* at 578–79.

[39] *See* Obergefell v. Hodges, 576 U.S. 644, 681 (2015).

[40] *Id.* at 664.

[41] Riley v. California, 573 U.S. 373, 378–79 (2014).

[42] *Id.* at 379.

[43] *Id.*

[44] *Id.* at 403.

[45] *Id.*

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

h. Carpenter v. United States *(2018)*

One of four men suspected of armed robbery was arrested and provided his cell phone to the FBI.[46] The FBI used phone numbers of the other participants found therein to obtain cell phone location records that placed the other three men, including the petitioner, at the robbery, leading to six counts of robbery and other charges.[47] The petitioner asserted that because his physical location was collected through cell phone location records that were obtained without a warrant, his Fourth Amendment right was violated.[48] Restating *Riley* and explaining that a person's reasonable expectation of privacy includes not expecting to have physical movements tracked through cell phone records, the Court held that the warrantless acquisition of cell phone records violated the petitioner's Fourth Amendment right. The Court referred back to Brandeis' dissent in *Olmstead*, writing, "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[49]

B. In Practice

Understanding the regulations currently protecting or failing to protect Americans' privacy depends on understanding the terms commonly used within them. An organization or entity that collects and stores data is a controller, while the entity that processes that data for business purposes like advertising or internal analytics is a processor.[50] An entity can sometimes be both the controller and the processor.[51] An individual whose data is being collected is a data subject, and data that contains personal information that can be traced back to that individual is personal data, and can sometimes qualify as personally identifiable information (PII).[52] The granularity of the definition of PII varies between regulations and even organizational policies.

The European Union enacted the General Data Protection Regulation (GDPR) in May of 2018 to protect the personal data and privacy rights of individuals in the

---

[46] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[47] *Id.*

[48] *Id.*

[49] *Id.* at 2223 (citing Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).

[50] *What is GDPR, The EU's New Data Protection Law?*, GDPR.EU (last visited Feb. 21, 2020), https://gdpr.eu/what-is-gdpr/?cn-reloaded=1.

[51] *Id.*

[52] *Id.*

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

EU.[53] GDPR contains 99 articles detailing privacy and technology rules that make other national privacy regulations pale in comparison, most of which are not discussed in this paper for brevity; however, a few examples are outlined below to illustrate its breadth and approach.[54]

An update to the 1995 EU Privacy Directive that required data processing, collection, and retention be limited, recommended Privacy by Design—privacy that is integrated into organizational processes from the inception of those process, and allowed data subjects to be able to edit their data to maintain a certain level of privacy and consent from the data subject. By creating this update, GDPR added a new right of data portability.[55]

Data portability allows the data subject to request their data be moved from one controller's databases to another's.[56] Not only are entities with at least 250 employees required to comply with GDPR, they also must employ a Data Protection Officer to provide expertise on data protection laws and procedures.[57] Small businesses with fewer than 250 employees are still required to be GDPR-compliant if they regularly process the personal data of international data subjects.[58] GDPR also mandates that controllers report any security breach where data was stolen, changed, lost, or accidentally disclosed "within 72 hours of discovery," one of the strictest breach notification requirements in the world right now.[59] The fine for being noncompliant is up to €20 million or 4% of annual revenue, whichever is higher.

Other countries have taken inspiration from GDPR and enacted similar regulations. South Africa enacted the Protection of Personal Information Act (POPIA) in November 2013.[60] Though it went into effect first, parts of POPIA were borrowed directly from released GDPR drafts.[61] Despite this, its scope is

---

[53] *Id.*

[54] GENERAL DATA PROTECTION REGULATION, https://gdpr-info.eu/ (May 25, 2018) [hereinafter GDPR].

[55] *What Is GDPR, The EU's New Data Protection Law?*, *supra* note 50; 1995 O.J. (L 281) 9.

[56] RIGHT TO DATA PORTABILITY, https://gdpr-info.eu/art-20-gdpr/ (last visited Feb. 21, 2020).

[57] *Article 30 Records of Processing Activities*, EU GDPR (last visited Feb. 21, 2020), http://www.privacy-regulation.eu/en/article-30-records-of-processing-activities-GDPR.htm.

[58] *Id.*

[59] CONTROLLER AND PROCESSOR, https://gdpr-info.eu/chapter-4/ (last visited Feb. 21, 2020).

[60] Russell Nel, *GDPR Matchup: South Africa's Protection of Personal Information Act*, IAPP (Sept. 5, 2017), https://iapp.org/news/a/gdpr-matchup-south-africas-protection-of-personal-information-act/.

[61] *Id.*

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

jurisdictionally much more limited than GDPR; POPIA applies to the personal information of data subjects and legal entities processed in South Africa, while GDPR applies to the personal data of all data subjects from EU member countries, regardless of where that data is collected or processed.[62] All businesses, no matter the size, must have a Data Protection Officer and report breaches "as soon as reasonably possible."[63] Finally, organizations within South Africa that do not follow POPIA are fined up to 10 million ZAR, which is roughly 3% of GDPR's maximum fine.[64]

Within the United States, California was the first state to enact a comparable privacy law. While every state has its own breach notification rule,[65] no other state has passed a thorough privacy regulation.[66] The California Consumer Privacy Act (CCPA) was signed in 2018 and went into effect on January 1, 2020.[67] CCPA adds onto current state laws, providing for further privacy protections for state residents.[68] Organizations that have at least $25 million in revenue, have personal information from at least 50,000 residents, devices, or households, or make 50% or more of their annual revenue from selling resident data must comply with CCPA. These rules cover many companies that GDPR would not. The fine for noncompliance is $7,500 per intentional violation, and $2,500 per unintentional violation that is not addressed within thirty days of notice.[69] In order to comply, companies can create an inventory of California resident data that has been collected or processed, create California resident-facing sites, create a toll-free hotline for residents to submit requests to access their data, provide a "Do Not Sell My Information" link on their site's homepage, update their privacy policy and data collection processes, and proactively determine the age of their data subjects to avoid being fined for collection of data from minors, among other privacy-protection measures.[70] Reading through the other California Civil Code sections, it becomes clear that CCPA is not simply based off of GDPR, but also builds on it. CCPA includes basic privacy requirements that can

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] For example, ALA. CODE § 8-38-12, TEX. CODE ANN. § 2054.1125.

[66] Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, IAPP (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

[67] *Id.*

[68] CAL. CIV. CODE §§ 1798.100-.199 (West 2018).

[69] *Id.* § 1798.155.

[70] *Id.* § 1798.135.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

be found in GDPR, as well as stricter elements like requiring organizations to have a hotline for data subjects, broadening the definition of "personal data," and widening eligibility requirements for organizations that must comply.

C. Global Models

At the beginning of this decade, over eighty countries had data protection frameworks in place.[71] As of the end of 2019, fifty-two more countries have joined that list.[72] These countries have employed one or more of four models: the comprehensive, sectoral, co-regulatory, or self-regulatory model.[73]

Countries that follow the comprehensive model "govern the collection, use, and dissemination of personal information" through an agency or other data protection authority (DPA).[74] The EU's GDPR is a notable example of the comprehensive model; GDPR acts as a one-size-fits-all regulation that certain businesses worldwide must employ to be compliant and avoid fines. Each EU member country has its own DPA, which in turn answers to the EU DPA.

Countries that follow the sectoral model govern only certain aspects or types of personal information. The sectoral model protects privacy by enacting laws that require companies within certain industries to take data protection measures. Like the comprehensive model, the sectoral model uses data protection authorities. The United States enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996 to address the use and disclosure of individual health information and provide a privacy standard for medical and health information.[75] The U.S. Department of Health and Human Services (HHS) ensures accountability to HIPAA and is responsible for updating the act as needed.[76]

Co- and self-regulatory models both involve a mix of governmental and independent institutions that protect personal information. Industries use the co-regulatory model to enforce privacy and data protection standards in conjunction

---

[71] Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills*, 157 PRIVACY LAWS & BUS. INT'L REP., Jan. 2019, at 1, 1–15.

[72] *Id.*

[73] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 31 (International Association of Privacy Professionals 2012).

[74] *Id.*

[75] *Summary of the HIPAA Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last updated July 26, 2013).

[76] *HIPAA Updates*, HIPAA J., https://www.hipaajournal.com/category/hipaa-updates/ (last updated July 14, 2020).

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

with existing national and state laws.[77] Ireland, for example, allows for codes produced by trade associations and other industry groups to go into effect after being approved by the Data Protection Commissioner and both houses of Parliament.[78] In some countries, industries use the self-regulatory model to enforce standards without the basis of existing laws. This model can be successful in some cases, such as the Payment Card Industry (PCI) Data Security Standard. In 2006, American Express, Discover Financial Services, JCB International, and Visa Inc. formed the PCI Security Standards Council to enforce global payment card security standards like protecting cardholder data and maintaining an information security policy, among other controls.[79]

II. MISSING THE MARK

A. Where the Models are Lacking

While it is not necessarily a weakness that the comprehensive model may be too strict for companies that do not collect or process PII or high-risk personal data, critics point out that the bureaucratic and financial resources required to implement such a model successfully are often hard to obtain and outweigh the risk of personal data being exfiltrated or otherwise compromised.[80] One finds support for this when considering how small the list of countries is where the comprehensive model has been successful; so far, only the European Union has implemented privacy regulations on this scale.[81] Even then, over one quarter of the EU member states were not prepared for GDPR when the deadline arrived.[82] GDPR has also faced thousands of proposed amendments since its enactment reflecting administrative costs that smaller governments, like those of U.S. states, could struggle with.[83] However, the

[77] *See* AHMAD & SWIRE, *supra* note 73, at 33.

[78] Section 13 Data Protection Act (1988) (Ir.), www.irishstatutebook.ie/eli/1988/ act/25/section/13/ enacted/en/html.

[79] A.M. Parker, *An Introduction to PCI DSS*, CRYPTOMATHIC (Mar. 23, 2018), https://www .cryptomathic.com/news-events/blog/an-introduction-to-pci-dss.

[80] *See* AHMAD & SWIRE, *supra* note 73.

[81] *See* GREENLEAF, *supra* note 71.

[82] Nikolaj Nielsen, *Eight Countries to Miss EU Data Protection Deadline*, EU OBSERVER (May 18, 2018), https://euobserver.com/justice/141860 (stating "Despite having two years to get their domestic legal acts sorted, Belgium, Bulgaria, Cyprus, the Czech Republic, Greece, Hungary, Lithuania and Slovenia will not be ready until far beyond the 25 May deadline.").

[83] *EU Council Presidency Releases Proposed Amendments to Draft ePrivacy Regulation*, HUNTON ANDREWS KURTH (Feb. 27, 2020), https://www.huntonprivacyblog.com/2020/02/27/eu-council-presidency-releases-proposed-amendments-to-draft-eprivacy-regulation/.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

tradeoff to these costs is that strict protections are better for user privacy, and changes across industries and jurisdictions can be enacted through a single body.

The sectoral model works best when different industries are regulated based on the risk level of the information they handle. For example, health information should have stricter privacy protection requirements than retail purchase information. A downside of using the sectoral model is that regulations that are not regularly updated can face the same privacy issues they strive to prevent due to the lag time between when a new technology is released and when an update to the regulation is written, edited, agreed upon, and finally enacted.[84] For instance, it took seven years for the Privacy Rule[85] and Security Rule[86] to be added to HIPAA. For those seven years, there were no rules within the act making it mandatory for institutions to obtain patient authorization for the use and disclosure of their private health information, giving patients the right to examine and request copies of their health records, or requiring health data to be encrypted.[87] In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was introduced, requiring privacy health vendors like Google Health and Microsoft HealthVault to provide breach notifications when private health information is accessed or exfiltrated by unauthorized parties.[88] While impressive that gaps in HIPAA's privacy protection were filled every few years to address new technologies, this is often not the case in countries that follow the sectoral model. More often than not, due to the same financial and bureaucratic resources necessary for the comprehensive model, and to the rotating door of political regimes that provide those resources, the sectoral model quickly lends itself to becoming an outdated source of loopholes for noncompliant organizations. An example of this is the U.S.'s Privacy Act of 1974, controlled by the Federal Trade Commission (FTC). According to the Department of Justice (DoJ), the act "governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."[89] Some important and forward-thinking measures the act put in place include providing individuals notice about which governmental agencies have their information, prohibiting individual data disclosure without obtaining the individual's

[84] *See* AHMAD & SWIRE, *supra* note 73, at 32.

[85] *See* HIPAA § 264(a), 110 Stat. 2024 at 2033.

[86] *See* HIPAA § 264, 110 Stat. 2024 at 2033–34.

[87] *The HIPAA Privacy Rule*, HEALTH AND HUM. SERV. (last visited Feb. 21, 2020), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[88] *See* AHMAD & SWIRE, *supra* note 73, at 32.

[89] *Privacy Act of 1974*, DEP'T OF JUST. (last visited Feb. 21, 2020), https://www.justice.gov/privacy-act-1974.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

consent or meeting one of twelve statutory exceptions, and creating a way for individuals to access and amend their data.[90] Unfortunately, no updates regarding new technologies have been made to the Privacy Act since its creation almost 50 years ago. This means the act has not been modernized to reflect the informational privacy concerns arising from the invention of the Internet. The FTC has not extended this act to cover the private sector either.

Meanwhile, the co-regulatory model is more of a theory than a reality.[91] In co-regulation, agencies and industry groups theoretically collaborate to develop policies that, in the best case scenario, are approved by the government to become national law.[92] Ireland's Data Protection Act, for example, has a code about breach notifications that the Office of Data Protection Commission (ODPC) treats as best practice, rather than authoritative laws the private sector must abide by.[93] All ODPC-approved codes have otherwise been geared to the public sector.[94] Even with GDPR's delineation of co-regulatory rules, it is unclear whether Ireland has taken steps towards compliance by solidifying its co-regulatory practice.[95]

Lastly, the self-regulatory model has its own accountability issues. Even the most notable instance of self-regulation was motivated by consequences laid out in existing regulations. PCI DSS was created because the increase in credit card fraud and scams at the time, in conjunction with the Truth in Lending Act's (TILA) stipulation that the credit card companies were liable for large fraudulent charges, meant the companies had to take immediate action to stop losing money.[96] While industry-developed policies like PCI DSS can be updated for modern technology relatively quickly but since the policies do not have to undergo multiple passes of governmental scrutiny, there is no incentive to update policies if the current version mostly addresses modern issues. There is no requirement or monetary incentive to

---

[90] *Id.*

[91] William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 980 (2016).

[92] *Id.*

[93] *Id.* (citing PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO IRISH AND EU LAW 12–17, 71 (2010)); DATA PROTECTION ACT 2003 (Act No. 6/2003) (Ir.) (last visited Feb. 21, 2020), http://www.irishstatutebook.ie/2003/ en/act/pub/0006/index.html.

[94] DATA PROTECTION COMM'R, ANNUAL REPORT OF THE DATA PROTECTION COMMISSIONER OF IRELAND 11 (2014), https://www.dataprotection.ie/sites/default/files/uploads/ 2018-11/Annual% 20Report%202014.pdf.

[95] *See* McGeveran, *supra* note 91, at 981; GDPR arts. 40–43 (2018).

[96] REGULATION Z, 12 C.F.R. 1026.4 (2011), https://www.fdic.gov/regulations/laws/rules/6500-200.html#fdic6500101#fdic6500101.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

update them.[97] Additionally, the strength of enforcement may not be appropriate in all cases; violating an industry regulation on software updates may carry the same hefty fine as failing to follow data retention policies.[98] Finally, industries that are allowed to create their own regulations will do so based on the incentives of profit or shareholder benefit rather than based on the concern for civil rights that presumably animates governmental agencies. While PCI DSS seems like a success for the self-regulatory model, these companies only had an incentive to protect user privacy because other governmental regulations (TILA) tied that privacy to their own profits. This illustrates why in most other cases, industries simply fail to protect their users' data.

B. Where the Consumer Experience Is Lacking

When a consumer signs up for a new service, he or she must agree to the terms and conditions and privacy policy to finish the account creation or application installation process. Regardless of whether the new account is for a social media site or a banking app, the user must agree to that company's policies if they wish to use the service. More often than not, users will click the "Agree" or "Okay" button to continue without reading the policies. It is understandable that users do not read about how their privacy may be infringed if they finish creating their account; privacy policies are intentionally dense and unnecessarily long. To meet industry guidelines, companies will often add boilerplate language to their privacy policies without any trimming or editing, making it harder for the average user to understand how this language applies to them and their intended use of the product. On top of this, longer terms and conditions can be used to disincentivize the user from discovering what exactly they are agreeing to.[99]

Carnegie Mellon University professor and former Chief Technologist of the Federal Trade Commission Lorrie Faith Cranor found that it would take more than 200 hours for the average Internet user to read all of the privacy policies for all the websites they visit each year, not including third-party advertiser and analytics policies that users implicitly accept just by visiting those websites.[100] Nationally, that equates to an estimated economic loss of $365 billion per year.[101] In his study about public knowledge of technology and the web, University of Pennsylvania

---

[97] *See* AHMAD & SWIRE, *supra* note 73, at 34.

[98] *Id.*

[99] *See generally* Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. L. & POL'Y FOR THE INFO. SOC'Y 543 (2008).

[100] *Id.* at 563.

[101] *Id.* at 544.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

communications professor Joseph Turow found that "most people don't actually read privacy policies" and assume that the title implies it describes how a company will keep user information private.[102] Turow confirms that privacy policies are filled with technical jargon clearly not meant for consumers.[103] One of the questions in Turow's study asks users to determine if the following statement is true or false: "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users." 52% of Internet users incorrectly believed this statement was true.[104]

Based on these studies, users believe that companies that update or have privacy policies are actively protecting user privacy, when in fact they may be exposing that data to breaches or selling it to third parties. If companies are protecting user privacy as consumers believe, then the user has no reason to read through the unnecessarily complex and lengthy policies they are required to accept to begin or continue using a company's services. If consumers do not read these policies, they are unlikely to object to them. If there are no objections, companies have no incentive to improve these policies, and therefore they remain vulnerable or continue selling user data. The private sector relies on this negative feedback loop to avoid implementing more robust protections for user privacy.

III. DISCUSSION AND MITIGATION

A. Lessons Learned from Existing Regulations

Before GDPR was implemented, American companies that faced data breaches had to update their state's Attorney General, follow that state's breach notification laws, and notify shareholders and the affected parties. That may seem tedious, but pre-GDPR, this process did not carry any significant fines or punishments for what was often technological irresponsibility or a lack of proper data security measures. In the now infamous Cambridge Analytica scandal, Facebook allowed third-party developers to access user data and target users, all without user consent.[105] Before GDPR went into effect, the UK's Information Commissioner's Office (ICO) fined Facebook only £500,000, despite the over 1 million UK users who were affected and

[102] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH CENTER (Dec. 4, 2014), https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/.

[103] *Id.*

[104] *Id.*

[105] Jim Waterson, *UK Fines Facebook £500,000 for Failing to Protect User Data*, THE GUARDIAN (Oct. 25, 2018), https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

£31.5 billion the company made that year in global revenue.[106] Facebook's fine pales in comparison to the fines given to unsecured companies after GDPR was enacted. International airline British Airways and international hospitality chain Marriot were the first culprits to receive GDPR fines, facing totals of £183 million and £99 million out of their £13 billion[107] and £16 billion[108] yearly revenues, respectively, for breaches of customer data.[109] If Facebook had been fined today, it would have owed up to £1.26 billion, or 4% of its revenue, making the fine less of a slap on the wrist and more of an accountability check for the social media giant, as well as an example to others. Companies can no longer respond to a breach with an apology email and no formal security updates. The GDPR and future CCPA fines are more than an annoyance—they are a reminder that there are real consequences to allowing data breaches to occur.

Another way regulations can protect users lies in the language they use. The wording in GDPR and POPIA is clear in places and approaches legalese in others. This does not come as a surprise, as both regulations are laws. The issue with using legal language to describe data privacy, a technical concept with technical solutions, is that legal writing "contains vague, general wording that actually means very little unless read in a specific context . . . and clear absolute statements from which no variation seems possible."[110] If laws are vague and absolute in the wrong places, compliance becomes more difficult and user privacy suffers.

Article 24 of GDPR states "the controller shall implement *appropriate* technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."[111] Article 6 allows companies to continue to process personal data if they have "a legitimate interest" in processing that data.[112] In this case, it is up to the controller to decide what solution is appropriate enough to comply with the regulation while ensuring the data that is

---

[106] *Id.*

[107] IAG ANNUAL REPORT (2018) (last visited Feb. 21, 2020), https://www.iairgroup.com/~/media/Files/I/IAG/documents/annual-report-and-accounts-2018-interactive.pdf.

[108] Marriott Int'l, Inc., Annual Report (Form 10-K) (Dec. 31, 2018), https://marriott.gcs-web.com/static-files/8799734e-b9e0-4e53-b194-7bd24a381118.

[109] Dan Swinhoe, *The Biggest Data Breach Fines, Penalties, and Settlements So Far*, CSO (Oct. 23, 2020), https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html?nsdr=true.

[110] Christopher Kuner et al., *The Language of Data Privacy Law (And How It Differs from Reality)*, 6 INT'L DATA PRIV. L. 259, 259–60 (2017).

[111] GDPR, *supra* note 54 at art. 24 (emphasis added).

[112] *See* GDPR.EU, *supra* note 50.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

processed is still usable and is legitimately important to their company. Similarly, the language in POPIA requires breaches to be reported "as soon as reasonably possible," which can be interpreted as narrowly or broadly as the breached company's DPO would like, and not necessarily in a way that would protect user privacy the most.[113]

GDPR protects not just EU citizens, but "data subjects," a term which includes EU citizens, residents, and in some cases, anyone else who has performed a transaction with an EU business. Unlike POPIA's breach notification clause, this intentionally vague terminology clearly benefits consumers as it forces EU businesses to comply with the regulation for all of their data and not just that of citizens.[114] The protective intent behind "data subjects" is confirmed in and clarified by specific language elsewhere in the regulation.[115]

The specific language in GDPR requires companies to provide a breach notification within seventy-two hours of discovering a security issue not just when data is stolen, but when it is changed, lost, or accidentally disclosed.[116] Scenarios under which notification is required benefit consumers because previously no notice was required unless illicitly accessed data was actually stolen.

However, if the language in this section was even less specific and included all instances of unauthorized access by a third party, economic principles support the conclusion that consumers would be even better protected. Two conditions of perfect competition in economics, which allows idealized free markets to operate most efficiently, are that services are truly interchangeable, or homogenous,[117] and that consumers have perfect information.[118] If the first condition is assumed to be true and consumers are given full knowledge about the collection and use of their information, they can then compare privacy practices across all available substitute companies that provide that service. Full transparency about privacy practices allows

---

[113] Russell Nel, *GDPR Matchup: South Africa's Protection of Personal Information Act*, IAPP (Sept. 5, 2017), https://iapp.org/news/a/gdpr-matchup-south-africas-protection-of-personal-information-act/.

[114] *See infra* note 115.

[115] Art. 3(2) states "This Regulation applies to the processing of personal data of data subjects who are in the Union." Art. 3(1) states: "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

[116] GDPR § 4.

[117] *See generally* JOHN BLACK, OXFORD DICTIONARY OF ECONOMICS (New York: Oxford Univ. Press, 2d ed. 2003).

[118] Joseph E. Stiglitz, *Information*, THE LIBR. OF ECON. AND LIBERTY (last visited Feb. 20, 2020), https://www.econlib.org/library/Enc/Information.html.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

consumers to make better choices because it forces companies to compete for business from the consumer by updating and maintaining privacy practices that are favorable to users. Companies would try to improve their data protection because it would ostensibly increase their revenue, and consumers would benefit from choosing the service that provides the most privacy. To provide consumers with the most privacy, the proposed U.S. regulation would then need to prioritize transparency about their privacy practices.

One thing to keep in mind is that there are some services, like the social media site Facebook or the LGBT dating app Grindr, that do not have true substitutes. The necessity for a critical mass of users on these sites means that their services are not interchangeable with any would-be competitors, thus true competitors do not actually exist on the market. This is a problem for consumers because both companies have faced multiple data breaches.[119] Yet these companies have no incentive to enact full security and privacy mitigations because consumers have no substitute to turn to, and simply have to accept the level of security and data privacy those apps provide. Such companies without competitors have no incentive to self-regulate. Separately, there are websites like Reddit that have a strong enough brand loyalty from their consumer base that users would likely continue using their site even if they do no more than the required minimum to protect consumer privacy.

Since its "go-live" date, GDPR has had mixed reactions. A survey was conducted in the United Kingdom to assess the public's reaction to GDPR three months after enactment.[120] Fifty-seven percent of consumers felt they had a better understanding of how companies used their personal data, and 65% believed it had not changed their experience with brands they use.[121] What is shocking is that 90% of the respondents thought they had witnessed brands acting unlawfully and trusted those brands less as a result.[122] This means that shortly after the deadline, consumers

---

[119] Janet Burns, *Report Says Grindr Exposed Millions of Users' Private Data, Messages, Locations*, FORBES (Mar. 29, 2018, 1:14 PM), https://www.forbes.com/sites/janetwburns/2018/03/29/report-says-grindr-exposed-millions-of-users-private-data-messages-locations/#5370eb7c5c4cl; Patrick Wardle, *The Do's and Don'ts of Location Aware Apps; A Case Study*, SYNACK (Sept. 11, 2014, 2:00 PM), https://www.synack.com/blog/the-dos-and-donts-of-location-aware-apps-a-case-study/; PCMag Staff, *Grindr Hack Leaves Hundreds of Thousands Exposed*, PCMAG (Jan. 20, 2012), https://www.pcmag.com/archive/grindr-hack-leaves-hundreds-of-thousands-exposed-293112; Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html; April Glaser, *Another 540 Million Facebook Users' Data has Been Exposed*, SLATE (Apr. 3, 2019, 7:41 PM), https://slate.com/technology/2019/04/facebook-data-breach-540-million-users-privacy.html.

[120] Lucy Tesseras, *GDPR Three Months On: Most Consumers Feel No Better Off*, MARKETINGWEEK (Aug. 24, 2018), https://www.marketingweek.com/gdpr-three-months-on/.

[121] *Id.*

[122] *Id.*

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

felt they better understood how their data was being used, and while it did not change their daily experience, this new understanding of how little user privacy companies actually protect negatively affected their trust. In the year after the GDPR deadline, consumers submitted 4,113 privacy complaints in Ireland alone, UK companies reported a total average of 500 breaches per week, and the ICO assigned €56,000,000 in fines to ninety-one noncompliant companies.[123] The increase in reporting metrics from both consumers and companies demonstrates the efficacy of a comprehensive model for privacy regulation in addressing abuse.

CCPA may not be a national law, but it still affects more businesses than just those within the state. Any business that collects, uses, or processes the data of California residents must comply with CCPA. Additionally, the intentionally vague definition of "personal information" as "any information that . . . relates to . . . a particular consumer or household" requires more companies to comply with the act and protects the privacy of more consumers than would be covered by a narrower definition.[124] While the existence of CCPA does not mean other states will immediately follow suit with equally strict regulations, other states like Washington and Illinois are already in the process of creating their own privacy bills.[125] As of the end of 2019, Maine has signed a bill into law, which will go into effect in July of 2020.[126] Each additional state that enacts such a law will bring its own compliance costs and challenges for businesses to navigate.

One issue to keep in mind with state-specific privacy laws is that certain states would require companies to comply with their stricter privacy protection rules, which might drive businesses that do not want to or cannot afford to comply into another state that does not have such a requirement. While states should also consider whether the rigidity and penalties in their privacy laws may squash innovation, privacy has value separate from profit. Furthermore, states can look to the example of Silicon Valley companies that have not left the state and continue to be profitable despite CCPA.

---

[123] Philip Lee, *One Year Later, Is GDPR Working?*, LEXOLOGY (May 27, 2019), https://www.lexology.com/library/detail.aspx?g=1679e81c-bd6e-4445-8841-e09170289596.

[124] CAL. CIV. CODE § 1798.140(o)(1) (2020).

[125] Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, IAPP (last visited July 6, 2020), https://iapp.org/resources/article/state-comparison-table/.

[126] *Id.*

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

B. What We Can Do

High-impact breaches have become more prolific every year.[127] In 2017, Equifax faced a security breach that exposed the personal information of 147 million people.[128] In 2018[129] and 2019,[130] Facebook faced multiple security breaches, affecting over 600 million total accounts. In 2019, Capital One faced a security breach that exposed over 100 million Americans' credit applications with distinct private information like Social Security Numbers.[131] Despite the severity of these annual breaches, there has not been a single national regulation to address the lack of data privacy protections.

It is true that the word "privacy" does not appear in the Constitution. Justice Scalia previously asserted that the Court should not assume that there is a constitutional right to informational privacy, as there is no such right explicitly provided for in the Constitution.[132] The Court in *Katz* even states that the "Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"[133] However, that immediately precedes a statement equating the "right to be let alone by other people" to "the protection of [man's] property and of his very life."[134]

While the Court in *Katz* does argue for privacy regulations to remain the responsibility of the states, in modern times, that solution would not adequately protect Americans. Just as the Court in *Furman v. Georgia* put a moratorium on the ability of states to impose the death penalty, so can the federal government decide that states should not have the primary role in creating baseline privacy regulations.[135] The moratorium enforced by *Furman* reflected the view that states

---

[127] *See supra* note 1.

[128] FTC EQUIFAX DATA BREACH SETTLEMENT, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement (last visited Feb. 21, 2020).

[129] Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach. html.

[130] April Glaser, *Another 540 Million Facebook Users' Data Has Been Exposed*, SLATE (Apr. 3 2019), https://slate.com/technology/2019/04/facebook-data-breach-540-million-users-privacy.html.

[131] Brian Krebs, *What We Learn from the Capital One Hack*, KREBS ON SECURITY (Aug. 2, 2019), https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/.

[132] Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 159–60 (2011).

[133] Katz v. United States, 389 U.S. 347, 350 (1967).

[134] *Id.* at 350–51.

[135] Furman v. Georgia, 408 U.S. 238, 238–40 (1972) (The Court placed a moratorium on states' rights to impose the death penalty, because states were violating the Eighth and Fourteenth Amendments

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

were not properly protecting their citizens' rights. It was lifted when states passed laws one by one to meet the Court's standard of protection. With privacy in the age of the Internet, however, states would pass potentially conflicting patchwork laws, each of which would bring additional compliance and uncertainty costs to businesses, and thus to citizens. Because of this, states are unlikely to reach a satisfactory standard of privacy protection on their own.

Having patchwork state laws without a national comprehensive-model privacy regulation as the baseline to build off of is like babyproofing the beach house as a hurricane threatens the coast. It is a good solution for the wrong problem, which makes it the wrong solution for this problem.

Tech companies like those behind the Committee to Project California Jobs, an Amazon, Microsoft, Uber, and Google-funded group that lobbied against CCPA, object to this kind of regulation.[136] They claim it would squash innovation if enacted now, and that any such regulation can wait.[137] America has witnessed laws lag behind demand for social change before. Support for LGBT marriage has been steadily increasing for sixteen years. The plurality of U.S. adults supported LGBT marriage in 2011,[138] but it was only recently addressed by the Court in 2015.[139] Similarly, support for privacy regulation in the United States is already very high. In fact, in a 2019 Pew study, 79% of Americans stated they were concerned about the way their data was being used by companies and 81% felt they had very little or no control over the data that companies collected about them.[140] Sixty-three percent of Americans said they understand very little or nothing at all about the current data privacy regulations in place.[141] Given this sentiment and the constant plague of privacy issues such as breaches and login credential theft, we should not let the enactment of these regulations lag any further.

---

by failing to give citizens adequate due process and life/liberty rights, until states enacted specific death penalty laws that were not cruel and unusual and involved better due process.).

[136] Colin Lecher, *Amazon, Microsoft, and Uber are Paying Big Money to Kill a California Privacy Initiative*, THE VERGE (June 15, 2018), https://www.theverge.com/2018/6/15/17468292/amazon-microsoft-uber-california-consumer-privacy-act.

[137] *Id.*

[138] *Attitudes on Same-Sex Marriage*, PEW RES. CTR. (May 14, 2019), https://www.pewforum.org/fact-sheet/changing-attitudes-on-gay-marriage/.

[139] Obergefell v. Hodges, 576 U.S. 644, 623 (2015).

[140] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https:// www.pewresearch .org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[141] *Id.*

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

Americans support having new privacy regulations—regulations that would inevitably come with new costs. However, enacting a comprehensive privacy regulation would not give companies carte blanche to displace costs to customers. There is discontentment with the current privacy climate in the United States, but that does not mean that consumers are willing to directly pay for improvement. The Center for Data Innovation found that only one in four Americans would pay a monthly subscription fee for companies like Facebook and Google to collect less of their data.[142] And that is completely understandable—America should improve privacy protections in a way that minimizes the cost to consumers.

The best way to minimize these costs is to craft a national privacy regulation using the comprehensive model. The cost companies will face to comply with CCPA over the next decade is forecasted to be up to $16.4 billion.[143] For companies to "absorb" that kind of cost, they would inevitably offload some of it onto the consumer. Companies that have a presence in multiple states will face an even higher bill when they take into account the costs associated with each state's privacy laws. If more states continue to enact patchwork data privacy bills, the compliance costs and potential conflicts will further harm our economy and increase uncertainty.

Instead, Congress should pass a law that expands the role of the FTC, empowering them to protect consumers' privacy not just from government agencies, as provided in the Privacy Act of 1974, but also from increasingly powerful private entities. This would allow the FTC, which has become the most influential regulating force on information privacy in the United States,[144] to create and enforce new, relevant regulations to serve as a national baseline for privacy protections. States would then have the option to further build upon these protections. The agency would update terms to match modern technological, data security, and privacy developments, and would pass new rules that no one in 1974 could have foreseen the need for. The new regulation would deal not only with privacy but also with security, as privacy cannot exist without proper security. "The fact that security implements privacy is a critical point often lost in legal (and other) scholarship and policy

[142] Daniel Castro & Michael McLaughlin, *Survey: Few Americans Willing to Pay for Privacy*, CTR. FOR DATA INNOVATION (Jan. 16, 2019), https://www.datainnovation.org/2019/01/survey-few-americans-willing-to-pay-for-privacy/.

[143] CALIFORNIA DOJ OAG, STANDARDIZED REGULATORY IMPACT ASSESSMENT: CAL. CONSUMER PRIV. ACT OF 2018 REG. (2019), www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[144] *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

debate . . . ."[145] Adequate data privacy is interconnected with good cybersecurity practices.

The proposed national privacy regulation would cover a necessary minimum set of requirements American businesses over a certain revenue mark must meet, like encrypting data, both at rest and in motion, using the most current government-approved encryption mechanism.[146] It is true that there are real costs associated with making such a change. The ICO's staff increased roughly 30% to almost 650 contract-based employees because of GDPR, with 722 permanent staff.[147] The ICO's annual costs also increased from £27 million to £43 million.[148] It would thus make sense for the government to encourage compliance by providing subsidies for small businesses that may not be able to afford such technical protections. Because the proposed regulation would cover basic privacy essentials, it would be up to the states' discretion to add more stringent rules that businesses in those states would comply with as well, but a national baseline would minimize such variation. The federal regulation would act as a floor for privacy protections. Additionally, the language in the new regulation should be in plain text with the only room for interpretation existing in the consumers' favor, and should be reviewed every four or so years.

Finally, there should be a contingency plan, in case specific rule enactment does not occur on time. When HIPAA was enacted, HHS, the agency responsible for the regulation, was given a deadline with a contingency plan if it failed to enact an appropriate version of the Privacy Rule. If it failed to revisit the privacy question within thirty-six months, HHS would be directed to promulgate regulations[149] consistent with basic "broad stroke" aspirational goals laid out in the HIPAA.[150]

---

[145] *See* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 354–55 (2014).

[146] Author note: SHA-1 encryption is still considered proper encryption despite its replacement with newer SHA versions and the sheer number of breaches that have occurred because SHA-1 is decryptable. The proposal would specify that only encryption methods that have not been decrypted yet are valid.

[147] Mark Sweney, *GDPR Fines: Where Will BA and Marriott's £300m Go?*, THE GUARDIAN (July 10, 2019), https://www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog.

[148] *Id.*

[149] HIPAA § 264(c)(1), 110 Stat. 2033, at 2033 (1996) (stating "If legislation governing standards with respect to the privacy of individually identifiable health information . . . is not enacted by the date that is 36 months after the date of the enactment of this Act [(Aug. 21, 1996)], the Secretary of Health and Human Services shall promulgate final regulations containing such standards . . . .").

[150] HIPAA § 262(a), § 1173(d), 110 Stat. 2024 at 2025–26 (codified as amended at 42 U.S.C. § 1320d-2(d)) (listing the major goals of ensuring integrity and confidentiality of information and protecting against reasonably anticipated threats and unauthorized uses).

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

Similarly, there can be a failsafe built into the process in case the FTC fails to properly update the protections in the 1974 Privacy Act to more technologically appropriate rules.

IV. CONCLUSION

In just the first two months of 2020, there have already been six breaches affecting over 206 million records.[151] No fines have been levied and no consequences have been faced. One of the breached companies stated they were "encourag[ing their] customers to remain vigilant in reviewing charges on their payment card statements," illustrating that the cost displacement problem costs consumers time and stress as well as money.[152] It is because of issues like this that Congress should afford the FTC the power to create and enforce an updated national privacy regulation that would serve as a baseline for data protections. Having a baseline gives states the option to enact additional more specific laws if they so choose. That way, even if states do nothing more, citizens' data privacy can still be sufficiently protected.

This Article calls on congressional power to protect Americans' data privacy because the executive and judicial branches are not well positioned to make an impactful change to our current privacy landscape. The executive branch can only act within the bounds of laws Congress has already passed. The more outdated the law under which they are acting, the more difficult it is for the executive branch to produce anything meaningful. Additionally, the lag in changes made through the judicial branch is particularly harmful when dealing with something that evolves as rapidly as data privacy. Even if the Supreme Court holds that Americans have the

[151] Allison Matyus, *Wawa Data Breach: Hacker Is Selling 30 Million Credit Cards on the Dark Web*, DIGITALTRENDS (Jan. 29, 2020), https://www.digitaltrends.com/news/convenience-store-data-breach-info-found-being-sold-on-dark-web/; *Household Names: How Tetrad Exposed Data on 120 Million Consumers*, UPGUARD (Feb. 20, 2020), https://www.upguard.com/breaches/tetrad-breach-120-million-households; Corbin Davenport, *Slickwraps Has Been Hacked, Customer Data Is Compromised*, ANDROID POLICE (Feb. 22, 2020), https://www.androidpolice.com/2020/02/22/slickwraps-has-been-hacked-customer-data-is-compromised/; Stacy Liberatore, *Massive Data Leak Exposes Medical Records, Mugshots and IDs of More Than 36,000 Inmates Across The Country That Were Left on an Unsecure Server*, DAILY MAIL (Feb. 14, 2020), https://www.dailymail.co.uk/sciencetech/article-8005123/Massive-data-leak-exposes-medical-records-mugshots-IDs-36-000-inmates.html; Shaun Nichols, *Why Is a 22GB Database Containing 56 Million US Folks' Personal Details Sitting On the Open Internet Using a Chinese IP Address? Seriously, Why?*, THE REGISTER (Jan. 9, 2020), https://www.theregister.com/2020/01/09/checkpeoplecom_data_exposed; Dustin Jermalowicz, *Jackpot247 Suffers Data Breach*, CASINO LISTINGS (Jan. 21, 2020), https://www.casinolistings.com/ news/2020/01/jackpot247-suffers-data-breach.

[152] Brian Krebs, *Wawa Breach May Have Compromised More Than 30 Million Payment Cards*, KREBS ON SECURITY (Jan. 28 2020), https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu

specific right to informational privacy, it is not a bureaucratic body that can produce detailed laws to reflect that ruling.[153]

While CCPA is a step in the right direction and is a better option for those it protects than no privacy protections at all, it was produced somewhat haphazardly using the resources of only one state. The reach and experience of a national bureaucratic agency would allow for a more thorough and systematic regulation. Further, states rarely need to consider the international impact their laws may have, leading to laws that are tailored to only their own criteria. CCPA created certain loopholes both despite and because of its specific language; Google and Facebook still claim that they are exempt from providing users a way to opt out of the sale of their personal data, because they do not technically "sell" user data but merely share it.[154] This example will inevitably encourage other tech companies to similarly subvert the spirit of the law. The past several decades have shown that this kind of abuse is rampant. With more of daily life relying on the Internet and with the breach count increasing every year, Americans deserve to have their privacy protected sooner rather than later. The near-constant threat to informational privacy and the unwillingness of companies to protect it mandates a comprehensive national regulation to secure the constitutional right to privacy in the 21st century.

[153] Furman v. Georgia, 408 U.S. 238, 238–40 (1972) (in which the Court did not pass a law ending the death penalty, but put a moratorium on the death penalty until states created more specific laws in furtherance of their holding).

[154] Aaron Holmes, *A New Law Gives You the Power to Tell Websites not to Sell Your Personal Data. Here's How to Exercise Your Rights*, BUSINESS INSIDER (Jan. 2, 2020), https://www.businessinsider.com/new-law-ccpa-privacy-tell-websites-not-sell-personal-data-2020-1.

Volume XXI—2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.241 ● http://tlp.law.pitt.edu