Journal of Law, Technology & the Internet • Vol. 9 • 2018

PRIVACY AND OUTRAGE

by Jordan M. Blanke*

INTRODUCTION

It is not an understatement that technology has dramatically altered virtually every aspect of our life in recent years. While technology has always driven change, these changes are occurring more rapidly and more extensively than ever before. We are fully entrenched in the world of Big Data, the Internet of Things, and Smart Cities – and we are never going back. As always, society and its laws must evolve, but it is not always an easy process.

The notion of privacy has certainly changed in our data-driven world and continues to change daily. While it has always been difficult to define exactly what privacy is, it is even more difficult to propose what privacy should become. Technology and its uses – or abuses – are altering the notion of privacy into something that may be unrecognizable in the near future.

Studies show that people say they are still concerned about privacy, but their behavior does not reflect that.[1] Like any value, the importance of privacy varies from person to person. This makes it even more difficult to establish a one-size-fits-all concept of privacy. This paper explores some of the historical, legal, and ethical development of privacy; discusses how some of the normative values of privacy may survive or change; and examines how outrage has been – and will continue to be – a driver of such change.

*Ernest L. Baskin, Jr. Distinguished Professor of Computer Science and Law, Stetson School of Business and Economics, Mercer University, Atlanta, GA. He teaches a variety of courses in law, ethics, and technology at both the graduate and undergraduate levels. His research includes privacy, cyberlaw, and copyright law and he has had articles published in journals such as the Hastings Law Journal, the Washington and Lee Law Review, the Columbia Science and Technology Law Review, and the American Business Law Journal. Professor Blanke presently serves as President of the Academy of Legal Studies in Business.

[1] Manoush Zomorodi, *Do You Know How Much Private Information You Give Away Every Day?* TIME (Mar. 29, 2017), http://time.com/4673602/terms-service-privacy-security/ (last visited Mar. 10, 2018); Lee Rainie, *The State of Privacy in Post-Snowden America,* PEW RESEARCH. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (last visited Mar. 10, 2018); Natasha Lomas, Do Americans Care About Privacy? It Depends, Because Privacy is Personal…(Jan. 14, 2016), https://techcrunch.com/2016/01/14/privacy-is-personal/ (last visited Mar. 10, 2018); Josh Steimle, Survey Shows You Don't Care About Privacy As Much AS You Think You Do. FORBES. (Nov. 7, 2014), https://www.forbes.com/sites/joshsteimle/2014/11/07/survey-shows-you-dont-care-about-privacy-as-much-as-you-think-you-do/#f9bf602d9de0 (last visited Mar. 10, 2018).

PRIVACY

While a legally protected right to privacy in the United States traces its roots back little more than a century and a quarter,[2] privacy as a social value or norm arguably has roots as old as humankind. In fact, one of the fathers of the notion of modern privacy, Alan Westin, believed that the importance of privacy as a basic characteristic is seen even among other species in the animal kingdom – "men and animals share several basic mechanisms for claiming privacy among their own fellows."[3]

Westin described four basic states of privacy: 1) solitude – the desire of an individual to separate from the group and be free, at least temporarily, from observation by others; 2) intimacy – the ability of an individual to have a close relationship with someone else in a pairing (e.g., marriage) or small group (e.g., family); 3) anonymity – the ability of a person to participate in a public forum or venue, while being free from identification or surveillance; and 4) reserve – the most subtle state, the "creation of a psychological barrier against unwanted intrusion."[4] Westin also defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[5] We will see that this becomes a dominant theme in privacy scholarship and is certainly relevant today.

Charles Fried stated that "[p]rivacy is not simply an absence of information about what is in the minds of others; rather it is the control we have over information about ourselves."[6] Similarly, Ruth Gavison described privacy as a form of limiting access to oneself, and stated that the "concept of privacy . . . is a complex of . . . three independent and irreducible elements: secrecy, anonymity, and solitude."[7]

More recently Daniel Solove summarized six different conceptions of privacy: 1) the right to be left alone; 2) limited access to the self; 3) secrecy; 4) control over personal information; 5) personhood – "the protection of one's personality, individuality, and dignity;" and 6) intimacy.[8] He noted that there may be overlap between and among the conceptions and that they are not independent of one another, "[f]or example, control over personal information can be seen as a subset of limited access to the self, which in turn bears significant similarities to the right to be let alone."[9]

---

[2] The origin of privacy as a legal notion in the United States traces back to Samuel Warren and Louis Brandeis's article proposing a right "to be let alone." Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L.R. 193, 206 (1890).

[3] ALAN F. WESTIN, PRIVACY AND FREEDOM, 8-11 (1967).

[4] *Id*. at 32-34.

[5] *Id*. at 7.

[6] Charles Fried, *Privacy*, 77 YALE L.J. 475, 477-78 (1968).

[7] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 433 (1980).

[8] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL L. REV. 1087, 1092 (2002).

[9] *Id*.

There have been many different approaches to describing what privacy is and what privacy should be throughout history[10]. It is a fundamental aspect of humankind that has evolved and continues to evolve. Technology often drives social change, and with respect to privacy, that has certainly been the case. As society adapts, so does the notion of privacy.

NORMATIVE VALUES OF PRIVACY AND CONTEXT

Robert Post wrote about the normative values of privacy behind the rationale for the four branches of the common law invasion of privacy tort[11]. In discussing the intrusion branch, he cited Erving Goffman's notion of "territories" or "preserves" that help define a space in which someone could expect to have privacy[12] . These spaces are not defined by objective standards like feet or inches, but rather by subjective standards that are socially determined based upon context. In discussing the public disclosure branch, he again refers to Goffman's notion of "information preserves" or "boundaries" within which information is contained and which are normatively determined[13]. "[J]ust as individuals expect to control certain spatial territories, so they expect to control certain informational territories."[14] The boundaries of these information spaces are determined by local custom and by "the norm of the ordinary man" and are important in defining the standards of civility which support the public disclosure tort.[15] "Information preserves, like spatial territories, provide a normative framework for the development of individual personality. Just as we feel violated when our bedrooms are invaded, so we

---

[10] *See generally* DANIEL J. SOLOVE and PAUL M. SCHWARTZ, CONSUMER PRIVACY AND DATA PROTECTION 25-45 (2015) for an excellent discussion on the history and evolution of the definition and value of privacy.

[11] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 971-72 (1989). The four branches of the tort of invasion of privacy are summarized in the RESTATEMENT (SECOND) OF TORTS § 652A (1977):

> (1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
> (2) The right of privacy is invaded by:
> (a) unreasonable intrusion upon the seclusion of another, as stated in 652B; or
> (b) appropriation of the other's name or likeness, as stated in 652C; or
> (c) unreasonable publicity given to the other's private life, as stated in 652D; or
> (d) publicity that unreasonably places the other in a false light before the public, as stated in 652E.

[12] Post, *supra* note 9, at 971-72 (citing Erving Goffman, *The Territories of the Self*, in RELATIONS IN PUBLIC: MICROSTUDIES OF THE PUBLIC ORDER 28 (1971)).

[13] *Id*. at 984.

[14] *Id*.

[15] *Id*. at 984-85.

experience the inappropriate disclosure of private information as 'pollutions or defilements'".[16]

Jeffrey Rosen continued the theme of privacy and context, describing how, in "a world of short attention spans," information can easily be taken out of context.[17] If personal information is shared in a group of people familiar with the subject of the information, they can digest that information in context, weighing it against other information they know about that person's character and personality[18]. If, however, that same information is shared with strangers, there is no context against which the information can be judged[19].

In her classic paper, *Privacy as Contextual Integrity*, Helen Nissenbaum emphasized the importance of context: "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'"[20]. Almost everything we do "happens in a context not only of place but of politics, convention, and cultural expectation."[21] In virtually every aspect of our daily life, we move among various spheres, realms, or contexts – being at home with one's family, visiting a doctor, going to church – that are, to various degrees, defined by distinct sets of norms. These spheres "offer a platform for a normative account of privacy in terms of contextual integrity."[22]

Nissenbaum stated that contextual norms can come from various sources, including history, culture and law[23]. Many of them involve information. She proposed "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."[24]

Contextual integrity often explains how social values evolve and become part of the social structure and law. Nissenbaum stated that the "context of elections for political office is [an example] of a settled normative framework."[25] There are high expectations of privacy when people vote. They vote without anyone knowing for whom or for what they voted. Unless they decide to share this information, no one else will know. They fully control the flow of information.

---

[16] *Id*. at 985.
[17] Jeffrey Rosen, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA, 8 (2000).
[18] *Id*. at 8-9.
[19] *Id*. at 9.
[20] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137 (2004).
[21] *Id*.
[22] *Id*. at 138
[23] *Id*.
[24] *Id*.
[25] *Id*. at 146.

In the United States, there are only a few areas in which individuals have control over their information. If it is credit-related, medical-related or pertains to video rental habits (amazingly), laws provide a degree of control over the information flow[26].For the most part, however, if the information pertains to anything else, there is very little law that controls the flow. Changes in law are often driven by changes in values. Is it possible that sufficient change in the normative values of privacy – particularly in the flow of information – can dictate changes in the law? Is it possible that such changes in normative values can sufficiently modify behavior even without changes in the law?

One of the cases that Nissenbaum examined in her 2004 article dealt with consumer profiling and data mining[27].The issues she presented then have only been exacerbated over time. With regard to consumer profiling and data mining, Nissenbaum noted 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."[28] With the proliferation of collection of data from sensors, smart phones and the Web, and the advent of Smart Cities, and the trend towards the merger of public and private data, this observation becomes even more significant and more prescient.

Nissenbaum shows how Amazon.com's use of data analytics on information provided to it by its customers arguably does not breach either the norm of appropriateness or the norm of flow[29]. A grocer's collection of information about customers' vacation or movie choices might not breach the norm of appropriateness. But if that grocer then sells the information to a data broker, where that information will likely be used out of context, there may very well be breaches of both the norms of appropriateness and flow. Society surpasses these examples from 2004, but is it still possible that our privacy norms can be modified? Can society develop a different value expectation regarding the collection or use of information? Is it possible to develop a new normative expectation of privacy in information?

Adam Moore gives an extreme example of the type of data shifting – or breach of contextual integrity – that Nissenbaum described[30]. Actress Rebecca Schaeffer provided her home address to her local department of motor vehicles, who then sold it to a data broker, who then sold it to a man, who went to Schaeffer's

[26] Privacy protection in the United States is very sectoral in its approach. For example, information relating to credit ratings is highly regulated under the Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681); medical information is highly regulated under the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104–191, 110 Stat. 1936, enacted August 21, 1996); and video rental habits are highly regulated under the Video Privacy Protection Act (18 U.S.C. § 2710). Information not regulated by one of these specific laws is subject to very little regulation.
[27] Nissenbaum, *supra* note 20, at 152.
[28] *Id*.
[29] *Id*. at 152-53.
[30] Adam D. Moore, *Toward Informational Privacy Rights*, 44 SAN DIEGO L. REV 809, 826 (2007).

house, and murdered her. Moore sees digitization and aggregation of data as making the potential for this type of misuse even more likely[31]. Certainly this is even more true today. Aggregation of data has reached a point where it is questionable whether uses of data can even be separated anymore.

Anita Allen writes that she has "explored the normative ethical value of privacy, evaluated the normative ethics of privacy laws, and pondered the extent of normative ethical obligations to protect one's own and others' privacy."[32] Recently she questions whether "individuals . . . have a moral obligation to protect their own privacy information."[33] Focusing on information privacy, she describes the current era as the "Great Privacy Give-Away," in which people are "giving away more and more personal data to intimates and strangers for a variety of . . . reasons."[34] Allen stated,

> Among duties to self is a duty to protect one's own informational privacy. One ought to limit disclosures of information about oneself for utility reasons, pertaining to one's reputation and future opportunity; and/or virtue reasons, pertaining to modesty, reserve and temperance; and/or Kantian reasons, pertaining to dignity, self-respect, autonomy, and freedom.[35]

In a presentation of Allen's recent paper regarding New York's decision to protect a photographer who took photographs of people, in various intimate positions, through the open windows of their homes, there was a discussion about how social norms of price vary[36]. A woman from the Netherlands said that back home many people also do not have curtains on ground floor apartments, but it is custom not to look into another person's home. She stated that children are taught this at an early age and it has become a social norm there.

Certainly, social norms are affected by many things – morals, ethics, values, customs, expectations, technology – and these change over time. Allen notes that within her lifetime it used to be socially – and legally – acceptable to ban marriage between people of different races[37]. Until very recently, marriage between people of the same gender was illegal. It was not until social values and

---

[31] *Id*.
[32] Anita L. Allen, *Privacy Law: Positive Theory and Normative Practice*, 126 HARV. L. REV. 241, 241 (2010).
[33] Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 846 (2013).
[34] *Id*. at 846-47.
[35] *Id*. at 852.
[36] Ninth Annual Privacy Law Scholars Conference at the George Washington University School of Law, June 2, 2016. *See infra* notes 75-80 and accompanying text.
[37] Allen, *supra* note 33, at 849.

norms changed sufficiently enough that there became a demand that the law change as well.

Roger Ford provided several examples of how social norms change, some becoming more permissive and some more restrictive, and how this sometimes also prompts changes in law[38]. He discussed how Douglas Ginsburg's admission in 1987 of marijuana use basically derailed his Supreme Court nomination. He also discussed how subsequent admissions by Clarence Thomas, Bill Clinton and Barack Obama did little more than make news headlines[39]. He noted how, as recently as 1968, "George Wallace won five states and forty-six electoral votes, running for president on an openly segregationist platform – a result that would be unimaginable today."[40] Social norms can and do change over time.

Ford discussed how privacy norms regarding information flows have become less permissive as more and more information is being collected and used for, among other things, targeted advertising. He noted that some privacy norms have changed over the years to become *more* protective of privacy. For example, voting in the 1880s and 1890s, student records under FERPA in 1974, and sensitive personal information in federal court filings in 2007.[41] While each of these examples involved changes of law, they were, as is often the case, a response to changing social norms.[42] Ford gave an example of Nissenbaum's contextual integrity: "[n]o one blinks an eye when a dating website asks someone about his or her romantic preferences . . . but it would be strange if Amazon, or the DMV, started asking shoppers or applicants for driver's licenses if they prefer blondes or brunettes."[43] Ford wrote his article in 2016. Unless our normative values of privacy and/or our laws change soon, there will be no need for Amazon or the DMV to ask that question – they will already know.

WHAT WILL IT TAKE TO CHANGE?

Much has been written in the last fifty years about the normative nature of privacy because of the *Katz* decision, and the importance of its normative reasonable expectation of privacy standard[44]. Unfortunately, much of the evolution

[38] Roger Allan Ford, *Unilateral Invasions of Privacy*, 91 NOTRE DAME L. REV. 1075, 1091 (2016).
[39] *Id*. at 1090.
[40] *Id*. at 1090 n.53.
[41] *Id*. at 1091.
[42] *Id*. at 1092.
[43] *Id*. at 1090.
[44] *See Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). The test has both a subjective and an objective part, although in recent years, there has been discussion that, as originally proposed, the test was to have had only an objective part. *See* 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);

of privacy in a digital world was thwarted by the events of 9/11 in 2001, which placed an almost insurmountable weight on the scales of the privacy versus security balancing test. For mostly understandable reasons, security is given great deference.

In describing what he says might be called the "security trumps" view – that "whenever privacy and security conflict, security wins", Adam Moore disputes why this view would have to be adopted over a "privacy trumps" view.[45] He questions why a strong privacy interest in ownership of data, for example, would not be "at least as fundamental or intuitively weighty as security."[46] Additional interest in privacy could actually increase security. He claims that "it is false to claim that more privacy means less security or that more security means less privacy."[47] Moore concludes that a "transparent society is not inevitable. Privacy at the personal level can be secured through custom and social pressure. Privacy related to big media, corporations and the state can be guaranteed by law and grounded in customs and social practices."[48]

The drive for transparency in cities and states adopting open records or open government laws provides another forum in which this issue may evolve[49]. There will be massive amounts of information, collected from a variety of sources – both public and private – and potentially used for a variety of purposes. Many of the same issues that apply to Nissenbaum's example of consumer profiling and data mining will apply here. Certainly there will be numerous issues of contextual integrity. Cities, like Seattle, which is using an open, collaborative, and iterative approach, are trying to develop new models for protecting privacy and may be instrumental in developing new norms and expectations for privacy[50].

Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015).

[45] Adam D. Moore, *Toward Informational Privacy Rights*, 44 SAN DIEGO L. REV 809, 839-40 (2007). There is a growing realization that privacy and security are intricately and necessarily intertwined. Often, one who works in security views privacy as a subset of security, and one who works in privacy views security as a subset of privacy. It is becoming apparent that the two interests are enhanced and stronger when designed and developed together. *See* Security and Privacy Controls for Information Systems, Draft NIST Special Publication 800-53, Revision 5, August 2017, http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf (last visited Sept. 5, 2017).

[46] *Id*. at 840.

[47] *Id*.

[48] *Id*. at 844.

[49] *See* What is Open Data? Open Data Handbook, http://opendatahandbook.org/guide/en/ (last visited Sept. 5, 2017); The 8 Principles of Open Government Data, https://opengovdata.org/ (last visited Sept. 5, 2017).

[50] *See* Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309, 332-34 (2017).

OUTRAGE

One of the things that can potentially shape a new norm is outrage. If enough people are outraged about an activity that violates a norm - or about a new activity for which there may not yet be a norm – change may result. For example, suppose an individual receives an email saying, "We notice how you voted for Reagan and Bush back in the 1980s, but that you then voted for Clinton and Obama in the 1990s and 2000s. We want you back. Please vote for the Republican candidate this year!"[51] Most people probably would be outraged. There are very strong social norms with regard to the privacy of information about voting – there are also laws protecting that privacy[52].

Several years back, there was an outcry when CVS sent non-customers a letter basically saying, "[w]e see your prescription for Prozac is about to run out. Why don't you transfer your prescription to us and we'll give you $20 off?" Many people were outraged at this seeming breach of privacy – at least what many people probably would have considered to be a breach of privacy.[53] And because it involved medical information, it also probably violated the law. In our current environment of Big Data and The Internet of Everything, there have certainly been many more examples of this type of use of data that would reach or exceed one's creepiness comfort level[54].

Data brokers, search engines, websites, apps and just about anything else capable of collecting information does so today. It is easy to say, "You have zero privacy. Get over it."[55] Regarding the massive amount of personal information that has already been collected, it is easy to think, "the cow is already out of the barn," or "the cat is already out of the bag." And to some extent, that is no doubt true.

---

[51] Or "We notice that you voted for Clinton and Obama. Why did you vote for Trump? We want you back. Please vote for the Democratic candidate this year!"

[52] *See* Caitriona Fitzgerald, Pamela Smith &Susannah Goodman, *The Secret Ballot at Risk: Recommendations for Protecting Democracy* (Aug. 18, 2016), http://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf (last visited Sept. 5, 2017).

[53] *See Health Privacy Stories* (Mar. 5, 2007), https://www.cdt.org/files/healthprivacy/20080311stories.pdf (last visited Sept. 5, 2017); David Lazarus, *Opening Your Pill Box for Bulk Mailers* (June 11, 2008), http://articles.latimes.com/2008/jun/11/business/fi-lazarus11 (last visited Sept. 5, 2017).

[54] *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59 (2013); Anna Johnston, *Creepiness is in the Eye of the Beholder* (Oct. 15, 2015), https://www.salingerprivacy.com.au/2015/10/15/creepiness/ (last visited Sept. 5, 2017); Sid Lipsey, *Collecting Customer Data Without Being Creepy,* https://relate.zendesk.com/articles/collecting-customer-data-without-creepiness/ (last visited Sept. 5, 2017).

[55] Edward C. Baig, Marcia Stepanek &Neil Gross, *Privacy: The Internet Wants Your Personal Information, What's in It for You?*, BUS. WK., Apr. 5, 1999, at 84 (quoting Scott McNealy, CEO of Sun Microsystems, at a product launch).

However, there are still abuses that can come from additional sharing of the data – certainly from cross-contextual uses – that can be avoided.

Bryce Newell wrote about defining a normative definition of informational privacy that would include "the right to control both initial and subsequent uses of personal information."[56] He stated that this right "should have legal 'teeth.'"[57] The absence of teeth in privacy law today is best illustrated by the many examples of leaked nude photographs of celebrities. For the most part, once the image is out of the barn or out of the bag, it is gone. There has been very little that one can do to enforce such a violation of privacy. Privacy law just has not had "teeth."

Due in great part to public outrage, we are finally beginning to see some change. Privacy law may actually be cutting some "baby teeth." In 2011, two nude selfies of Scarlett Johansson were published on the Web. Aware of the lack of success by previous attempts to threaten lawsuits alleging invasion of privacy, Johansson instead turned to copyright law, complete with its full set of teeth. Utilizing the "takedown" provision of the Digital Millennium Copyright Act, a very toothy provision, she notified websites that they were displaying copyrighted content and that they risked liability under copyright law if they failed to remove the photos[58]. This resulted in far more websites removing the photos than if the threat had been merely one involving privacy violations.

However, somewhat surprisingly, the hacker who stole the photos from Johansson's email account was prosecuted, and pleaded guilty to violations of the federal Computer Fraud and Abuse Act ("CFAA"), and was sentenced to the maximum 10 years in prison[59]. The court found that Johansson (and the other celebrities involved) had suffered both economic loss and severe emotional distress[60]. The Assistant Director in charge of the local FBI office stated that defendant's actions were "tantamount to breaking and entering of [the celebrities'] private homes by a thief in the night."[61] Consistent with slowly changing societal

---

[56] Bryce Clayton Newell, *Crossing Lenses: Policing's New Visibility and the Role of "Smartphone Journalism" as a Form of Freedom-Preserving Reciprocal Surveillance*, 34 U. ILL. J.L. TECH. & POL'Y 59, 75 (2014).

[57] *Id*.

[58] Pursuant to 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). This so-called "DCMA takedown notice" has become extremely common as a way of preventing liability for copyright infringement. Regardless of whether there might be infringement, taking down the allegedly infringing item is an easy and effective way to avoid liability.

[59] *See* 18 U.S.C. §§ 1030(a)(5) and 1030(a)(2)(C) (2012). *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, 580-81 (2016); Jessica E. Easterly, *Terror in Tinseltown: Who is Accountable When Hollywood Gets Hacked*, 66 SYRACUSE L. REV. 331, 348 (2016).

[60] Satti, *supra* note 59, at 580.

[61] *Id*. at 580-81.

values, some privacy laws, which have been on the books for quite some time, are beginning to be used more frequently and more effectively.

Similarly, in 2014, nude photos of many celebrities, including Jennifer Lawrence, were leaked and published on many websites[62]. While efforts to quickly remove the photos were not particularly effective, there have been two convictions under the CFAA. Apparently, most of the photos were obtained as a result of at least two, apparently independent, phishing scams whereby the hackers convinced the celebrities to divulge username and password information. Both convictions were obtained under a section of the CFAA prohibiting unauthorized accessing of a protected computer[63] . While both faced up to 5 years in prison, one defendant was sentenced to 18 months in October 2016[64] and the other to 9 months in January 2017[65].

We are beginning to see the results of some public outrage because of these celebrity hackings. Regarding the Jennifer Lawrence incident, the publication of the stolen photographs "has been lambasted by the public and media for being a gross invasion of privacy . . . Beloved public figures like Jennifer Lawrence, made vulnerable by having their naked bodies non-consensually exposed to the world, are . . . sympathetic characters."[66]

Public outrage has also been evident a few times regarding the failure of existing Peeping Tom statutes to successfully prosecute "upskirt photographers."[67] There have been several instances where upskirt photographers escaped conviction either because of narrow interpretations of "reasonable expectation of privacy" or because of the specific language in the relevant statute. In 2014 the Massachusetts Supreme Judicial Court overturned a conviction under the state's Peeping Tom statute because the statute required proof that the person photographed be "nude or partially nude."[68] Even though the "victim" was a transit officer who was part of a sting operation and there was ample evidence of the upskirt photography, the court

---

[62] *See* Easterly, *supra* note 56, at 334-35.

[63] 18 U.S.C. § 1030(a)(2)(C) (2012); *See* Satti, *supra* note 56, at 581-82; Easterly, *supra* note 59, at 348-49.

[64] Alan Yuhas, *Hacker Who Stole Nude Photos of Celebrities Gets 18 Months in Prison*, The Guardian (Oct. 27, 2016), https://www.theguardian.com/technology/2016/oct/27/nude-celebrity-photos-hacker-prison-sentence-ryan-collins.

[65] *Chicago Man Gets 9 Months in Celebrity Nude Photo Hack*, USA Today (Jan. 24, 2017), http://www.usatoday.com/story/life/movies/2017/01/24/chicago-man-gets-9-months-celebrity-nude-photo-hack/97011632/.

[66] Easterly, *supra* note 59, at 345.

[67] *See* 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); 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).

[68] Commonwealth v. Robertson, 5 N.E.3d 522, 529 (Mass. 2014) (refusing to apply Mass. Gen. Laws ch. 272, § 105(b) to upskirt photography)

strictly interpreted the language of the statute – because she was not nude or partially nude.[69] The public outcry was immediate[70] and two days after the court's decision, the governor signed into law new language to close the loophole[71].

Similarly, in Georgia, a 6-3 decision by the Georgia Court of Appeals overturned the conviction of an upskirt photographer because the relevant statute required that the photograph or recording be taken "in any private place and out of public view."[72] The court ruled that "place" referred to a physical location, rather than a part of the body, and since the recording was done in a public grocery store, it was not done in a private place as required by the statute.[73] There has been a great deal of public outrage about the decision and it is probably just a matter of time before the Georgia legislature fixes the loophole[74].

Another incident involving what many would likely deem to be an invasion of privacy has also sparked a call to action – most notably from the court rendering the decision. In the case mentioned earlier, regarding the photographer who surreptitiously took photographs of his neighbors through their open windows from his apartment, the New York Appellate Division of the Supreme Court, affirmed the dismissal of an invasion of privacy action brought by the parents of two children who were photographed[75]. Despite the fact that the subjects never knew about nor gave permission to the taking of the photographs, despite the fact that the photographs were of people in their own homes – and in some cases, in their bedrooms, despite the fact that some of the individuals, including one of the children, were recognizable from the photographs, and despite the fact that the address of the building was publicly disclosed as part of one of the exhibitions of

---

[69] *Id*.

[70] Haimy Assefa, *Massachusetts Court Says 'Upskirt' Photos Are Legal*, CNN (Mar. 6, 2014, 7:33 AM), http://www.cnn.com/2014/03/05/us/massachusetts-upskirt-photography/.

[71] Mark Mermot, Update: Massachusetts Bans 'Upskirt' Photography, NPR (Mar. 7, 2014, 9:00 AM), http://www.npr.org/sections/thetwo-way/2014/03/06/286690512/read-it-and-rate-it-court-rules-upskirt-photos-are-legal.

[72] *Georgia Appeals Court Says "Upskirting" is Legal*, CBS NEWS (July 25, 2016, 12:58 PM), http://www.cbsnews.com/news/georgia-appeals-court-upskirting-is-legal/.

[73] *Id*.

[74] Kristina Torres, *Senate Votes to Ban 'Upskirting' in Georgia*, AJC.com (Feb. 15, 2017, 12:02 PM), http://www.ajc.com/news/state--regional-govt--politics/senate-votes-ban-upskirting-georgia/lqjMcLuH55z6YZBPcV5K4M/..

[75] Foster v. Svenson, 128 A.D.3d 150 (N.Y. App. Div. 2015). *See* Hili Perlson, *Voyeuristic Photographer Arne Svenson Wins New York Appellate Court Case*, ARTNET NEWS (April 10, 2015), https://news.artnet.com/market/arne-svenson-neighbors-photographs-supreme-court-286916; Eugene Volokh, *N.Y. Court: Legal to Surreptitiously Photograph People in Their Own Homes, and Sell Those Photographs*, The Washington Post (April 10, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/04/10/n-y-court-legal-to-surreptitiously-photograph-people-in-their-homes-and-sell-those-photos/?utm_term=.ed161a4dcb3f ; Christopher Visentin, *Case Review: Foster v. Svenson (2015),* Center for Art Law (May 29, 2015), https://itsartlaw.com/2015/05/29/foster-v-svenson/.

the photographs, the case was dismissed. New York has never adopted the traditional common law tort of invasion of privacy, but rather, has statutory protection that addresses only the misappropriation prong of the tort[76]. Accordingly, the court held that the First Amendment value of the photographs as art, along with an absence of traditional commercial appropriation, required a dismissal of the claim[77].

The court held that "the defendant's conduct, however disturbing it may be, cannot properly, under the current state of the law, be deemed so 'outrageous' that it went beyond the decency and the protections" of the statutes[78]. The court continued, "we do not, in any way, mean to give short shrift to plaintiffs' concerns[79]. Undoubtedly, like plaintiffs, many people would be rightfully offended by the intrusive manner in which the photographs were taken in this case. However, such complaints are best addressed to the legislature."[80]

In an area of the law that may become the poster child for public outrage as a driver of change, 35 states and the District of Columbia have enacted legislation to ban so-called "revenge porn," or the nonconsensual publication of sexually graphic or intimate photographs or video[81]. Typically, it is an ex-husband or ex-boyfriend who distributes these photos or videos without the consent of his prior partner. In addition to legislation, many social media sites, including Google, Twitter and Reddit, largely in response to the public outcry, have also banned the practice[82].

An example of what might be better described as public outcry, rather than public outrage, about half of the states have passed, and almost all of the states have proposed, legislation that bans employers from requiring the disclosure of passwords related to an employee's or an applicant's social media accounts.[83] In

---

[76] N.Y. CIV. RIGHTS LAW §§ 50 and 51 (Consol. 2000).

[77] *Foster,* 128 A.D.3d at 160.

[78] *Id*. at 163

[79] *Id*.

[80] *Id*.

[81] *See* Ari Ezra Waldman, *A Breach of Trust: Fighting Nonconsensual Pornography*, 102 IOWA L. REV. 709, 710-11 n.4 (2017). The number of states is now up to 38 according to the web site, Cyber Civil Rights Initiative. *See* https://www.cybercivilrights.org/revenge-porn-laws/ (last visited Sept. 5, 2017).

[82] Waldman, *supra* note 81, at 711.

[83] *See* Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 J. HIGH TECH. L. 42 (2014); Susan Park, *Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy*, 51 AMER. BUS. L.J. 779 (2014); Robert Sprague, *No Surfing Allowed: A Review and Analysis of Legislation Prohibiting Employers from Demanding Access to Employees' and Job Applicants' Social Media Accounts*, 24 ALB. L.J. SCI. & TECH. 481(2014). *See also Access to Social Media Usernames and Passwords,* NAT'L CONF. ST. LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

2010, there was a well-publicized story about a job applicant in Maryland, who was required by a prospective employer to disclose his Facebook log-in and password as part of his job application process[84]. In 2012, largely in response to the public outcry from this incident, Illinois, Maryland, California and Michigan became the first states to pass legislation to curb this practice, with many other states modelling their legislation after those first efforts[85].

In recent decades, we have seen changes in social norms and behavior regarding copyright protection, first in the 1980s and 1990s regarding software, and then again in the late 1990s and early 2000s regarding digital music[86]. One significant difference, however, is that the drivers of the change in those cases were the content holders – the software companies and the music labels – and they had the significant "teeth" of the copyright law behind them. Lawrence Lessig wrote about how far behind protection for privacy is compared to protection for intellectual property, largely because of the traditional view of intellectual property as property[87]. It takes much longer to effect change if the general public is the driver rather than a defined group with a specific interest involved.

Another interesting example of outrage – although it may more properly be described as fear – dates back to the nomination of potential Supreme Court Justice Robert Bork. After a local Washington, D.C. reporter was able to obtain the history of all of Bork's videotape rentals from his local video store, a number of Congressmen learned that these type of records were actually being maintained[88].

---

[84] Meredith Curtis, *Want a Job? Password, Please!*, ACLU.org (Feb. 18, 2011, 2:04 PM), http://www.aclu.org/blog/technology-and-liberty/want-job-password-please. (video interview *available at* http://www.youtube.com/watch?v=bDaX5DTmbfY); Aaron C. Davis, *Md. Corrections Department Suspends Facebook Policy for Prospective Hires*, Wash. Post Breaking News Blog (Feb. 22, 2011, 9:58 PM), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207486.html.

[85] Blanke, *supra* note 83, at 42-48.

[86] In the 1980s and 1990s, the software industry was losing a lot of money from the illegal copying of software. After several years of playing cat and mouse games with a variety of copy-protection schemes, the industry more-or-less gave up on those schemes and relied instead on educating the public that while you *can* make a copy of the software, you *should not* make a copy. While illegal copying of software can never be eradicated, many people learned that it was not ethically appropriate to use software without paying for it. It took a long time for the software industry to change this normative behavior. Similarly, in the late 1990s and early 2000s, with the introduction of Napster and other peer-to-peer networks, the illegal copying of music was rampant. It took a long time for the music industry to effect some change in behavior with a combination of education, a series of lawsuits by the Recording Industry Association of America, and the introduction of the Apple Store (as a relatively painless alternative). Again, while illegal copying of music can never be eradicated, normative behavior has changed.

[87] *See* Lawrence Lessig, Privacy as Property, 69 SOC. RES. 247 (2002).

[88] *See* Stephen Advokat, *Publication of Bork's Video Rentals Raises Privacy Issue*, CHI. TRIB. (Nov. 20, 1987), http://articles.chicagotribune.com/1987-11-20/entertainment/8703270590_1_video-rentals-video-stores-bork-opponent (last visited Sept. 6, 2017); Michael Dolan, *Borking Around*, NEW REPUBLIC (Dec. 20, 2012),

In very short order, Congress passed the Video Privacy Protection Act of 1988[89]. Fortunately for members of Congress, their outrage – or fear – can be immediately remedied; unfortunately, for society, it generally takes a long time for public outrage to effect change.

WHAT THE FUTURE HOLDS

While public outrage can often trigger quick legislative response, it usually takes a good bit of time for social normative behavior to evolve. With regard to informational privacy, it becomes even more difficult because of the ever-changing technology and its immediate effect on daily life. Too often, this comes with a ready acceptance of a diminished privacy. There is reason, however, to be optimistic that the tide is beginning to turn when it comes to society's expectation of privacy and evolving social norms. Specifically, there are six themes or developments regarding privacy that are making the environment ripe for changes in values, social norms, and privacy laws:

1. The shift from an emphasis on notice and choice to collection and use[90]. While this is mostly attributable to the utter failure of notice and consent to provide any real privacy protection, the reality is that it is more important now to try to limit the collection and use of data - both data that has already

https://newrepublic.com/article/111331/robert-bork-dead-video-rental-records-story-sparked-privacy-laws (last visited Sept. 6, 2017).

[89] 18 U.S.C. § 2710 (1988).

[90] The Fair Information Privacy Principles (FIPPs) have been variously stated and have evolved over time, but have always included the notions of both notice and choice and collection and use. Introduced in 1973 by the Department of Health, Education, and Welfare in a document entitled *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm (last visited Sept. 6, 2017)), the FIPPs were then revised in 1980 by the Organization of Economic Cooperation and Development (OECD) in a document entitled *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the "OECD Guidelines") http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Mar. 10, 2018)). The OECD Guidelines were a primary source for the development of the European Data Directive of 1995 (Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1005 O.J. (L 281) (EC)) and are also largely the basis for the current iteration of FIPPs adopted by many federal agencies and incorporated into the Office of Management Budget's important 2016 revision, Circular A-130 (https://iapp.org/media/pdf/resource_center/a130revised.pdf (last visited Sept. 6, 2017). *See* Richard Warner and Robert Sloan, *Beyond Notice and Choice: Privacy, Norms and Consent*, 14 J. HIGH TECH. L. 370 (2014).

been collected and that which has not. Nissenbaum's contextual integrity theory is largely responsible for driving this change[91].

2. The recognition of the importance of trust as it pertains to privacy. Neil Richards and Woodrow Hartzog recently wrote that "modern privacy law is incomplete because from its inception it has failed to account for the importance of trust."[92] The role of trust in privacy relationships is beginning to emerge as an integral part of the normative value of privacy.
3. The recognition that the *Katz* "reasonable expectation of privacy" test is – and always should have been described as – solely an objective test[93]. This will empower courts to more accurately assess, based upon normative data, what "reasonable expectations" truly are and should be.
4. All of the efforts to convince people to design for privacy are starting to pay dividends[94] . Furthermore, people are realizing that both privacy and security solutions need to be designed harmoniously[95]. NIST's recent publication is a perfect example of this: *Security and Privacy Controls for Information Systems and Organizations*[96].
5. Peer pressure. The General Data Protection Regulation (GDPR) will become effective in May 2018 in the European Union[97]. Its omnibus approach to data protection is a stark contrast to the sectoral approach taken by the United States.[98]
6. Privacy as strategy. Companies are beginning to realize that privacy pays. Richards and Hartzog wrote "If people don't trust a company, they are more likely to switch to a competitor."[99] While NIST guidelines are required for federal agencies only, private industry has adopted many of the security standards set forth in its Cybersecurity Framework[100]. It is hoped that many

---

[91] *See supra* text accompanying notes 20-43.

[92] Neil Richards and Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 435 (2016).

[93] *See supra* note 44.

[94] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (2011), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (discussing how the Privacy by Design movement focuses on the notion of embedding principles of privacy in the design and architecture of information systems).

[95] *See supra* footnote 45.

[96] *Id*.

[97] Council Regulation 2016/679, 2016 O.J. (L 119) 87.

[98] *See supra* footnote 26.

[99] Richards and Hartzog, *supra* note 92, at 435.

[100] "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." Venable LLP, NIST in the Private Sector (March 22, 2017), http://www.lexology.com/library/detail.aspx?g=2878150e-9c01-4c05-b6fd-06dbac58b4f7 (last visited Sept. 6, 2017). *See also Nat'l Inst. of Standards and Tech., Framework for Improving Critical Infrastructure Cybersecurity (2014),*

companies will also adopt the principles of its Privacy Framework[101]. Additionally, while the GDPR pertains only to the EU and its citizens, many U.S. companies function globally and will have to comply with the new standards anyway, and are expected to adopt some of those standards across the board[102]. Companies are realizing that it makes sense for them to embrace and sell privacy.

CONCLUSION

One of the drivers of social change has always been outrage. We are beginning to see a number of examples of changes occurring because of dissatisfaction with current privacy standards.[103] There is often a swift legislative response, but it usually takes longer for social values or norms to adjust. It appears that the environment is ripe for change to take place. People's actual "expectations of privacy" may finally be able to shape new privacy values and norms for our digital world.

---

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (detailing what the framework consists of).

[101]Nat'l Inst. of Standards and Tech., Privacy Risk Management for Federal Information Systems (NISTIR 8062, 2017), http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf (a draft discussing NIST principles which could be implemented elsewhere).

[102]*See, e.g., Evidon, Evidon Debuts Industry's First GDPR and Cookie Law Universal Consent Platform (July 18, 2017), https://www.evidon.com/company/press-releases/evidon-debuts-universal-consent-platform/ (describing a U.S. company's development of web products targeted at companies who wish to comply with new GDPR standards).*

[103]As this article goes to press, Mark Zuckerberg and Facebook are attempting to survive the public outrage after the disclosure that vast amounts of personal information were acquired from Facebook by Cambridge Analytica. Facebook's value dropped $50-60 billion dollars within days of the disclosure. Romain Dillet, *Facebook Has Lost $60 Billion in Value* (Mar. 20, 2018), https://techcrunch.com/2018/03/20/facebook-has-lost-60-billion-in-value/ (last visited Mar. 28, 2018); Joseph Karaian, Facebook's Value Destruct-o-Meter: $50 Billion and Counting (Mar. 20, 2018), https://qz.com/1233816/facebook-has-lost-50-billion-in-market-value-over-the-past-two-days/ (last visited Mar. 28, 2018). Zuckerberg will likely testify before Congress amid cries for greater privacy regulation. Cecilia Kang and Sheera Frenkel, *Facebook's Zuckerberg Said to Agree to Testify Before Congress Over Data Privacy*, N.Y. TIMES (Mar. 27, 2018), https://www.nytimes.com/2018/03/27/technology/facebooks-zuckerberg-said-to-agree-to-testify-before-congress-over-data-privacy.html (last visited Mar. 28, 2018); Julia Carrie Wong abd Sabrina Siddiqui, Mark Zuckerberg agrees to testify before Congress over data scandal, The Guardian (Mar. 27, 2018 5:51 PM), https://www.theguardian.com/technology/2018/mar/27/mark-zuckerberg-testify-congress-cambridge-analytica-data-scandal (last visited Mar. 28, 2018); *Apple's Tim Cook Calls for More Regulations on Data Privacy*, BLOOMBERG NEWS (Mar. 24, 2018 12:08 AM), https://www.bloomberg.com/news/articles/2018-03-24/apple-s-tim-cook-calls-for-more-regulations-on-data-privacy (last visited Mar. 28, 2018).