Idaho Law Review

Volume 55 | Number 3 Article 2

# Top Ten Reasons to be Optimistic About Privacy

Jordan M. Blanke

# TOP TEN REASONS TO BE OPTIMISTIC ABOUT PRIVACY

JORDAN M. BLANKE

FULL CITATION:

Jordan M. Blanke, *Top Ten Reasons to be Optimistic About Privacy*, 55 IDAHO L. REV. 281 (2019).

# TOP TEN REASONS TO BE OPTIMISTIC ABOUT PRIVACY

JORDAN M. BLANKE*

ABSTRACT

*Much has been written about the demise of privacy. There is no doubt that the notion of privacy has changed dramatically and continues to evolve. All, however, is not doom and gloom. While technology and societal changes have radically altered the environment in which privacy must survive, the same basic human needs and values continue to transform it into a new shape. Some of the momentum comes from the law itself, some from the business world, some from societal values, and some from new emphases in research. This paper will discuss the top ten reasons to be optimistic about the future of privacy.*

TABLE OF CONTENTS



## I. INTRODUCTION

It seems like we have been hearing about the death of privacy for a long time. From Scott McNealy's proclamation in 1999 that "[y]ou have zero privacy anyway. . . . Get over it"[1] to Mark Zuckerberg's declaration in 2010 that privacy is no longer

* Ernest L. Baskin, Jr. Distinguished Professor of Computer Science and Law at the Stetson School of Business and Economics at Mercer University in Atlanta.

1. Polly Sprenger, *Sun on Privacy: "Get Over It,"* WIRED (Jan. 26, 1999, 12:00 PM), http://archive.wired.com/politics/law/news/1999/01/17538.

a social norm;[2] from privacy legislation's relegation to the back burner after 9/11;[3] to the utter failure of the notice and consent model on the Web.[4] While there is no doubt that privacy is very different than it was a generation or two ago, all is not doom and gloom. There are some glimmers of hope.

Obviously, the notion of privacy has evolved tremendously in the past several decades. As society changes – often driven by new technology – the law evolves. It must. As Professor Neil Richards argued in his classic article *Four Privacy Myths*, privacy is *not* dead and young people *do* care about their privacy.[5] While the technocentric world that young people have grown up in certainly differs from the world of just a few years ago, they are likely far more savvy about how to navigate that world and how to protect their privacy.[6]

In this article, I have compiled a list of ten reasons to be optimistic about the future of privacy. I have tried to put them in an order of increasing importance, but there no doubt, will be room for differing opinions regarding that order. One of the things that I tried to do is weigh both the significance of the item as well as the likelihood of it happening. For example, if the *Katz* test were to be completely overhauled by the Supreme Court, making it the one-prong objective test it should have been for the past fifty years, it would be tremendously important.[7] However, the likelihood of that happening is very small. Here are the top ten reasons to be optimistic about the future of privacy:

## 10. CRIMINAL PRIVACY LAWS ARE FINALLY BEING USED MORE

Despite the fact that there have been criminal sanctions for various forms of computer misuse and invasion of privacy for decades, there has been relatively little use of those statutes.[8] It appears that this is beginning to change.

---

2. Marshall Kilpatrick, *Facebook's Zuckerberg Says the Age of Privacy is Over*, N.Y. TIMES (Jan. 10, 2010), https://archive.nytimes.com/www.nytimes.com/external/reawriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html.

3. Daniel Klau*, Privacy, Security, and the Legacy of 9/11*, UCONN TODAY (Sept. 10, 2015), https://today.uconn.edu/2015/09/privacy-security-and-the-legacy-of-911/; Jason Noble*, U.S. Debates Security vs. Privacy 12 Years After 9/11*, USA TODAY (Sept. 10, 2013, 11:11 PM), https://www.usatoday.com/story/news/nation/2013/09/10/us-debates-security-vs-privacy-12-years-after-911/2796399/.

4. *See* Joel R. Reidenberg et al., Norton, *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 485, 490–96 (2015); Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, (Oct. 2009), https://nissenbaum.tech.cornell.edu/papers/ED_SII_On_Notice.pdf.

5. Neil M. Richards*, Four Privacy Myths*, SSRN (Apr. 24, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864; *see also* Chris Jay Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* SSRN (Apr. 14, 2010), https://poseidon01.ssrn.com/delivery.php?ID=857005071031026003082071122117116000040032020031003054085119122096081002023113002064054114001037062104014030012009124109067025033016010081059112029003087070119065086082084025086092010084030127065069087090100089095068028074020075124080109112065000067&EXT=pdf.

6. Richards, *supra* note 5, at 16–18.

7. *See infra* notes 40–68 and accompanying text.

8. Jordan M. Blanke, *Criminal Invasion of Privacy: A Survey of Computer Crimes*, 41 JURIMETRICS 443, 456 (2001).

Arizona and Florida passed the first "computer crime" statutes in 1978.[9] Georgia, Virginia, and West Virginia passed the first criminal invasion of privacy statutes in 1999 and 2000.[10] The federal government enacted the Comprehensive Crime Control Act in 1984[11] and amended it with the Computer Fraud and Abuse Act (CFAA) in 1986.[12] We are finally beginning to see more prosecutions under these statutes.

There have been several well-publicized hacking or phishing incidents involving celebrity photographs in recent years. When two nude selfies of Scarlett Johansson were published on the Web in 2011, the most effective and immediate remedy was for her to use the "takedown" provision of the Digital Millennium Copyright Act.[13] Because she took the selfies and was the owner thereof, Johannsson could have threatened liability under the copyright law for web sites that did not respond to her notice by immediately removing the photographs from their web sites.[14] Privacy statutes do not provide similar protection. Johannsson would not have been able to use the "takedown" provision of the copyright law had she not been the author and owner of the copyright-protected work.[15] Obviously, quite often the subject of the offending photograph is not the author and is, therefore, unable to avail themselves of that provision.

While Johansson's use of copyright law resulted in the removal of her photographs from many more web sites than if she had threatened merely to sue for invasion of privacy, it is encouraging to see some computer crime statutes now being used to prosecute the hackers.[16] In the aftermath of this episode, dubbed *Operation Hackerazzi* by the press, the perpetrator of the breach was prosecuted under two sections of the CFAA, pleaded guilty, and was sentenced to the maximum ten years in prison.[17] The court found that Johansson, and several other celebrities,

9. *Id.* at 449. ARIZ. REV. STAT. ANN. §§ 13-2301(E), 13-2316 (West 2000); FLA. STAT. §§ 815.01–815.07 (West 1999).

10. *See* Blanke, *supra* note 8, at 451; GA. CODE ANN. § 16-9-93(c) (West 1999); VA. CODE ANN. § 18.2-152.5 (West 2000); W. VA. CODE ANN. § 61-3C-12 (West 2000).

11. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976 (1984).

12. Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986).

13. *See* Christopher Satti, *A Call to (Cyber) Arms: Applicable Statutes and Suggested Courses of Action for the Celebrity iCloud Hacking Scandal*, 34 QUINNIPIAC L. REV. 561, 579–88 (2016); Jessica E. Easterly, *Terror in Tinseltown: Who is Accountable When Hollywood Gets Hacked*, 66 SYRACUSE L. REV. 331, 332–37 (2016); Jordan M. Blanke, *Privacy and Outrage*, 9 J.L., TECH. & INTERNET 1, 10–11 (2018).

14. Under Section 512(g)(1) of Title 17 of the United States Code, "a service provider shall not be liable to any person for any claim based on the service providers' good faith disabling of access to, or removal of, material . . . regardless of whether the material or activity is ultimately determined to be infringing." 17 U.S.C. § 512(g)(1) (2010). The use of this so-called "DCMA takedown notice" has become extremely common. As long as a web host removes the allegedly infringing work, this "safe harbor" provision will protect it from liability. *See* Easterly, *supra* note 13, at 358–59.

15. Section 512(b)(2)(E) permits the owner of a copyrighted work to make such a claim. 17 U.S.C. § 512(b)(2)(E) (2010).

16. David Kravets, *Scarlett Johansson Hacker Gets 10 Years*, WIRED (Dec. 17, 2012, 6:12 PM), https://www.wired.com/2012/12/scarlett-johansson-hacker/.

17. *See* Satti, *supra* note 13, at 580–81; *see also* Easterly, *supra* note 13, at 348.

had suffered both economic loss and severe emotional distress.[18] An FBI agent involved in the case likened the defendant's actions to the "breaking and entering of [the celebrities'] private homes by a thief in the night."[19]

Similarly, in what widely became known as *The Fappening*, and as a result of multiple phishing scams, nude photographs of many celebrities were again leaked to the Web in 2014.[20] One of the celebrities involved was Jennifer Lawrence, whose representative threatened that authorities would "prosecute anyone who posts the stolen photos."[21] Two men were successfully prosecuted under a section of the CFAA prohibiting the unauthorized access of a protected computer.[22] One received a sentence of eighteen months in prison and the other nine months.[23]

Part of the reason for more successful prosecution under computer crime statutes is likely attributable to evolving societal views regarding privacy: "[b]eloved figures like Jennifer Lawrence, made vulnerable by having their naked bodies nonconsensually exposed to the world, are . . . sympathetic characters[.]"[24] Public outrage about some of the more egregious breaches of privacy are starting to shape a new sense of what should and should not be permitted in our digital world.[25] Other examples include the trends towards banning revenge porn[26] and upskirt photography.[27]

## 9. INFLUENCE OF CONTEXTUAL INTEGRITY RESEARCH

In 2004 Helen Nissenbaum wrote the landmark article *Privacy as Contextual Integrity*.[28] It has been arguably the most influential article ever written about privacy in terms of shaping the direction of privacy research and its literature. Many of the article's basic propositions have spawned numerous other articles in a variety of disciplines.[29]

---

18. Satti, *supra* note 13, at 580.

19. *Id.* at 580–81.

20. Easterly, *supra* note 13, at 334.

21. *Id.*

22. *Id.* at 349.

23. Alan Yuhas, *Hacker Who Stole Nude Photos of Celebrities Gets 18 Months in Prison*, GUARDIAN (Oct. 27, 2016, 7:15 PM), https://www.theguardian.com/technology/2016/oct/27/nude-celebrity-photos-hacker-prison-sentence-ryan-collins; ASSOC. PRESS, *Chicago Man Gets 9 Months in Celebrity Nude Photo Hack*, USA TODAY (Jan. 24, 2017, 6:21 PM), http://www.usatoday.com/story/life/movies/2017/01/24/chicago-man-gets-9-months-celebrity-nude-photo-hack/97011632/.

24. Easterly, *supra* note 13, at 345. *See infra* notes 118–37 and accompanying text.

25. *See* Blanke, *supra* note 13, at 9–17.

26. *See generally* Ari Ezra Waldman, *A Breach of Trust: Fighting Nonconsensual Pornography*, 102 IOWA L. REV. 709 (2017); *see also 41 States + DC Have Revenge Porn Laws*, CYBER CIV. RTS. INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ (last visited Jan. 14, 2019) (Forty-one states and Washington, D.C. have now passed revenge porn laws).

27. Blanke, *supra* note 13, at 11–12; Marc Tran, *Combatting Gender Privilege and Recognizing a Woman's Right to Privacy in Public Spaces: Arguments to Criminalize Catcalling and Creepshots*, 26 HASTINGS WOMEN'S L.J. 185 (2016). *See generally* Jeffrey T. Marvin, *Without a Bright-Line on a Green Line: How Commonwealth v. Robertson Failed to Criminalize Upskirt Photography*, 50 NEW ENG. L. REV. 119 (2015).

28. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

29. Hundreds of law journal articles have written about contextual integrity. *See, e.g.*, Nizan Geslevich Packin and Yafit Lev-Aretz, *On Social Credit and the Right to Be Unnetworked*, 2016 COLUM. BUS. L. REV. 339 (2016). A special issue of Ohio State's I/S: A Journal of Law and Policy for the Information Society was

The first part of Nissenbaum's article presented the three basic principles that had dominated discussion of privacy: "(1) limiting surveillance of citizens and use of information about them by agents of government, (2) restricting access to sensitive, personal, or private information, and (3) curtailing intrusions into places deemed private or personal."[30] The second part of her paper described privacy in terms of "contextual integrity."[31]

> A central tenet of contextual integrity is that there are no arenas of life *not* governed by *norms of information flow*, no information or spheres of life for which "anything goes." Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation . . . .
>
> Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices. For certain contexts, such as the highly ritualized settings of many church services, these norms are explicit and quite specific. For others, the norms may be implicit, variable, and incomplete . . . .
>
> Contexts, or spheres, offer a platform for a normative account of privacy in terms of contextual integrity. As mentioned before, contexts are partly constituted by norms, which determine and govern key aspects such as roles, expectations, behaviors, and limits. There are numerous possible sources of contextual norms, including history, culture, law, convention, etc. Among the norms present in most contexts are ones that govern information, and, most relevant to our discussion, information about the people involved in the contexts. I posit two types of informational norms: norms of appropriateness, and norms of flow or distribution. Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated.[32]

Nissenbaum proposed that contextual integrity set up a "presumption in favor of the status quo; common practices are understood to reflect norms of appropriateness and flow, and breaches of these norms are held to be violations of privacy."[33] She discussed how the status quo of norms regarding information flows could be challenged for sufficient reason, but that there would need to be a balancing with relevant social, political, and moral values.[34] Among the important privacy

devoted to contextual integrity. VOL. 13 I/S J. L. & POL'Y (2017). Nissenbaum and others wrote an article surveying the computer science literature for applications of contextual integrity. Sebastian Benthall, Seda Gürses & Helen Nissenbaum, *Contextual Integrity Through the Lens of Computer Science*, 2 FOUND. & TRENDS PRIVACY & SEC. 1 (2017).

30. Nissenbaum, *supra* note 28, at 125.
31. *Id.* at 136–56.
32. *Id.* at 137–38.
33. *Id.* at 145.
34. *Id.* at 146–47.

values presented were prevention of informational harms, informational equality, autonomy and freedom, and preservation of important human relationships.[35]

An example of an informational harm and a severe breach of contextual integrity was the murder of actress Rebecca Schaeffer.[36] A disturbed fan was able to purchase a database containing Schaeffer's home address from the Department of Motor Vehicles.[37] The fan used the address to track her down and kill her.[38] Obviously, the information was not provided to the DMV by Schaeffer with an expectation that it could be purchased by private individuals. The incident caused a change in law prohibiting such sales in the future.

Nissenbaum's discussion of informational inequality presaged the proliferation of articles written about abuses and potential abuses of sophisticated use of data analytics.[39] Her discussion of autonomy and freedom—or "the right to control information about oneself"[40]—is, obviously, a basic theme in privacy literature and in privacy legislation.[41] Her discussion of the preservation of important human relationships and the role that trust plays in the ability to limit access to personal information has also spawned a number of articles on this topic.[42]

One of the cases that Nissenbaum used to illustrate the application of contextual integrity involved an example of what has become one of the most difficult and offending abuses of information flow—consumer profiling and data mining. She stated that "the crucial issue is not whether the information is private or public, gathered from private or public settings, but whether the action breaches contextual integrity."[43] This is, if anything, truer and more important today. With the failure of a notice and consent scheme capable of protecting personal information, coupled with the vast amounts of information already out there, the major hope today is a regulatory scheme that limits subsequent use of information—and the purposes for which the information can be used and the period of time it can be retained. All of these speak to the contextual integrity of the information.

Nissenbaum's article has been responsible for a generation of literature that has built upon her basic propositions and informed the direction of much research

35. *Id.* at 147–50.

36. Nissenbaum, *supra* note 28, at 147; s*ee also* Adam D. Moore, *Toward Informational Privacy Rights*, 44 SAN DIEGO L. REV. 809, 826 (2007).

37. Paul Jacobs, *Addresses at DMV Remain Accessible*, L.A. TIMES, (Aug. 19, 1991), http://articles.latimes.com/1991-08-19/news/mn-608_1_address-information.

38. *Id.*

39. *See* FRANK PASQUALE, BLACK BOX SOCIETY (2015); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016); Janine S. Hiller, *Healthy Predictions? Questions for Data Analytics in Health Care*, 53 AM. BUS. L.J. 251, 267–81 (2016); Robert Sprague, *Welcome to the Machine: Privacy and Workplace Implications of Predictive Analysis*, 21 RICH. J.L. & TECH. 13 (2015); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. TELECOMM. & HIGH TECH. L. 351 (2013).

40. Nissenbaum, *supra* note 28, at 149.

41. A major theme of one of today's most significant pieces of legislation, the GDPR, is the protection of the fundamental rights and freedoms of natural persons with respect to the collection of their personal data. *See infra* note 186.

42. *See infra* notes 138–53 and accompanying text.

43. Nissenbaum, *supra* note 28, at 152.

that is occurring today.[44] Much of this literature will shape the direction of privacy as it evolves in the near future.

## 8. REINTERPRETATION OF THE *KATZ* TEST

Ever since 1967 and the Supreme Court's decision in *Katz v. United States*, much of this country's jurisprudence on privacy law has been the result of the two-pronged test enunciated in Justice Harlan's concurring opinion: "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[45] Unfortunately, much of the fifty-year body of law is built upon an erroneous interpretation of that test. It is impossible to truly understand the *Katz* case without reading two excellent companion articles by Peter Winn and Harvey Schneider.[46] Winn's article, which reads more like a detective story than a law journal article—and is befitting the underlying facts of the case, involving a bookie living in an apartment on Sunset Boulevard—uncovers the story behind the origin of the now-famous *Katz* test.[47] The proposed test was not mentioned in the record of the lower courts nor in the briefs filed with the Supreme Court.[48] Rather, the notion of an *objective* test based upon the tort law reasonable man standard came as an epiphany to a twenty-nine-year-old lawyer during his preparation for oral argument before the Supreme Court.[49]

Schneider, who was the then twenty-nine-year-old lawyer, wrote that as he prepared for oral argument, it dawned upon him that the proper argument and questions were not about whether the FBI agents engaged in a trespass or whether the phone booth was a constitutionally protected area, but rather "whether a reasonable person . . . could have expected his communication to be private."[50] "The test was an *objective* one, not the *subjective* test that had been . . ." discussed in the briefs.[51] Schneider wrote that during oral argument, he made clear that what he was proposing was an objective test.[52] He wrote that when Justice White "asked . . . a question that seemed to suggest he was focusing on a subjective test," he (Schneider) responded that he was suggesting "an objective test of whether a third party, looking at the overall scene, would arrive at that conclusion."[53] Schneider wrote about how he explained to the Court how he thought the reasonable expectation of privacy test should be applied:

> We propose a test using a way that's not too dissimilar from the tort "reasonable man" test . . . . [W]e would ask that the test be applied as to

44. *See supra* note 29 and accompanying text.

45. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

46. Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1 (2009); Harvey A. Schneider, Katz v. United States: *The Untold Story*, 40 MCGEORGE L. REV. 13 (2009).

47. Winn, *supra* note 46.

48. *Id.* at 10.

49. *Id.*

50. Schneider, *supra* note 46, at 19.

51. *Id.* (emphasis added).

52. *Id.*

53. *Id.* at 20.

> whether or not a third person objectively looking at the entire scene could reasonably interpret, and could reasonably say, that the communicator intended his communication to be confidential.[54]

Winn wrote about how the background and origin of the reasonable expectation of privacy test remained largely unknown for over forty years.[55] It was not until the transcripts of the oral arguments of Supreme Court cases became available online that this story came to light.[56] Winn wrote that while listening to the oral arguments,

> one cannot help but sense the electricity in the air as he [Schneider] presented the test for the first time to the public. The justices seized on the test like children with a new toy, ran through various hypothetical fact situations, and then tested it against common intuitions of privacy norms.[57]

Winn wrote that, during the oral argument, Schneider repeatedly "emphasized the *objective* nature of the test."[58] Nonetheless these exchanges were largely ignored and the *Katz* test took on a life of its own—one that was likely very different than the one proposed for it at its conception.

In a 2015 article, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*,[59] Orin Kerr made two important points: 1) in the vast majority of cases that have applied the *Katz* test over the years, the vast majority apply only the objective test, and 2) Justice Harlan very likely never intended that there be a second-prong, a subjective inquiry.[60] Regarding the first point, Kerr did an empirical study of the 540 cases that used the *Katz* test, and concluded that very few even attempted the second part of the test.[61]

> The results of the study suggest that the subjective prong of *Katz* is irrelevant. A majority of cases applying *Katz* did not mention subjective expectations. Only 12 percent of *Katz* cases purported to apply the subjective test. Only 2 percent of *Katz* cases claimed to hinge their analysis on the subjective test.[62]

Regarding the second point, Kerr argued that Harlan never intended that there be a separate subjective test.[63] Despite the fact that the test has almost always been described and applied with two parts, Kerr focused on Harlan's statement in the concurring opinion that the test was "an understanding of the rule that has emerged from prior decisions."[64] Harlan "did not intend to create a new test

54. *Id.*
55. Winn, *supra* note 46, at 10.
56. *Id.*
57. *Id.*
58. *Id.*
59. Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015).
60. *Id.*
61. *Id.* at 116–22.
62. *Id.* at 122.
63. *Id.* at 124.
64. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

from whole cloth."[65] Rather, Kerr read Harlan's oft-quoted paragraph enunciating the test as three separate sentences: one articulating the test, one explaining the subjective test, and one explaining the objective test.[66]

> [1] My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." [2] Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. [3] On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[67]

Rather than creating the prongs of a two-part test, and true to Harlan's assertion that he was not creating a new test, one can read the second sentence as referring to the then-existing line of cases involving a "voluntary exposure of protected spaces" and the third sentence as referring to the then-existing "protected-area cases."[68] This explanation is consistent with the language in the second sentence that states that one loses protection in "objects, activities, or statements that he exposes to the 'plain view' of outsiders."[69] This would explain why Harlan referred to this line of cases as "subjective" in nature. It would also explain why he stated that the "rule . . . has emerged from prior decisions."[70] In this regard, Harlan's *subjective* test merely restated language from the majority opinion that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[71] This view is certainly consistent with what Winn and Schneider wrote about the purely *objective* nature of the test proposed in the *Katz* oral arguments before the Supreme Court. It would also add a great bit of sad irony in explaining fifty years of misguided judicial interpretation.

Regardless of what may or may not have been intended by *Katz*, as Dan Solove has written, "the reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency."[72] Solove wrote that while the test promised the flexibility of being able to evolve with and adapt to emerging technologies and societal values, it has "failed to live up to aspirations."[73] In the years following *Katz*, the Supreme Court has "adopted a conception of privacy that countless

65. Kerr, *supra* note 59, at 124.
66. *Id.* at 123.
67. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
68. Kerr, *supra* note 59, at 126.
69. *Id.* at 126–27.
70. *Id.* at 124.
71. *Id.* at 126 (quoting *Katz*, 389 U.S. at 351–52).
72. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511 (2010).
73. *Id.* at 1519.

commentators have found to be overly narrow, incoherent, short-sighted, deleterious to liberty, and totally out of touch with society."[74] "As Justice Scalia once stated, 'In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, [reasonable expectations of privacy] bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable.'"[75]

Another problem with the reasonable expectation of privacy standard is the inevitability of shrinking expectations. As Shaun Spencer predicted in 2002, every time there is an encroachment of privacy, society's expectations are diminished.[76]

> So, for example, if employers monitor their employees' telephone or e-mail use while they are in the workplace, they diminish the expectation of privacy in the workplace. If merchants routinely sell consumers' personal data, they diminish the expectation of privacy in one's transactional information. And if the Supreme Court holds that law enforcement may review citizens' bank records without a warrant, it diminishes the societal expectation of privacy in one's bank records.[77]

These encroachments occur gradually and just "seem to be the inevitable price of progress."[78] Spencer predicted that from time to time, industry or government might go too far with its intrusions into "settled societal expectations" and that an adjustment or retreat would be necessary.[79]

If the Supreme Court were ever to revisit the *Katz* test and redefine it as the one-prong, subjective test that it was proposed and intended to be, it could dramatically change the much-distorted notion of a "reasonable expectation of privacy." As I do not believe that this re-interpretation is very likely to happen, I will keep this item fairly low on my list.[80]

### 7. PRIVATE ADOPTION OF FEDERAL STANDARDS

Given the absence of omnibus legislation that dictates specifics regarding protection of personal information, there has been a growing trend in private industry to adopt some of the best practices of the federal government. The National Institute for Standards and Technology (NIST), a federal agency, has been very active in producing stringent standards for federal agencies regarding security and privacy.[81]

---

74. *Id.*

75. *Id.* at 1521 (quoting Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring)).

76. Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L.R. 843 (2002), at https://scholarship.law.umassd.edu/fac_pubs/74/.

77. *Id.* at 860; *see also* Susan Park, *Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy*, 51 AM. BUS. L.J. 779, 798–99 (2014).

78. *Id.* at 861.

79. *Id.* at 866.

80. For purposes of this article, "low" means closer to reason #10 and "high" means closer to reason #1.

81. *See* NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/ (last visited Mar. 23, 2019).

Its Cybersecurity Framework[82] was created to "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[83] It has been so successful that many private organizations, while not required to do so, have adopted it.

> A recent Gartner study reported that NIST's Cybersecurity Framework is already used by 30% of U.S organizations. This number is expected to rise to 50% by 2020. According to a March 2016 survey by Dimensional Research, 70% of these organizations adopted the framework to align themselves with cybersecurity best practices, 29% were required to do so by business partners, and 28% adopted the framework because of federal contract requirements.[84]

Lee Kim, Director of Privacy and Security at the Healthcare Information Management Systems Society (HIMSS) urged healthcare organizations to adopt NIST's Cybersecurity Framework: "it is voluntary and can be applied to virtually all organizations."[85] "The Framework not only provides technical guidance on how to build a comprehensive security program, but it also provides suggested methodology for communicating among internal and external stakeholders about cybersecurity risk."[86] "The NIST Cybersecurity Framework provides guidance on how executives and non-executives can communicate about cybersecurity risk both inside and outside of the organization."[87]

Similarly, in a document called "Why you should adopt the NIST Cybersecurity Framework," PwC urged its clients to adopt the standard:

> It is our opinion that the NIST Cybersecurity Framework represents a tipping point in the evolution of cybersecurity, one in which the balance is shifting from reactive compliance to proactive risk-management standards. While the Framework is voluntary, organizations across industries may gain significant benefits by adopting the guidelines at the highest possible risk-tolerance level given investment capital.[88]

---

82. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. NIST released version 1.1 of the Cybersecurity Framework on April 16, 2018. NAT'L INST. OF STANDARDS AND TECH., NIST RELEASES VERSION 1.1 OF ITS POPULAR CYBERSECURITY FRAMEWORK (Apr. 16, 2018), https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

83. Executive Order 13636, 78 Fed. Reg. 11,739, 11741 (Feb. 19, 2013).

84. Armand J. Zottola, *NIST in the Private Sector*, LEXOLOGY (Mar. 22, 2017), http://www.lexology.com/library/detail.aspx?g=2878150e-9c01-4c05-b6fd-06dbac58b4f7.

85. Lee Kim, *Building Holistic, Robust Security with the NIST Cybersecurity Framework*, HIMSS (Apr. 18, 2017), http://www.himss.org/news/building-holistic-robust-security-nist-cybersecurity-framework.

86. *Id.*

87. *Id.*

88. JIM GUINN, II, PWC, WHY YOU SHOULD ADOPT THE NIST CYBERSECURITY FRAMEWORK 7 (2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

In January 2017 Congressman Ralph Abraham introduced a bill that would strengthen the reach of the Cybersecurity Framework.[89] Among other things, it would establish a federal working group and a public-private working group "to help the public and private sector use the framework more effectively."[90]

As more structured approaches to security and privacy emerge—and they will likely come from governmental bodies, either here or in the European Union—private organizations will be more inclined to adopt them. As private organizations realize that they are facing more liability for breaches in security or privacy, they will likely move towards whatever established standards exist in order to be able to claim adherence to best practices. We are starting to see this happen, and I believe it will continue to become more and more common.

### 6. MERGER OF SECURITY AND PRIVACY INTERESTS IN SYSTEM DESIGN

At least since 9/11, privacy and national security often have been viewed as competing interests. Security can only be achieved at the cost of privacy, and privacy can only be achieved at the cost of security. Security experts often view privacy as a subpart of security, and privacy experts often view security as a subpart of privacy. Fortunately, there is a growing recognition that, rather than being competing interests, they are actually complimentary interests, and are often intricately intertwined.

Given the success of NIST's Cybersecurity Framework, it is not surprising that NIST followed up with a Privacy Framework.[91] One of NIST's goals was to "enable the creation of new systems that mitigate the risk of privacy harm and address privacy risks in a measurable way within an organization's overall risk management process."[92] The Privacy Framework is built upon three objectives, predictability, manageability, and disassociability "for the purpose of facilitating the development and operation of privacy-preserving information systems."[93] The general approach in designing the Privacy Framework was the same as for the Cybersecurity Framework: to have objectives that would "provide a degree of precision and measurability, so that system designers and engineers, working with policy teams, can use them to bridge the gap between high-level principles and implementation."[94]

The Privacy Framework acknowledges that while security and privacy are clearly different, they are often intertwined: "[p]ublic discourse on the relationship

---

89. Press Release, Abraham Introduces the NIST Cybersecurity Framework Bill (February 28, 2017), https://abraham.house.gov/media-center/press-releases/abraham-introduces-nist-cybersecurity-framework-bill.

90. *Id.*; *see also* Amber N. Craig, Scott J. Shackelford, Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 723–24 (2015).

91. SEAN BROOKS ET AL., NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS, NAT'L INST. STANDARDS AND TECH. (2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. This was actually a revised version of an initial document. MICHAEL GARCIA ET AL., PRIVACY RISK MANAGEMENT FOR FEDERAL INFORMATION SYSTEMS, NAT'L INST. STANDARDS AND TECH. (2015), http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.

92. INFO. TECH. LAB., NAT'L INST. STANDARDS AND TECH., SUMMARY OF THE PRIVACY ENGINEERING WORKSHOP AT THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/privacy-workshop-summary-052114.pdf.

93. GARCIA ET AL., *supra* note 91, at 1.

94. *Id.* at 21.

between security and privacy often includes colloquial phrases such as 'security and privacy are two sides of a coin' and 'there is no privacy without security.'"[95] "Recognizing the boundaries and overlap between privacy and security is key to determining when existing security risk models and security-focused guidance may be applied to address privacy concerns—and where there are gaps that need to be filled in order to achieve an engineering approach to privacy."[96]

The privacy principles in the Privacy Framework are built largely upon the requirements enunciated in the Office of Management and Budget's Circular A-130,[97] which were built largely upon the Fair Information Practice Principles first enunciated by the Department of Health, Education, and Welfare in 1973.[98] By presenting these principles as much as possible as system privacy requirements, NIST attempts to facilitate a privacy-by-design, engineering approach to building systems that will be trustworthy and will protect personal information.[99]

The Privacy Framework represents the most ambitious attempt to covert fuzzy privacy principles into quantifiable and measurable system requirements. Inasmuch as this approach has been very successful regarding Cybersecurity, there is good reason to believe it will have similar success as this approach evolves and becomes more widely accepted in both the public and the private realm.

### 5. NARROWING OF THE THIRD-PARTY DOCTRINE

Two Supreme Court cases from the 1970s significantly directed the evolution of privacy law as it pertained to personal information. In *United States v. Miller*, the Supreme Court held that an individual does not have an expectation of privacy in financial records once he or she has shared them with a bank.[100] Three years later, in *Smith v. Maryland*, the Court held that there was no expectation of privacy in a list of phone numbers that a person has dialed once that list has been shared with the phone company. [101] This so-called "third-party doctrine" evolved way beyond what those justices could have possibly envisioned at the dawn of the digital age. It has proven to be a major obstacle to the protection of personal information. Basically, the doctrine has been interpreted to mean that as soon as someone transmits data to any third party, he or she has waived any right to limit its distribution or use. This is, way more often than not, an absurd result, and the doctrine has been rightfully criticized.[102]

---

95. BROOKS ET AL., *supra* note 91, at 7.

96. *Id.* at 8.

97. OFFICE MGMT. AND BUDGET, CIRCULAR NO. A-130 (2016), https://iapp.org/media/pdf/resource_center/a130revised.pdf.

98. U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41-42 (1973).

99. BROOKS ET AL., *supra* note 91, at 1.

100. United States v. Miller, 425 U.S. 435, 443 (1976).

101. Smith v. Maryland, 442 U.S. 735, 742 (1979).

102. Daniel Solove criticized the doctrine as being ill-suited for today's data-driven world and as over-emphasizing the *secrecy* aspect of privacy: "Life in the modern Information Age often involves exchanging information with third parties, such as phone companies, Internet service providers, cable companies, merchants, and so on. Thus, clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world." Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1152 (2002). Solove has also asked: "Would the Supreme Court really hold that people lack an expectation

In *Carpenter v. United States*, the Supreme Court limited the scope of the third-party doctrine in a 5-4 decision written by Chief Justice Roberts and joined by Justices Ginsburg, Breyer, Sotomayor and Kagan.[103] The Court refused to extend the doctrine to cell-site location information (CSLI) that is generated automatically and continuously whenever an individual's phone is turned on.[104] The Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[105] It recognized that there is a "world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of information casually collected by wireless carriers today."[106] The Court held that this chronicle of information "implicates privacy concerns far beyond those considered in *Smith* and *Miller*," and refused to extend the doctrine to CSLI.[107] The Court did not, however, provide a bright-line test for future cases.[108]

Four separate dissenting opinions presented a variety of objections, some of which were focused on traditional Fourth Amendment jurisprudence, but some of which, arguably, provided some hope for the future of data protection.[109] Justice Thomas questioned the defendant's interest and ability to object to a search of the CSLI maintained by the cell phone company, but stated that the "more fundamental problem with the Court's opinion, however, is its use of the 'reasonable expectation of privacy' test."[110] He believed that the Court needs to reconsider the *Katz* test.[111]

Justice Alito began his dissent: "I share the Court's concern about the effect of new technology on personal privacy, but I fear that today's decision will do far more harm than good."[112] His dissent focused on two objections: first, that "the Court ignor[ed] the basic distinction between an actual search . . . and an order merely requiring a party to look through its own records and produce specified documents,"[113] and second, that "the Court allows a defendant to object to the search of a third party's property."[114] His decision in *Carpenter* was much anticipated because of his concurring opinion in *Jones v. U.S.* (which was joined by Justices Ginsburg, Breyer and Kagan), regarding the use of a GPS tracking device.[115] In *Jones*,

---

of privacy in their medical information because they convey that information to their physicians? This result would strike many as absurd." Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1532 (2010); *see also* Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441 (2017).

103. Carpenter v. United States, 138 S. Ct. 2206 (2018).

104. *Id.* at 2220.

105. *Id.* at 2219.

106. *Id.* at 2220.

107. *Id.*

108. *Id.* at 2221–23.

109. *See* Jordan M. Blanke, Carpenter v. United States *Begs for Action*, 2018 U. ILL. L. REV. Online 260 (2018); *see also* Peter Ormerod and Lawrence J. Trautman*, A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALBANY L.J. SCI. & TECH. 73 (2018).

110. *Carpenter*, 138 S. Ct. at 2236 (Thomas, J., dissenting).

111. *Id.*

112. *Id.* at 2246–47 (Alito, J., dissenting).

113. *Id.* at 2247.

114. *Id.*

115. United States v. Jones, 565 U.S. 400, 418 (2012) (Alito, J., concurring).

Justice Alito was very concerned about how new technology could affect expectations of privacy:

> [T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately provide significant changes in popular attitudes.[116]

He suggested that in "circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[117]

Justice Gorsuch's dissent provides several instances of optimism for the future of data privacy protection. First, he appeared ready to abandon the third-party doctrine entirely, agreeing with criticisms like the "third-party-doctrine is not only wrong, but horribly wrong,"[118] recognizing that people "often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private,"[119] and stating that the Court has never provided a persuasive justification for the doctrine.[120]

Second, Justice Gorsuch criticized the "often unpredictable—and sometimes unbelievable—jurisprudence"[121] that has come from the *Katz* test and warned about extending it to "data privacy cases."[122] In criticizing the Court's lack of direction on how to apply what's left of the third-party doctrine, he stated that "[a]ll we know is that historical cell-site location information . . . escapes *Smith* and *Miller's* shorn grasp, while a lifetime of bank or phone records does not."[123] "In the Court's defense, though, we have arrived at this strange place not because the Court has misunderstood *Katz*. Far from it. We have arrived here because this is where *Katz* inevitably leads."[124]

Finally, Justice Gorsuch suggested another way of approaching the facts of the case. First, just because a third party "has access to or possession of your papers and effects does not necessarily eliminate your interest in them"[125] and "[j]ust because you entrust your data—in some cases, your modern day papers and effects—to a third party may not mean you lose any Fourth Amendment protection in its contents."[126] Second, he stated that he doubted whether "complete ownership or exclusive control of property is always necessary to the assertion of a Fourth Amendment right."[127] "At least some of this Court's decisions have already suggested that use of technology is functionally compelled by the demands of modern

116. *Id.* at 427.
117. *Id.* at 429.
118. *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).
119. *Id.* at 2263.
120. *Id.*
121. *Id.* at 2266.
122. *Id.*
123. *Id.* at 2267.
124. *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).
125. *Id.* at 2268.
126. *Id.* at 2269.
127. *Id.*

life."[128] Third, Justice Gorsuch concluded by also calling for legislation: "positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition. State (or sometimes federal) law often creates rights in both tangible and intangible things."[129] "If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decision-making than judicial guesswork about societal expectations."[130]

While *Carpenter* did not overturn the third-party doctrine as it applies to data, it did provide a majority of justices who recognized that there have been "seismic shifts in digital technology"[131] since the doctrine arose in the 1970s and refused to extend it to CSLI. Furthermore, there are several justices who would like to see legislation that addresses privacy data protection and who would like to see the *Katz* test revisited.

### 4. SOCIAL NORMS CONTINUE TO EVOLVE

This is the item that is the most difficult to quantify, yet is most related to and most intertwined with many of the other items in this list.[132] Ultimately, it is the most important factor because the strength and prevalence of privacy values and social norms will determine the extent and scope of data privacy protection.

Ever since Scott McNealy's and Mark Zuckerberg's proclamations that privacy is dead,[133] there has been much discussion about whether people even care about privacy anymore, and if so, just how much. A number of studies seem to suggest that, while people say they care about their privacy, they often are unwilling to do anything to protect it.[134]

---

128. *Id.* at 2270.

129. *Id.*

130. *Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J., dissenting).

131. *Id.* at 2219.

132. Regarding *supra* #9 Influence of Contextual Integrity Research, Alice Marwick and danah boyd describe privacy as a "social construct that reflects the values and norms of individuals within cultures" and discuss how contextual privacy is key to privacy. Alice E. Marwick & danah boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y 1051, 1053–54 (2014); *see supra* text accompanying notes 27–44. Regarding *supra* #8 Reinterpretation of the Katz Test, the very nature of the "reasonable expectation of privacy" standard is dependent upon social values and norms. *See supra* text accompanying notes 45–75. Regarding *supra* #5 Narrowing of Third Party Doctrine, *Carpenter's* narrowing of the third-party doctrine and the call for legislation are largely a result of the disconnect between society's perception of privacy and the law's treatment of same. *See supra* text accompanying notes 103–131. Regarding *infra* #3 Recognition of Trust as Privacy Factor, trust is one of the major factors driving the evolution of social values and norms. *See infra* text accompanying notes 155–166. Regarding *infra* #2 Privacy as Business Strategy, businesses are realizing that consumers' expectations are changing and are, possibly, willing to pay for privacy. *See infra* text accompanying notes 171–185. And regarding *infra* #1 Peer Pressure—The European Union and California, people are realizing that they can and should expect more data privacy protection from the law. *See infra* text accompanying notes 186–239.

133. Sprenger, *supra* note 1; Kilpatrick, *supra* note 2.

134. *See* Idris Adjerid, Eyal Peer & Alessandro Acquisti, *Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making*, SSRN (April 16, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765097; *see* Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509 (2015); Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249 (2013); SARAH SPIEKERMANN, JENS

More recent information seems to support Neil Richards' positions that 1) privacy is not dead, and 2) young people do care about privacy.[135] An Australian study about privacy in the digital world found that 40 percent of respondents disagreed with the statement, "[t]here is no privacy, get over it."[136] People over 70 years old were the group most likely to agree with that statement.[137] More than half of the respondents disagreed with the statement, "[c]oncerns about privacy online are exaggerated."[138] Interestingly, about a third of them were undecided, perhaps suggesting some confusion about the issue. When asked whether they felt that they could control their privacy online, almost half of 18 to 29 year-olds said they could; only 34 percent of those over 40 thought that they could.[139] This is certainly consistent with the view that, while younger people have grown up with a different privacy environment, they are concerned about and take steps to protect their privacy.

In the aftermath of the Facebook debacle involving the use of personal data Cambridge Analytica, the Pew Research Center found that there is "a renewed focus on how social media companies collect personal information and make it available to marketers."[140] As will be discussed in more detail below, California recently passed a very extensive privacy law, under threat of an even stricter proposal planned as a ballot initiative.[141] The "ballot measure had been polling at around 80 percent approval."[142] The California Assembly approved the measure 69-0 and the Senate approved it 36-0.[143] "It was a remarkable sea change from last year when one of the authors of the new bill . . . tried to pass a bill that [was much less rigorous]. That bill didn't make it out of committee."[144] There appears to be much more concern for data protection than there has been in quite some time.

In his classic book *Code and Other Laws of Cyberspace*, Lawrence Lessig wrote that four constraints regulate behavior in cyberspace: the law, social norms, the

---

GROSSKLAGS & BETTINA BERENDT, E-PRIVACY IN 2ND GENERATION E-COMMERCE: PRIVACY PREFERENCES VERSUS ACTUAL BEHAVIOR, 38–47 (2001).

135. *See generally* NEIL M. RICHARDS, FOUR PRIVACY MYTHS (2014).

136. Catherine Hanrahan, *Young People Do Care About Privacy, Despite What Mark Zuckerberg and George Brandis Say*, ABC NEWS (Nov. 27, 2017), http://www.abc.net.au/news/2017-11-27/digital-privacy-surveillance-facebook-young-australians/9179240.

137. *Id.*

138. *Id.*

139. *Id.*

140. Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/. Kimberly Houser and Gregory Voss discussed how Facebook's share of the social media market dropped after the Cambridge Analytica incident, likely suggesting that people *do* care about their privacy. Kimberly Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1 (2018), https://jolt.richmond.edu/gdpr-the-end-of-google-and-facebook-or-a-new-paradigm-in-data-privacy/.

141. *See infra* text accompanying notes 218–239.

142. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html.

143. Jessica Guynn, *California Passes Nation's Toughest Online Privacy Law*, USA TODAY (June 28, 2018), https://www.usatoday.com/story/tech/2018/06/28/california-lawmakers-pass-tough-new-online-privacy-rules-could-model-other-states/743397002/.

144. *Id.*

market, and architecture (or code).[145] In describing how social norms can easily be downplayed when it comes to defining the regulation of privacy, danah boyd and Alice Marwick stated that "social norms are inherently unstable and constantly evolving; they vary widely and are difficult to pin down."[146] They wrote, "[w]hen it comes to privacy, social norms are evolving, but not disappearing."[147]

Omer Tene and Jules Polonetsky questioned the "role of regulation in the absence of stable social norms"[148] when society attempts to address rapid and drastic changes in technology. "Should restrictions on conduct be based on law or on softer social norms? Should regulation drive or be driven by volatile individual expectations, market best practices, and social norms? Should we wait for norms to develop to form societal expectations?"[149] They observed that in the past, "privacy values and norms took years or even centuries to develop,"[150] but that as "technological innovation accelerates, so does the need to recalibrate individual expectations, social norms, and, ultimately, laws and regulations."[151] They stated that "[t]hree main vectors of influence drive the changes that affect individuals' perceptions of privacy and social norms:" businesses, technologies, and individuals.[152]

We have seen ever-increasing acceleration from each of these forces since they wrote their article in 2013. Businesses "are constantly pushing *more* users to engage *more* often and share *more* data, sometimes pushing against social norms and challenging traditional values."[153] Technology continues to push the envelope with smaller, faster, more powerful, and more invasive devices. And individuals continue to share more and more information as they are tempted by—and generally satisfied by—all the new and shiny bells and whistles.

Social norms develop over time. Generally, they are molded by advancements and improvements in technology, along with individuals' willingness to participate in new flows of information. Sometimes, however, adjustments are made. Often, they are a result of outrage.[154] When something like Cambridge Analytica happens, the public pays more attention to the issues directing those evolving norms. I believe that we are at a time now where those norms are particularly in flux.

### 3. RECOGNITION OF TRUST AS IMPORTANT PRIVACY FACTOR

In recent years there has been a good bit of research indicating just how important trust is today regarding privacy and the digital world. Neil Richards and Woodrow Hartzog stated that trust is an "essential ingredient for our digital

145. *See generally* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 123 (Version 2.0 2006).

146. danah boyd & Alice E. Marwick, *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*, SSRN (Sept. 22, 2011), https://ssrn.com/abstract=1925128.

147. *Id.*

148. Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 71 (2013).

149. *Id.*

150. *Id.* at 72.

151. *Id.* at 73.

152. *Id.* at 76.

153. *Id.* at 77.

154. *See* Jordan M. Blanke, *Privacy and Outrage*, 9 CASE W. RES. J.L. TECH. & INTERNET 1 (2018).

lives."[155] "Without trust, people share less information, bad information, or no information at all. They become anxious, bewildered, and suspicious . . . . If people don't trust a company, they are more likely to switch to a competitor or resist or fail to become fully invested in the commercial relationship."[156] They argued that "modern privacy law is incomplete because from its inception it has failed to account for the importance of trust."[157] "One of the bedrock notions of privacy law is that companies should be transparent about their data collection, use, and disclosure practices so that individuals will be on notice of any potentially worrisome practices and can tailor their disclosures accordingly."[158] "Trust need not be exclusively a matter of government policy. Companies can also voluntarily adopt trust-enhancing internal policies, safeguards, and organizational schemes . . . . Companies can delete data when it is no longer needed and collect no more information than is necessary for the information relationship."[159]

Richards and Hartzog summarized how trust can best be promoted in the context of personal information by describing four characteristics or values that must exist within our data stewards:

> First, trustworthy stewards are *honest* because they explain to us the terms under which they hold and use our data. . . .
>
> Second, they are *discreet* because they treat our data as presumptively confidential and do not disclose it in ways contrary to our interests or expectations.
>
> Third, trustworthy stewards are *protective* because they hold the data securely against third parties, doing everything within reason to protect us from hacks and data breaches.
>
> Fourth, and most fundamentally, those we trust are *loyal* because they put our interests ahead of their own short-term potential for gain.[160]

Ari Ezra Waldman has written extensively about privacy as trust.[161] He wrote that "privacy, particularly in the information-sharing context, is really a social construct based on trust between social sharers, between individuals and Internet intermediaries, between groups of people interacting online and offline. . . ."[162] He believes that trust underlies our most basic notions of privacy. He wrote that at the

---

155. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 433 (2016).

156. *Id.* at 435.

157. *Id.*

158. *Id.* at 462.

159. *Id.* at 465.

160. Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1214 (2017).

161. Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2015) [hereinafter *Privacy as Trust*]; Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193 (2016) [hereinafter *Privacy, Sharing, and Trust*]; Ari Ezra Waldman, *A Breach of Trust: Fighting Nonconsensual Pornography*, 102 IOWA L. REV. 709 (2017) [hereinafter *Breach of Trust*]; *see generally* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018).

162. *Privacy as Trust*, *supra* note 161, at 590.

core of society's relatively quick response to ban "revenge porn" was the recognition that this represented a flagrant and egregious breach of trust.[163] "Trust is a resource of social capital between or among two or more persons concerning the expectations that other members of their community will behave according to accepted norms. It is . . . the belief that others will behave in a predictable manner."[164] This is yet another example of how it often takes an incident, or a series of incidents, to illicit public outrage that prompts a legislative or regulatory response.[165]

Waldman also wrote about how important trust is to our ever-growing social networks, most notably, Facebook. He described how Facebook's model is built almost entirely on trust and about how extensively Facebook manipulates and abuses that trust. He wrote that Facebook's platform

> not only creates the circumstances for social interaction with those we trust, it exploits the trust we have in our friends and families for financial gain by manipulating us into sharing information with third party advertisers . . . [and that] Facebook's design strategy to leverage trust to manipulate us into clicking on those advertisements should give us pause. Regulators should step in.[166]

Facebook keeps trying to push the envelope. It has certainly had opportunities to cultivate, rather than destroy, public trust—or at least, the perception of trust. It recovered from a good bit of bad publicity in 2014 regarding its unauthorized experimental with A/B testing.[167] It is now mired in possibly its biggest challenge—to

163. *Breach of Trust*, *supra* note 161, at 716.

164. *Id.*; *see also* Jordan M. Blanke & Janine S. Hiller, *Predictability for Privacy in Data Driven Governments*, 20 MINN. J.L. SCI. & TECH. 32 (2018).

165. *See* Jordan M. Blanke, *Privacy and Outrage*, 9 CASE W. RES. J.L. TECH. & INTERNET 1 (2018); *see* Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 J. HIGH TECH. L. 42 (2014).

166. *Privacy, Sharing, and Trust*, *supra* note 161, at 196.

167. Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, ATLANTIC (June 28, 2014), https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/; Vindu Goel, *Facebook Tinkers With Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (June 29, 2014), https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html; Josh Constine, *The Morality of A/B Testing*, TECHCRUNCH (June 29, 2014), https://techcrunch.com/2014/06/29/ethics-in-a-data-driven-world/.

justify the use of data by Cambridge Analytica to apparently manipulate a presidential election.[168] Mark Zuckerberg publicly acknowledged that this was a "major breach of trust."[169]

Facebook seems willing to try to get away with as much as it possibly can. In 2016 it vehemently denied using geolocation data to suggest new friends in one's news feed.[170] Anecdotally, I recently visited some softball fields on which I played for many years. Many of my current Facebook friends are former softball buddies. The day after my visit, at least seven of the first ten suggested friends that popped up on my Facebook feed were guys with whom I had just spoken in person the day before. Most of these were people I had not seen in many months and, I don't believe, had ever appeared in my suggested friends list before.

The growing body of literature about trust suggests that there is finally a basic understanding that this is an important aspect of our digital lives. Companies will no longer be able to claim a blind eye with regard to this important factor—and those that do will likely suffer in the marketplace.

### 2. PRIVACY AS BUSINESS STRATEGY

In a Harvard Business Review article, *Privacy is a Business Opportunity*, David Hoffman wrote a few years ago that "privacy protection should be a practice as fundamental to the business as customer service. Privacy is an essential element of

168. *Can Facebook Restore Public Trust After Cambridge Analytica Scandal?*, CBSNEWS (Mar. 24, 2018 4:34 PM), https://www.cbsnews.com/news/facebook-cambridge-analytica-restore-public-trust-after-privacy-scandal/; Chris Kahn & David Ingram, *Americans Less Likely to Trust Facebook than Rivals on Personal Data: Reuters/Ipsos Poll*, REUTERS (Mar. 25, 2018 8:04 AM), https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3; Cyrus Farivar, *Facebook Accused of Massive Fraud in New Lawsuit Filed by Cook County*, ARSTECHNICA (Mar. 25, 2018 11:30 AM), https://arstechnica.com/tech-policy/2018/03/cook-county-illinois-sues-facebook-and-cambridge-analytica-over-data-breach/; Eric Johnson, *The Facebook-Cambridge Analytica Apology Tour Continues, With Full-Page Ads in Major Newspapers*, RECODE (Mar. 25, 2018 11:36 AM), https://www.recode.net/2018/3/25/17161262/facebook-cambridge-analytica-apology-ads-newspapers-data-washington-post-new-york-times.

169. Kevin Roose & Sheera Frenkel, *Mark Zuckerberg's Reckoning: 'This Is a Major Trust Issue'*, N.Y. TIMES (Mar. 21, 2018), https://www.nytimes.com/2018/03/21/technology/mark-zuckerberg-q-and-a.html; Ben Riley-Smith, *Mark Zuckerberg 'Really Sorry' for Facebook's 'Major Breach of Trust' over Cambridge Analytica Scandal*, TELEGRAPH (Mar. 22, 2018 8:51 AM), https://www.telegraph.co.uk/technology/2018/03/21/mark-zuckerberg-breaks-silence-facebook-made-mistakes-cambridge/; Daniel Politi, *Facebook's Zuckerberg Takes Out Full Page Ads to Say "Sorry" for "Breach of Trust"*, SLATE (Mar. 25, 2018 12:42 PM), https://slate.com/news-and-politics/2018/03/facebooks-zuckerberg-takes-out-full-page-ads-to-say-sorry-for-breach-of-trust.html.

170. Kashmir Hill, *Facebook is Using Your Phone's Location to Suggest New Friends—Which Could Be a Privacy Disaster*, SPLINTER (June 28, 2016, 1:45 PM), https://splinternews.com/facebook-is-using-your-phones-location-to-suggest-new-f-1793857843; Denver Nicks, *Facebook Might Be Using Your Location to Suggest Friends. Here's How to Make Sure It Doesn't*, TIME (June 28, 2016, 5:42 PM), http://time.com/money/4386138/facebook-friend-suggestions-privacy-concerns/; Kate Conger, *Facebook Says It's Not Making Friend Suggestions Based on Your Location After All*, TECHCRUNCH (June 28, 2016), https://techcrunch.com/2016/06/28/facebook-says-its-not-making-friend-suggestions-based-on-your-location-after-all/; Lauren O'Neil, *Is Facebook Using Your Location Data to Suggest 'People You May Know'?*, CBC (June 28, 2016, 9:41 PM), http://www.cbc.ca/news/trending/facebook-gps-location-data-new-friends-people-you-may-know-1.3656555.

being a good business partner."[171] He stated that many corporate boardrooms are now discussing "what should be done to integrate privacy as an added value to the business."[172] He stated that it had been estimated "that brand value represents nearly one-third of the $12 trillion in market capitalization of the S&P 500."[173] "When an incident related to privacy occurs, it is a direct blow to the brand's esteem and its financial value."[174] This has certainly been the case recently with Facebook losing an estimated $50-60 billion in value in a matter of days as a result of the Cambridge Analytica episode.[175]

Hoffman wrote that the "shift to a fundamentally digital economy means that, regardless of the sector you are in, your ability to protect individuals will distinguish your company from competitors who have taken a passive approach or who ignore their responsibilities."[176] He predicted that in the near-future, "some healthcare provider will surely earn a reputation among consumers and within the industry as the company that takes the greatest care to protect their patients' information."[177] He predicted similar results in other sectors.

In a recent white paper entitled *Revitalizing Privacy and Trust in a Data-Driven World*, PwC summarized some if its findings from The Global State of Information Security Survey 2018.[178] Among its nine insights on data privacy and trust were: "The challenge for CEOs is going beyond awareness to action," "[b]eyond confidentiality, privacy expectations focus on data use," and "[c]onsumers will vote for responsible innovation and data use with their wallets."[179]

Regarding the first item, PwC reported that "[t]here is some cause for optimism . . . 87% of global CEOs say they are investing in cybersecurity to build trust with customers. Nearly as many (81%) say they are creating transparency in the usage and storage of data."[180] Regarding the second item, PwC stated that "data privacy is becoming more about controlling how data is *used*."[181] It noted that NIST included the goal of "disassociability" in its recent Privacy Framework and that the EU's GDPR emphasized both privacy by design and data minimization.[182]

Regarding the third item, PwC contended that "[c]onsumers do put a monetary value on privacy—but context matters. It may seem paradoxical when consumers voice privacy concerns while still providing personal data online, but this does

171. David Hoffman, *Privacy is a Business Opportunity*, HARV. BUS. REV. (Apr. 18, 2014), https://hbr.org/2014/04/privacy-is-a-business-opportunity.

172. *Id.*

173. *Id.*

174. *Id.*

175. Romain Dillet, *Facebook Has Lost $60 Billion in Value* TECHCRUNCH (Mar. 20, 2018), https://techcrunch.com/2018/03/20/facebook-has-lost-60-billion-in-value/; Joseph Karaian, *Facebook's Value Destruct-o-Meter: $50 Billion and Counting*, QUARTZ (Mar. 20, 2018), https://qz.com/1233816/facebook-has-lost-50-billion-in-market-value-over-the-past-two-days/.

176. Hoffman, *supra* note 171.

177. *Id.*

178. PWC, REVITALIZING PRIVACY AND TRUST IN A DATA-DRIVEN WORLD 1 (2018), https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf.

179. *Id.* at 2.

180. *Id.* at 4.

181. *Id.* at 6 (emphasis added).

182. *Id.* at 7.

not mean consumers do not value privacy."[183] It discussed the work of Alessandro Acquisti, whose "research suggests that privacy preferences are shaped by context as opposed to being absolute."[184] The report stated that "consumers will pay more for technology products that are designed with security and privacy in mind." In its summary, among the things that PwC urged leaders to do were "prioritize data-use governance" and "view GDPR as an opportunity . . . to align their organizations to where they need to be for future success, not merely for compliance but rather for strategic risk management."[185]

This recognition by corporate leadership that privacy is important and can be used for strategic advantage is long overdue. As more businesses recognize the dangers of ignoring its consumers concerns about their data, we will see a major growth in an attempt to "sell privacy." More companies will invest in best practices to protect data and to inform their customers exactly what and why they are doing. As the PwC report noted, with the GDPR having recently come into effect, there has never been a better time for companies to become serious about protecting data.

## 1. PEER PRESSURE—THE EUROPEAN UNION AND CALIFORNIA

### A. The European Union

The much-anticipated General Data Protection Regulation (GDPR) of the European Union became effective on May 25, 2018,[186] basically replacing the Data Directive of 1995.[187] It is the most aggressive attempt anywhere to provide for the protection of personal data. It contains many significant changes that appear likely to have, in many cases, worldwide effect.

Any company that wants to continue doing business globally—and that includes doing business in the EU or having customers, suppliers, or other contacts who reside in the EU—will have to make changes to its past practices. The scope of the GDPR includes the processing of the personal data of any EU resident, regardless of where that data may actually be stored and processed.[188] Any company that does business with or in the EU will have to pay attention to the new regulations.

Companies will have to decide if it is worth maintaining different policies and practices for EU residents and for non-EU residents. I do not think it will be. For most large companies, it will be easier just to adopt GDPR-friendly practices across the board. Obviously, this would be a major bonus for residents of the United States—and elsewhere—when it comes to protecting personal data.

---

183. *Id.* at 14.

184. PWC, *supra* note 178, at 14; *see* Alessandro Acquisti, Curtis R. Taylor & Liad Wagman, *The Economics of Privacy*, 52 J. ECON. LITERATURE 1, 29 (2016); *see also* Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509 (2015).

185. PWC, *supra* note 182, at 15–16.

186. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ (EC) (General Data Protection Regulation), 2016 O.J. (L 119) 1 (hereinafter "GDPR"); *see also* W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L. J. (forthcoming 2019).

187. Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 1 (EC).

188. GDPR, *supra* note 186, at 32–33.

At the heart of the GDPR is its Article 5: Principles relating to processing of personal data:

> 1. Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; . . . ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; . . . ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; . . . ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').[189]

These principles are based upon, and are the most rigorous manifestation of, the principles first enunciated in the FIPPs (1973),[190] then in the OECD Guidelines (1980),[191] the EU Data Protection Directive (1995),[192] and most recently, for federal agencies, the Office of Management and Budget Circular A-130 (2016).[193] Some of the trickle-down effects of the GDPR will likely provide the greatest amount of data protection that U.S. residents have ever had.

A major change under the GDPR is a return to one of the cornerstone principles of the FIPPS—a true and legitimate consent.[194] Consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes . . . by a statement or by clear affirmative action signif[ying] agreement to the processing of personal data."[195] If consent is obtained by a written document that also concerns any other matter, the "request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible

---

189. *Id.* at 35–36.

190. U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41–42 (1973).

191. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION & DEV., (Sept. 1980), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

192. Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 1 (EC).

193. OFF. OF MGMT. AND BUDGET, CIRCULAR NO. A-130 (2016), https://iapp.org/media/pdf/resource_center/a130revised.pdf.

194. *See* Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" The Keys to Successful Spyware Legislation*, 7 COLUM. SCI. & TECH. L. REV. 1, 16–18 (2006).

195. GDPR, *supra* note 186, at 34.

form, using plain and clear language."[196] This means that the request for consent can no longer be in fine print or legalese, and there can no longer be pre-checked boxes or opt-in consent. Furthermore, consent can be withdrawn at any time.[197]

Once there is consent, and according to the principles of Article 5, the data shall be "processed lawfully, fairly and in a transparent manner,"[198] "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible manner,"[199] "adequate, relevant and limited to what is necessary" for the specified purposes,[200] "accurate and . . . kept up to date,"[201] and "kept in a form which permits identification of data subjects for no longer than necessary."[202] This marks a sea change in how data would be processed in the United States.

Additionally, without specific consent, the processing "of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of generic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or orientation shall be prohibited."[203] Member states would be able to further restrict or limit the processing of "genetic data, biometric data or data concerning health."[204]

Individuals will have the right to access their personal data held by controllers,[205] will have the right to have inaccurate information corrected,[206] will have the right to have personal data erased "without undue delay"[207] if the data is "no longer necessary in relation to the purposes for which they were collected. . . or processed,"[208] or if the individual withdraws consent,[209] or if the data "ha[s] been unlawfully processed."[210]

Furthermore, an individual may object to the processing of data used for purposes of direct marketing and the practice of profiling to the extent that it is used for direct marketing.[211] When an individual objects to the use of personal data for direct marketing purposes, "the personal data shall no longer be processed for such purposes."[212] The individual also has "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[213]

196. *Id.* at 37.
197. *Id.*
198. *Id.* at 35.
199. *Id.*
200. *Id.*
201. GDPR, *supra* note 186, at 35.
202. *Id.* at 36.
203. *Id.* at 38.
204. *Id.* at 39.
205. *Id.* at 43.
206. *Id.*
207. GDPR, *supra* note 186, at 43.
208. *Id.*
209. *Id.* at 44.
210. *Id.*
211. *Id.* at 45.
212. *Id.*
213. GDPR, *supra* note 186, at 46.

The GDPR will apply to the processing of personal data of residents of the EU "regardless of whether the processing takes place in the [EU] or not."[214] In order to continue to do business with, and maintain personal data on EU residents, companies around the world will have to make drastic changes to their current policies and practices.

While many U.S. companies have already made changes to their privacy policies,[215] it remains to be seen just how much of the GDPR they actually adopt. There are many far-reaching requirements of GDPR that appear highly unlikely to be followed by U.S. companies. While some basic provisions will probably be modeled, it will be surprising if many companies adopt all of the GDPR. For example, in a statement made recently before Congress, Facebook's Mark Zuckerberg appeared to say that Facebook would abide by the new law[216] but later seemed to backtrack from that statement.[217]

Even if companies were to adopt the basic principles relating to the processing of data, as described above—which would be in and of itself an enormous change for most companies—it would be hard to imagine adoption of some of the more far-reaching requirements related to access, correction, erasure, and retention of data. Furthermore, it is unlikely that some of the restrictions on the use of data for direct marketing and profiling purposes would be widely adopted voluntarily.

### B. California

Shortly after the GDPR became effective, California adopted a rigorous new law that incorporates many of the same basic principles: The California Consumer Privacy Act of 2018 (CCPA) becomes effective on January 1, 2020.[218] The bill was passed unanimously by the California legislature under threat of a stricter law that was being planned for submission as a ballot initiative that "had been polling at around 80 percent approval."[219] High tech companies "Google, Facebook, Verizon,

214. *Id.* at 32.

215. Many companies notified users of changes to their privacy policies on or before May 25, 2018. Julia Powles, *The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy*, NEW YORKER (May 25, 2018), https://www.newyorker.com/tech/elements/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy.

216. Josh Constine, *Zuckerberg Says Facebook Will Offer GDPR Privacy Controls Everywhere*, TECHCRUNCH (Apr. 4, 2018), https://techcrunch.com/2018/04/04/zuckerberg-gdpr/; Sarah Jeong, *Zuckerberg Says Facebook Will Extend European Data Protections Worldwide — Kind Of*, VERGE (Apr. 11, 2018), https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection.

217. Michael Veale*, Ignore Mark Zuckerberg*, SLATE (Apr. 12, 2018), https://slate.com/technology/2018/04/mark-zuckerbergs-misleading-promise-that-eu-privacy-rules-will-apply-to-american-facebook-users.html; Mark Scott & Nancy Scola, *Facebook Won't Extend EU Privacy Rights Globally, No Matter What Zuckerberg Says*, POLITICO (Apr. 19, 2018), https://www.politico.eu/article/facebook-europe-privacy-data-protection-mark-zuckerberg-gdpr-general-data-protection-regulation-eu-european-union/.

218. A.B. 375, 2017–18 St. Assemb., Reg. Sess. (Cal. 2018); Jessica Guynn, *California Passes Nation's Toughest Online Privacy Law*, USA TODAY (Jun. 28, 2018), https://www.usatoday.com/story/tech/2018/06/28/california-lawmakers-pass-tough-new-online-privacy-rules-could-model-other-states/743397002/; Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (Jun. 28, 2018), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/; *see* Wakabayashi, *supra* note 142.

219. Wakabayashi, *supra* note 142.

Comcast and AT&T each contributed $200,000 to a committee opposing the proposed ballot measure, and lobbyists had estimated that businesses would spend $100 million to campaign against it before the November election."[220] There is still concern that those same groups will use the time before the law becomes effective to "water it down."[221]

The CCPA will give Californians far greater protection for their personal information than anywhere else in the United States. Californians will have "the right to request that a business that collects . . . personal information disclose . . . the categories and specific pieces of personal information the business has collected."[222]

> A business that collects . . . personal information, shall, at or before the point of collection, inform . . . as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing . . . notice.[223]

"Personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[224] It includes, but is not limited to a "real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport, or similar identifiers."[225]

Californians will have the right to request a business to delete personal information that has been collected about them.[226] They will be able to request that a business disclose to them the categories of personal information it has collected, the categories of sources from which the personal information is collected, the business or commercial purposes for collecting or selling the personal information, the categories of third parties with whom the business shares the personal information, and the specific pieces of personal information it has collected.[227] They will be able to make similar requests about personal information that was sold to third parties by the business.[228]

Californians will have the right to opt out from the sale of their personal information to third parties.[229] Additional restrictions may apply when individuals are less than 16 years of age.[230] Businesses will not be able to discriminate against those making requests under the law by denying goods or services, or charging different

---

220. *Id*.
221. *Id*.
222. A.B. 375, 2017–18 St. Assemb., at 1798.100 (a) (Cal. 2018).
223. *Id.* at 1798.100 (b).
224. *Id.* at 1798.140 (o)(1).
225. *Id.* at 1798.140 (o)(1)(A).
226. *Id.* at 1798.105 (a). The business is not required to comply with the request for a number of specified reasons. A.B. 375, 2017–18 St. Assemb., at 1798.105 (d) (Cal. 2018).
227. A.B. 375, 2017–18 St. Assemb., at 1798.110 (a) (Cal. 2018).
228. *Id.* at 1798.115 (a).
229. *Id.* at 1798.120 (a).
230. *Id.* at 1798.120 (d).

prices, or providing a different level or quality of goods or services,[231] unless the "difference is reasonably related to the value provided to the consumer by the consumer's data."[232] Businesses will be able to "offer financial incentives, including payments to consumers as compensation, for collection of personal information, the sale of personal information, or the deletion of personal information."[233] A business will only be able to enter a consumer into a financial incentive program with prior opt-in consent[234] and cannot use a program that is "unjust, unreasonable, coercive, or usurious in nature."[235]

The law will require businesses to "[m]ake available to consumers two or more designated methods for submitting requests for information required to be disclosed . . . including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address."[236] It will require that certain information about the law be included in a business's online privacy policy.[237] The law will also require that a business which sells personal information "[p]rovide a clear and conspicuous link on the business' Internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information."[238] A business will not be able to "require a consumer to create an account in order to direct the business not to sell the consumer's personal information."[239]

It will be interesting to see if special interest groups will be able to water down the requirements of the law as it now stands. California has certainly raised the bar for data protection in the United States. It will also be interesting to see how many other states use this law as a model for legislation.

## II. CONCLUSION

The last several items on this list, particularly the evolution of societal privacy norms and values, the recognition of the importance of trust as a privacy factor, the realization that privacy can be used as a successful business strategy, and the EU and California legislation, have provided a climate that is probably as conducive for change in privacy laws as it has been since prior to 9/11. Hopefully there is enough energy from these factors to push the evolution of data privacy protection in a new direction. Only time will tell.

231. *Id.* at 1798.125 (a)(1).
232. *Id.* at 1798.125 (a)(2).
233. A.B. 375, 2017–18 St. Assemb., at 1798.125 (b)(1) (Cal. 2018).
234. *Id.* at 1798.125 (b)(3).
235. *Id.* at 1798.125 (b)(4).
236. *Id.* at 1798.130 (a)(1).
237. *Id.* at 1798.130 (a)(5).
238. *Id.* at 1798.135 (a)(1).
239. A.B. 375, 2017–18 St. Assemb., at 1798.135 (a)(1) (Cal. 2018).