# Principles for Privacy Legislation:

## Putting People Back in Control of Their Information

Harold Feld

December 2017

Public Knowledge

# Table of Contents

# INTRODUCTION

On September 7, the credit reporting firm Equifax announced that it had suffered a security breach exposing the financial information of nearly 145 million Americans to unknown hackers.[1] Since then, Equifax has provided a steady stream of examples of everything wrong with our current haphazard digital privacy protection regime. It took Equifax over a month from discovery of the breach to announce the breach, during which time several executives sold off stock.[2] Equifax initially required consumers trying to determine if their information was compromised to waive their right to sue or participate in a class action.[3] In line with previous statements by its then-CEO that "fraud is a huge opportunity for us,"[4] Equifax initially charged those impacted standard fees to freeze their credit reports – until public backlash forced them to drop their fees.[5] Further investigation revealed that Equifax had suffered a major breach in March 2017 that it had never publicly reported.[6]

Unsurprisingly, the Equifax breach has placed personal control over digital information in the public policy spotlight. As of this writing, 10 bills have been introduced in Congress to address various aspects of the Equifax breach.[7] But even before the Equifax breach, consumer concerns about their inability to control – or even discover – who has access to their personal information had become a substantial consumer concern and source of considerable activism. As chronicled in

---

[1] *See* Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information*, (Sept. 07, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[2] *See* Michael Hiltzik, *Here Are All the Ways the Equifax Data Breach Is Worse Than You Can Imagine*, Los Angeles Times (Sept. 8, 2017), http://beta.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html.

[3] *See* David Kravetz, *Are You an Equifax Victim? You Could Give Up Your Right to Sue to Find Out*, Arstechnica (Sept. 8, 2017), https://arstechnica.com/tech-policy/2017/09/are-you-an-equifax-breach-victim-you-must-give-up-right-to-sue-to-find-out/

[4] *See* Jen Wieczner, *How Equifax Is 'Making Millions of Dollars Off Its Own Screwup'*, Fortune (Oct. 4, 2017), http://fortune.com/2017/10/04/equifax-breach-elizabeth-warren/.

[5] *See* Ron Lieber, *Equifax, Bowing to Public Pressure, Drops Credit-Freeze Fees*, New York Times (Sept. 12, 2017), https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html?mcubz=1;
Katie Lobosco, *Equifax Will Offer You Free Credit Locks. Here's What That Means for You*, CNN (Sept. 28, 2017), http://money.cnn.com/2017/09/28/pf/equifax-credit-lock/index.html.

[6] *See* Michael Riley, Anita Sharpe & Jordan Robertson, Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed, Bloomberg (Sept. 18,2017), https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed.

[7] *See* Data Broker Accountability and Transparency Act of 2017, S. 1815, 115th Cong. (2017); H.R. 3816, 115th Cong. (2017); Data Breach Accountability and Enforcement Act of 2017, S. 1900, 115th Cong. (2017); Data Protection Act of 2017, H.R. 3904, 115th Cong. (2017); Cyber Breach Notification Act of 2017, H.R. 3975, 115th Cong. (2017); Consumer Privacy Protection Act of 2017, H.R. 4081 115th Cong. (2017); Consumer Privacy Protection Act of 2017, S__, 115th Cong. (2017).

the Washington Post, lobbyists for the technology/"edge provider" industry and lobbyists for the cable and telephone industry engineered one of the most comprehensive rollbacks of consumer privacy protection.[8] On April 3, President Trump signed the Congressional Resolution of Disapproval repealing the Federal Communication Commission's (FCC's) broadband privacy rules.[9] The one silver lining from this profoundly anti-consumer action has been to dispel once and for all the persistent myth that Americans "don't care about their privacy." To the contrary, as the May 2017 Harvard-Harris Poll confirmed, 9 out of 10 Americans are "uncomfortable" with the extent companies can access their personal information.[10] This backlash has prompted both the introduction of legislation at the state level and the federal level to address the gap in privacy protection created by the resolution of disapproval.[11]

Finally, while Public Knowledge focuses primarily on the harm to consumers from the essentially unregulated market for personal information and the lack of national standards for breach liability or breach notification, it is important to recognize the enormous economic cost as well. As reported by the National Telecommunications Information Administration in 2016, lack of trust in internet privacy and security deters consumers from engaging in certain electronic transactions or other e-commerce activities.[12] Identity theft, made possible from stolen information following a data breach, cost consumers $16 billion in 2016, with billions of dollars in costs passed on to banks and other financial institutions.[13] Creating strong federal protections for consumer privacy minimizes the risk of identity theft by both limiting the availability of personal financial information and requiring companies to provide adequate protection for the information they store.

---

[8] *See* Kimberly Kind, *How Congress Dismantled Federal Internet Privacy Rules*, Washington Post (May 30, 2017), https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html?utm_term=.22f9c160de89.

[9] Brian Fung, *Trump Has Signed Repeal of FCC Privacy Rules*, *Here's What Happens Next*, The Washington Post (Apr. 4, 2017) https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/?utm_term=.5cf315ee54c4.

[10] *See* Harris Insights & Analytics & Harvard Center for Political Studies, *Harvard-Harris Poll May 2017* (2017), *available at* http://media.theharrispoll.com/documents/Harvard-Harris-Poll_May-Wave_05.26.2017_Final.pdf.

[11] *See, e.g.,* American Civil Liberties Union, *Status of Internet Privacy Legislation* (2017), https://www.aclu.org/issues/privacy-technology/internet-privacy/status-internet-privacy-legislation-state; National Conference of State Legislatures, *Privacy Legislation Related to Internet Service Providers*, National Conference of State Legislatures (Aug. 4, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx.

[12] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security may Deter Economic and Other Online Activities*, National Telecommunications & Information Administration (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[13] Kelli B. Grant, *Identity Theft, Fraud Cost Consumers More Than $16 Billion*, CNBC (Feb. 1, 2017), https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

Rather than endorse any specific bill or one-size-fits-all approach, this Public Knowledge working paper outlines the principles we believe Congress should adhere to when considering how to provide privacy and information security to all Americans.

1. ***Americans deserve the right to own and control their personal information***. Those who collect and store this personal information have a duty to protect it. When a breach of this trust occurs, the party that failed to properly secure the information should make the individual whole to the greatest extent possible. As discussed below, personal ownership and control of one's personal information was the basis for privacy law in the United States until the deployment of computers and computer networks and the rise of data processing. Since then, the law in the United States has drifted further and further away from this traditional approach to increasingly privilege data aggregators at the expense of individuals. It is time to reverse this trend and move back toward the traditional American approach of individual ownership and control.

2. ***Context matters***. We all willingly trade information every day, but the circumstances of these decisions vary widely. Where an individual cannot avoid sharing information without forgoing critical services, the law must recognize a greater obligation to protect the information. Likewise, when the information is particularly sensitive, the law should recognize this fact.

3. ***Americans need more privacy protection, not more federal preemption***. Industry lobbyists have long sought to include federal preemption of state privacy and data breach laws as part of any new federal legislation. While the federal government should set minimum standards of protection for all Americans, over 100 years of shared responsibility between the states and the federal government for protecting consumers demonstrates the value of having multiple "cops on the beat." Additionally, states have been in the vanguard of privacy protection and breach notification laws, allowing policymakers to assess which protections work and which don't. To the extent federal preemption is necessary to create a manageable national framework, it should be narrowly tailored to meet specific concerns.

4. ***Backward compatibility with existing federal privacy and data breach protections.*** The United States has relatively few federal statutes that directly impose privacy protections on industries. But while few in number, these laws form the basis for consumer privacy protection in critical industries such as health,[14] communications,[15] and financial protection.[16] New federal protections for consumers should be "backward compatible" with existing protections. Congress should reject efforts by industry lobbyists to eliminate specific privacy protections tailored to their industry. Nor should Congress delay providing needed protections while seeking to draft a perfect,

---

[14] Health Insurance Portability and Accountability Act of 1997, 104-191. *See also HIPAA Privacy Rule*, U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[15] *See* Communications Act of 1934, as amended, §§ 222, 338(i), 631.

[16] *See* Graham-Leech-Bliley Act, Pub. L. 105-257, 15 U.S.C. §§ 66501-05; http://files.consumerfinance.gov/f/201410_cfpb_final-rule_annual-privacy-notice.pdf.

all encompassing privacy law. If Congress can agree on positive steps that provide even incremental improvements in privacy protection, Congress should enact what it can with the understanding that this is only an incremental step rather than a complete solution. Given the enormous breadth and complexity of the problem, Congress should expect to pass several laws designed to work together rather than spend years trying to draft the perfect law.

# Part I. The Lesson of Equifax: Consumers Cannot Protect Themselves Without Clear, Enforceable Rights

The debate over privacy and data breach notification has gone on for some years. Opponents of strong federal regulation have generally made the following arguments. First, consumers voluntarily trade their information in exchange for goods and services. If they do not wish to share their personal information, they can avoid doing so. Second, companies have all the incentive they need to handle information with caution, rather than risk punishment in the marketplace. Third, existing laws provide more than adequate protection for consumers in the event of a breach. The Equifax breach demonstrates exactly why each one of these arguments is wrong – and why the private sector cannot be trusted to respond properly without a federal law with real enforcement teeth.

## A. The Market Does Not Allow Consumers to Avoid Sharing Personal Information, or to Punish Firms That Fail to Adequately Protect Their Information

Most of the impacted consumers never had direct dealings with Equifax. Equifax's customers are banks, employers, landlords, and anyone else doing a credit check on an individual for any reason. A person does not have the option to tell a mortgage broker: "I don't trust Equifax. They had a huge data breach. Use another credit reporting agency instead." Nor can individuals control how these companies collect or store their personal information. As others have noted, the vast majority of people whose highly sensitive personal information was compromised had never heard of Equifax – let alone know that Equifax stored their social security numbers in a vulnerable database. Even people who never go online, never use social media and never make online purchases had their personal data compromised. When even the most necessary activities of daily life, such as renting a place to live, can trigger a credit check and produce digital records of your personal information, the argument that consumers could somehow avoid creating digital records of their information is ludicrous.

## B. When a Breach Occurs, Companies Have Incentive to Protect Themselves at the Expense of Consumers

Additionally, the Equifax breach demonstrates the inadequacy of relying on incentives or on existing laws. Equifax certainly did not find the incentives adequate. To the contrary, Equifax's incentives ran in the direction of protecting themselves, and even profiting themselves, rather than protecting consumers or providing any real remedy for the breach. Equifax had every financial incentive to hide news of the breach for as long as possible, allowing whoever unlawfully accessed the information to exploit it without fear that impacted individuals would even be aware of the

danger. Equifax executives realized personal profit from selling stock before the announcement of the breach. Equifax initially forced consumers to waive their rights as a condition of even discovering whether or not they were harmed, and then charged them to protect themselves from Equifax's negligence. While public outrage may have forced Equifax to backtrack, nothing stops other firms in less high profile cases from doing the same thing.

Finally, it is not clear that Equifax will suffer any serious harm in the long term. Indeed, Equifax received a contract with the IRS shortly after the breach occurred.[17] As one of only three credit reporting companies in the United States, Equifax will likely suffer little loss of business even in the short term for the simple reason that businesses relying on Equifax have no incentive to stop using it. Those harmed, i.e. the majority of the adult population of the United States, do not have any means to "vote with their pocketbooks" or employ any other market correcting mechanism. Equifax has suffered some loss in its stock value, but that will likely reverse itself over time in the absence of any serious consequences to Equifax.

## C. Existing Laws Are Poorly Designed to Protect Consumers in the Digital Age

Nor is it clear that any of Equifax's conduct violated existing law, or created any civil liability. Although investigations remain ongoing at this time, it is unclear that the existing laws covering credit reporting agencies, or covering the collection and storage of personal information, apply to the circumstances of the Equifax breach.[18] Several state Attorneys General have sued, as have some class action plaintiffs. But these lawsuit face numerous hurdles, years of litigation, and traditionally result in low-cost settlements.[19]

That leaves the Federal Trade Commission (FTC). Although hailed as the "expert agency" on protecting digital privacy, the FTC has no specific statutory authority covering data breaches or consumer privacy generally.[20] Nor does the FTC have the power to issue regulations to prohibit

---

[17] *See* Steven Overly, *IRS Temporarily Suspends Contract With Equifax*, Politico (Oct. 12, 2017), https://www.politico.com/story/2017/10/12/irs-equifax-contract-suspended-243732 (The IRS has since suspended the contract. Review remains pending at the time of this writing.)

[18] *See* Anna Bahney, *Will Equifax be held accountable?*, CNN Money (Sept. 15, 2017), http://money.cnn.com/2017/09/15/pf/equifax-lawsuits/index.html; Peter J. Henning, *Hack Will lead to Little, if Any, Punishment for Equifax*, N.Y. Times (Sept. 20, 2017), https://www.nytimes.com/2017/09/20/business/equifax-hack-penalties.html?_r=0; Stacy Cowley, *Equifax Breach Prompts Scrutiny, But New Rules May Not Follow*, N.Y. Times (Sept. 15, 2017), https://www.nytimes.com/2017/09/15/business/equifax-data-breach-regulation.html

[19] *See* Max Kenerly, *Equifax and The Long Legal Road in Data Breach Class Actions*, Litigation and Trial (Sept. 15,2017), http://www.litigationandtrial.com/2017/09/articles/attorney/equifax-data-breach-class-actions/

[20] The FTC has limited authority under the Child Online Privacy Protection Act (COPPA) to issue regulations with regard to websites and online services targeting children below the age of 13. *See* 16 C.F.R. 312. It also has certain limited authority with regard to some financial institutions under the Graham-Leach-Bliley Act. *See* Pub. L. 106–102.

future breaches. The FTC's general consumer protection statute[21] generally limits the FTC's enforcement power to consumer services, rather than to businesses like credit reporting agencies that provide service to other businesses. In addition, the FTC must show that consumers have suffered actual harm from the data breach, or that the data breach creates a "substantial risk" of harm. Courts have held that, absent a specific statute providing for damages, the mere fact of a data breach does not give rise to an actionable injury. The Federal Trade Commission Act explicitly prohibits the FTC from using public policy considerations "as a primary basis" for finding an act or business practice "unfair" to consumers.[22]

In short, absent Congressional action, Americans have limited rights to control, or even reliably protect, their personal information. State law provides the bulwark of protection in the absence of national standards – with some notable subject area exceptions such as health and telecommunications. Americans who live in states without strong data breach laws do not even have the right to know who *has* their personal information, let alone the right to know when those storing their personal information have suffered a data breach that places them at risk.

---

Neither appears to apply to Equifax, although investigation remains pending at the time of this writing. *See* David McLaughlin & Todd Shields, *FTC Opens Investigations Into Equifax Breach*, Bloomberg (Sept. 14, 2017), *https://www.bloomberg.com/news/articles/2017-09-14/equifax-scrutiny-widens-as-ftc-opens-investigation-into-breach*.

[21] FTC Unfair Methods of Competition Unlawful; Prevention by Commission, 15 U.S.C. § 45 (2012).

[22] *Id.* at § 5(n).

## Part II: Equifax Is Not Unique

Credit agencies are hardly the only collector of private information. Increasingly, consumers find themselves under surveillance from their cars[23], their television sets,[24] and even their sex toys.[25] An entire industry of data brokers exists, collecting information on individuals without their knowledge or permission and reselling that information to whoever wants it.

To make it even more difficult for a person trying to avoid revealing personal information, it has become for all practical purposes almost impossible to avoid. Consider, as an example, the consumer trying to avoid revealing personal information to Google because she does not like their information practices. Most people understand that Google owns its search engine and YouTube. But it is utterly unrealistic to expect everyone to research what companies Google's parent company Alphabet owns (assuming the average consumer is even aware that Google's parent holding company is Alphabet). After avoiding the Chrome browser and any mobile phone using the Android operating system, she must then research the ownership of every application she might wish to download. She must check at work to see if her employer uses Google as their email provider, and quit her job to avoid opening a Google account. If her child has a homework assignment to watch a video on YouTube, she must take him to the library to avoid accessing it through her home network on a device she owns. She must constantly purge her browser and any other device of cookies and other tracking software, lest Google have a sharing arrangement with a company she has electronically touched.

But even after all that, even after devoting her every free minute to avoiding Google, her efforts are likely in vain. Some friend – or even stranger – may have uploaded her picture to a Google Group. She may send email to someone who has a Gmail account. The advertisements served to her on other websites may report back information of any digital impression. And, if all else fails, Google can supplement any information it wants by going to a data broker – a business that specializes in collecting personal information from a variety of available sources.[26]

It is important to recognize that there is nothing nefarious in the operations of Google, Facebook, and other online companies that collect information. To the contrary, it is entirely predictable – and, from the perspective of for-profit enterprises, even appropriate – to expand their

---

[23] *See* Sen. Edward J. Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* (Feb. 2015), available at: https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[24] James K. Wilcox & Glen Derene, *How to Turn Off Smart TV Snooping Features*, Consumer Reports (Feb. 8, 2017), https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/.

[25] Luke Darby, *A Sex Toy App Is Recording Orgasm Data Without Users Knowing It*, GQ (Nov. 11, 2017), https://www.gq.com/story/sex-toy-record-user.

[26] *See* Federal Trade Commission, *Data Brokers, A Call for Transparency* (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

ability to collect information and target advertisements to the limit permissible by law and technology. It is the job of public policy to set appropriate limits, and ensure that the conduct of these companies is not contrary to the public interest. As long as Congress insists on relying on "self-regulation," rather than taking steps to provide consumers with enforceable rights, we should expect companies that rely on collecting personal information for revenue to continue to improve and expand on their information collecting capabilities.

Nor are large digital platforms like Google, Facebook, or Amazon the only companies with such a vast reach. Thanks to the repeal of the FCC's privacy regulations, whatever company you use to access the internet can follow you wherever you go. Comcast, AT&T, and other Internet Service Providers (ISPs) have built their own advertising networks that pull together all information on your internet habits and on what devices access your network and when. It can combine this information with your television watching habits and data from other internet enabled devices that access the internet through your home network. Even without reading the content, your ISP can use this information to build a disturbingly thorough picture of your daily habits and routine.[27]

Finally, even the companies themselves do not necessarily know who else can access their information, or for what purpose. A recent study from researchers at the University of Washington found that for a mere $1000, any person could use any of the existing mobile advertising platforms to track you through your mobile phone without your knowledge.[28] As the study's authors warn:

> *Regular people*, not just impersonal, commercially motivated merchants or advertising networks, can exploit the online advertising ecosystem to extract private information about other people, such as people that they know or that live nearby. (Emphasis in original)[29]

---

[27] *See, e.g.,* Jeffrey Chester, *Big Data Is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers*, Center for Digital Democracy (Mar. 23, 2016), https://www.democraticmedia.org/article/big-data-watching-growing-digital-data-surveillance-consumers-isps-and-other-leading-video.

[28] *See ADINT: Using Targeted Advertising for Personal Surveillance*, Paul G. Allen Sch. of Computer Sci & Engineering, U. Wash., https://adint.cs.washington.edu/; Andy Greenberg, *It Takes Just $1,000 to Track Someone's Location with Mobile Ads*, Wired (Oct. 18, 2017), https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/?mbid=nl_101817_daily_list1_p1.

[29] For elected officials in particular, this should sound alarm bells. After the repeal of the FCC privacy regulations, angry protesters tried to buy browser information for members of Congress. At the moment, ISPs do not sell individualized information except to law enforcement. *See* Kate Cox, *AT&T Makes Money Mining, Selling Phone Use Data to Police Nationwide*, Consumerist (Nov. 1, 2016), https://consumerist.com/2016/10/25/att-makes-money-mining-selling-phone-use-data-to-police-nationwide/. But that step now seems unnecessary. One thousand dollars is a trivial line item in the tens of millions of dollars spent every election cycle on opposition research – and we can expect the price to drop as services designed to take advantage of this access enter the market. If lawmakers are unmoved by the risk of stalking to their constituents, perhaps the concern that some future enterprising reporter or political opponent can track their every move will persuade them of the need for action. *See* Jay Stanley, *When Privacy Gets Personal for Policymakers*, American

To conclude, every happy assumption that opponents of enhancing privacy continue to ask us to believe – that we can somehow avoid revealing our private information if we try, that there is no real danger in having all the details of our lives from our social security numbers to our browsing habits all compiled in one place, and that the only people who could possibly wish to access this information are "impersonal, commercially motivated merchants" eager to sell us innovative products and thus motivated to protect our private information that they store – is demonstrably false to fact. The Equifax breach is simply the dramatic event that has finally caught the attention of the public and lawmakers and demonstrated why the current law is dangerously inadequate.

---

Civil Liberties Union (Sept. 19, 2012), https://www.aclu.org/blog/national-security/when-privacy-gets-personal-policymakers?redirect=blog/technology-and-liberty/when-privacy-gets-personal-policymakers.

# Part III. Four Basic Principles for Designing Real Privacy Protection

We must begin by acknowledging that an issue so broad and complicated as privacy in the digital age cannot be solved by adopting a single law or quick fix. The entire internet economy has evolved to depend heavily on advertising, which at the moment increasingly relies on targeted advertising based on collection of personal information. Certain types of information collection and storage are unavoidable, or may have positive effects. Additionally, there are strong differences of opinion among privacy advocates over how best to achieve the goal of protecting what the late Justice Louis Brandeis referred to as "the fundamental right to be let alone," while respecting the right of people who do want online services to learn their preferences and exclude irrelevant or offensive advertisements or search results.

We should therefore expect that Congress should move swiftly to correct immediate and blatant abuses, but will continue to revisit this issue over time to make incremental improvements. Likewise, we should expect that multiple agencies charged with protecting privacy in a variety of specialized sectors will need to continue to revisit their decisions from time to time as technology evolves and as the regulatory environment changes.

## A. The History of American Privacy Law Provides the Appropriate Framework for Future Privacy Regulation

Accordingly, rather than try to present a particular legislative approach, this working paper provides four basic principles we believe should guide legislators and regulators in developing appropriate privacy protections.

American privacy law formally begins with Justice Louis Brandeis' seminal 1890 article *The Right To Privacy*.[30] As described by Brandeis, the right of privacy is a further evolution of property rights prompted by changes in technology. The initial natural rights of John Locke and contained in the common law and the U.S. Constitution, "life, liberty, and property," evolved over time to extend from simple protection of the physical person ("thou shalt not kill") to then include protection of physical property, and then to include protection of intangibles such as reputation or trade secrets. In light of the rise of new surveillance technologies (specifically, the portable camera) and new information distribution platforms (specifically, the rise of the tabloid press), "the next step which must be taken for securing . . . the right to be let alone." This required moving away from a requirement to show some actual harm (as required by slander and libel laws), but a recognition that the harm arises from the act of appropriating the details of one's personal life and exposing them to the world. This, Brandies proposed, is "the right of property in the widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate

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

personality, affords alone that broad basis upon which the protection of the individual demands can be rested. [...]These rights, therefore, are not arising from contract or from special trust, but are rights against the world."

For more than half a century, American privacy law followed this concept of protecting privacy as an exercise of the "right to an inviolate personality." This included various state and common law "rights of publicity."[31] It also provided a general guide for "sector specific" statutory laws. For example, the Federal Radio Act of 1927 prohibited any provider of any form of communication, by wire or radio, from disclosing any information with regard to a transmission from one person to another – including the fact of transmission.[32]

[31] *See, e.g., Zachinni v. Scripps-Howard Broadcasting Co.*, 433 U.S. 562 (1977).
[32] Radio Act of 1927, Section 27 (codified at 47 U.S.C. § 605(a)).

## B. The Introduction of Database Computing Shifts Personal Ownership to "Mutuality"

In the 1960s, the rise of computing power, and the ability to connect computers via telecommunications networks gave rise to the new field of data processing and prompted a new investigation into the concept of privacy and the need for federal legislation to protect individual privacy. This inquiry produced the landmark report, "Records, Computers, and the Rights of Citizens," published by the Housing, Education, and Welfare Department – generally known as the *HEW Report*.[33] The *HEW Report* recognized that the rapid growth of information processing technology promised enormous benefits to society as a whole, but also threatened to virtually eliminate the ability of people to ascertain who had access to their personal information, and for what purposes. While recognizing the traditional American approach to privacy as providing personal control over information, the authors of the *HEW Report* found that approach unworkable in the digital age.[34] In particular, the *HEW Report* found that modern record creation and data processing "usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals."[35]

The *HEW Report* therefore proposed "a redefinition of the concept of privacy based on the idea of "*mutuality*." Rather than retaining ultimate ownership of the information with the individual, the individual would retain "a right to participate meaningfully" in what information became part of a record about the individual, and rules governing the use and storage of personal information. This recognized the interest of the individual; the interest of the institution creating the record; and the broader interest of the public in ensuring certain types of data processing necessary for statistical research, public health and safety, or the smooth functioning of technology necessary to modern society.[36]

To provide guidance, the *HEW Report* formulated the Fair Information Practice Principles (FIPPs):

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for individuals to find out what information about them is in a record and how it is used.
3. There must be a way for individuals to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of identifiable information about them.

---

[33] U.S. Department of Health, Education, and Welfare, *Records Computers and the Rights of Citizens* (July, 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
[34] *Id. at* 38-40.
[35] *Id.*
[36] *Id.* at 40-41.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Since publication of the *HEW Report*, the FIPPs have become extremely influential in the development of privacy law both in the United States and internationally. Nevertheless, despite the overall influence of the *HEW Report* and the FIPPs, the United States declined to adopt privacy legislation broadly applicable to commercial data collection and data storage.[37]

## C. Competition Policy as Further Influence on Privacy

Of equal importance to the development of modern, sector-specific privacy regulation has been the promotion of competition for services provided (or potentially provided) by an entity that controls the relevant records.[38] In these cases, the principle of "mutuality" yields back to the basic principle of individual ownership of the consumer's own information. Statutes designed to promote competition generally include provisions requiring the entity holding the information to disclose that information to a third party when so directed by a consumer.

The Health Insurance Portability and Accountability Act of 1996,[39] as modified by the American Recovery and Reinvestment Act of 2009,[40] imposes obligations to protect "protected health information," to make the information available to the patient, and to disclose the information to a competing provider when required by the patient.[41] Similar provisions requiring service providers to not only protect personal or "proprietary" information, but to disclose it to third parties at the direction of individual, can be found in the Cable Privacy Act of 1984,[42] and the Telecommunications Act of 1996.[43]

---

[37] The Privacy Act of 1974, Pub. L. 93-579 (codified at 5 U.S.C. § 552(a)) (adopted fair information practice principles for data on individuals collected and stored by federal agencies. While influenced by the *HEW Report*, the Privacy Act did not apply any fair information practice principles to commercial data collection or storage. As discussed in the following section, the FTC has promoted a version of the FIPPs as a voluntary best practices, but lacks authority to require FIPPs compliance as a matter of law.)

[38] *See, e.g.,* Harold Feld et al., *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Privacy Rules for the Digital World*, Public Knowledge (Feb. 16, 2016), available at https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper (describing competitive concerns with regard to formulation and final enactment of Section 222 of the Communications Act).

[39] *See* Pub. L. 104-191.

[40] *See* Pub. L. 104-191.

[41] *See generally supra* note 14.

[42] *See* Pub. L. 98-549 (codified at 47 U.S.C. § 551).

[43] *See* Pub. L. 104-104 (codified at 47 U.S.C. § 222).

## D. The Failure of Public Policy to Respond Adequately to the Rise of the Internet

It is important to understand that while consumer control of one's personal information is central to both common law and "sector-specific" privacy law in the United States, the FTC has taken a different approach. The FTC treats the information as belonging to the service provider or merchant, and then limits the use of the information by applying principles of contract law through the publication of a "privacy statement" or "privacy policy." This approach came not from a deliberate decision to abandon the traditional American reliance on consumer control of information, but as a combination of statutory limitation and accident of history. As the age of internet commerce and the digital economy began in the 1990s, the United States had no general privacy law or federal agency to address the growing concern over the future of privacy. The Federal Trade Commission, as the general consumer protection agency for the United States, responded by interpreting its existing statute to include protecting consumers from harms associated with the digital collection and storage of information.

This was entirely appropriate and necessary. Had the FTC waited for express Congressional authority, consumers would have been completely unprotected. But the FTC's general consumer protection statute, Section 5 of the Federal Trade Commission Act (FTCA), was designed for an industrial age. It assumes willing buyers and willing sellers, where the chief danger to consumers lies in fraudulent goods and deceptive contacts for services. The FTC does not have general rulemaking power, and must proceed through enforcement cases in which it bears the burden of persuasion that the challenged conduct meets the definition of "unfair or deceptive" trade conduct or practices.

In 1994, just as questions surrounding privacy in the digital age were beginning to be debated, Congress further amended Section 5 of the FTCA to limit the FTC's authority to find a practice "unfair or deceptive,"[44] requiring that the conduct must cause, or be likely to cause, "substantial harm" to consumers. Section 5(n) further requires that consumers can not "reasonably avoid the harm." Even if the FTC finds that the conduct meets these criteria, it must further prove that this "substantial harm" is not "outweighed by countervailing benefits to consumers or to competition." Finally, while Section 5(n) permits the FTC to consider "established public policies" when determining whether a practice is unfair, "[s]uch public policy considerations may not serve as a primary basis for such determination."

In other words, at precisely the moment when the FTC was required by circumstances to step up and formulate the appropriate policy for digital privacy, Congress instructed the FTC to (a) balance any harms to consumers against the burden on businesses that might deter "competition;" and (b) expressly prohibited the agency from using public policy considerations as its primary basis for decision making. This not only prohibited the FTC from even considering the traditional

[44] Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, a*vailable at* https://www.gpo.gov/fdsys/pkg/STATUTE-108/pdf/STATUTE-108-Pg1691.pdf#page=1

American approach of protecting privacy by investing control in the individual: It explicitly required the FTC to make the right of privacy both subject to contract and required a showing of material harm beyond the publication of the information – precisely the opposite of the American tradition since Brandeis.

The FTC itself recognized the limits on its authority from the beginning, and has therefore focused on voluntary frameworks. In the FTC's 1998 report to Congress, the FTC found that most industry codes of conduct for collection and storage of consumer information failed to comply with the basic FIPPs framework, primarily in the failure to promote appropriate safeguards from unauthorized access.[45] A survey of commercial websites at the time found that while approximately 84% of websites collected personal data from visitors, only 14% provided notice.[46] While acknowledging that this represented a failure of self-regulation, the agency also acknowledged that it would require Congressional action to provide "greater incentives" for commercial providers to protect personal privacy. Similarly, in the FTC's 2012 Report recommending a "Privacy Framework" and "best practices,"[47] the agency stressed that its recommendations were voluntary, not mandatory.[48] On numerous occasions, the FTC has urged Congress to augment its authority to protect privacy and require data breach notification -- including provision of rulemaking authority.[49]

Congress did provide the FTC with both direct statutory authority and privacy in two specific cases. In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA).[50] COPPA provides the FTC with narrow rulemaking authority to govern privacy practices for

---

[45] *See generally* Federal Trade Commission, *Privacy Online: A Report to Congress*, (June 1998), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[46] *Id.*

[47] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[48] *Id. Cf.* Dissenting Statement of Commissioner Rosch (expressing concern that industry would interpret voluntary code of conduct as mandatory).

[49] *See, e.g.,*Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (requesting Congressional authorization to address data brokers and privacy via rulemaking); Federal Trade Commission, *Prepared Statement of the Federal Trade Commission on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime* (Feb. 4, 2014), https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-digital-age-preventing-data-breaches-combating/140204datasecuritycybercrime.pdf at 11-12 (requesting rulemaking authority to address security and data breach notification); Federal Trade Commission, *Prepared Statement of the Federal Trade Commission on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime* (Mar. 26, 2014).

[50] See Pub. L. 105-257 (Codified at 15 U.S.C. §§ 6501-05).

websites that explicitly target children under the age of 13.[51] Under the Gramm Leach Bliley Act of 1999[52] (GLBA), the FTC has statutory authority to enforce the financial privacy provisions of the GLBA. These provisions require disclosure by the financial institution of the information collected, the purpose for which it is collected, with whom the information is shared, and how the collected information is protected. The institution must also inform the consumer of the right to opt out of sharing information with unaffiliated parties under the Fair Credit Reporting Act. Congress imposed significant limits on these statutory grants of authority, further hobbling the ability of the FTC to to address changes in technology and business practices since the late 1990s.

For more than 20 years, the FTC has valiantly struggled to protect consumer privacy with the tools available to it.[53] But the time has come to remove the artificial shackles on the FTC and American privacy law and return to the traditional American approach of protecting the "fundamental right to be let alone" by providing consumers the right to control the use and distribution of their personal information. While these principles are consistent with the FIPPs, the principle of mutuality central to the FIPPs should not displace the principle of individual control of personal information (including the pro-competitive principle of information portability to rival service providers), except where either necessary to provide the service or otherwise necessary to the public interest. We therefore propose these four basic principles to transition American privacy law from the current a-historic and inadequate framework to one consistent with robust protection and the traditions of American statutory and common law.

---

[51] *See* 16 C.F.R. Part 312.

[52] *See* Pub. L. 106-102 (codified in relevant part at 15 U.S.C. §§ 6801-09).

[53] *See, e.g.,* Edith Ramirez et al., *Data Broker Report*, Federal Trade Commission (May 2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (requesting Congress pass enact legislation to govern data brokers); Federal Trade Commission, *Prepared Statement of the Federal Trade Commission on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime before the Committee on the Judiciary, Federal Trade Commission* (Feb. 4, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-digital-age-preventing-data-breaches-combating/140204datasecuritycybercrime.pdf (asking Congress to provide authority for the FTC to address data breeches and impose notice requirements).

### *Principle 1: Recognize the basic principle that Americans have a fundamental right to control their personal information, and to expect that third parties will provide adequate protection for personal information*

No one can participate in modern society without generating a vast footprint of personal information. The law must recognize that no one can voluntarily avoid providing to third parties information that, when combined and analyzed, reveals far more about each of us as an individual than we feel comfortable exposing to the world. Consumers should not need to choose between living in 21st century society and keeping private the basic facts about their personal lives and habits.

Digital privacy law developed in the 1990s under the assumption that consumers could easily avoid digital markets or digital devices and could continue to live comfortably in an analog world as the price of keeping their privacy. Even then, that premise was highly questionable. Now, it is intolerable. We cannot on the one hand say that broadband is an essential service for all Americans, that our children must use electronic textbooks, that our President and public officials will communicate with the public through social media, and still pretend that participation in the digital world is "voluntary" and therefore we must give up our privacy to participate in our digital society.

Future legislation should, in the tradition of Justice Brandeis and American common law privacy law, make clear that information collected by companies online belongs to the individual. When an individual does business with another entity, she has a right to expect that the business will respect and protect this information in the same way that any business has an obligation to respect and protect property of another entrusted into its care. Congress should make clear that failure to take appropriate precautions constitutes negligence, subject to liquidated damages. Only by imposing the traditional common law, and statutory remedy[54] of liquidated damages, can Congress ensure that companies have the incentive to take adequate precautions to protect user data. Equifax may have been the victim of an illegal attack, but it was also negligent in failing to install a necessary security patch that would have prevented the data breach.

Liability, for liquidated damages where actual damages may provide insufficient incentive to take adequate precautions, is the tried and true market mechanism for aligning the incentives of private actors with the public interest. Congress should not hesitate to employ it here.

[54] *See supra* note 42.

Additionally, as with negligent damage to real property, companies that mishandle personal data have a responsibility to notify affected users and do what is possible to make them whole. Equifax has demonstrated that, despite state breach notice laws, companies will not only act to conceal news of a breach as long as possible, but will try to leverage the breach for their own gain. Individuals informed that their personal data is at risk should not be required to waive their rights or pay fees simply to verify whether or not they are at risk. Nor should they be required to pay for the negligence of another – especially if they never gave permission for that company to have the information in the first place.

This approach has several salutary improvements over the existing FTC regime (assuming the FTC regime is applicable). First and foremost, imposing liability will encourage companies to minimize their collection and retention of personal information to only what they need. Increasingly, manufacturers of "smart" products that consumers have no expectation will record their personal information use available technology to gather and store as much personal information as they can.[55] Oftentimes these companies have no explicit plans for the information, but simply collect it because they can and because it might be valuable. Imposing liability for creating (and failing to secure) vast collections of personal information will discourage this sort of casual corporate spying.

Second, giving consumers control of their personal information has had pro-competitive effects. In those areas where Congress has provided consumers with the right to direct companies to detail the information in their possession, prohibit the company from sharing the information without consent, and allowing the consumer to direct that the company share the information with a third party *if directed by the consumer*, it has become possible for competitive providers to offer services.[56] While an ancillary rather than a primary concern, facilitating the development of competition is a public policy benefit that offsets the potential costs to businesses (and therefore customers) of compliance.

Finally, recognizing that the harm comes from the exposure of the information, not merely the sensitivity or type of information, enormously simplifies the existing FTC regime. The FTC's sensitive/non-sensitive dichotomy (a result of the need to find "substantial harm" and balance the potential harm against the potential cost to businesses) is increasingly arbitrary in a world where the aggregation of non-sensitive information allows a data collector to determine sensitive information, and has been subject to criticism for being both impractical and requiring collectors of information, rather than individuals, to determine what should constitute "sensitive" information.[57]

---

[55] *See supra* note 23.

[56] *See Generally supra* note 14, 43.

[57] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Ex Parte*, WC Dkt. No. 16-106 (Oct. 20, 2016), https://ecfsapi.fcc.gov/file/1021127642458/2016-10-20%20-%20FCC%20Privacy%20Ex%20Parte.pdf.

In restoring privacy law to its traditional frame, we should recall Brandeis' dictum that "if privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting."[58] Rather, just as trespass upon property is a violation even if the trespasser does no harm, just as any attack upon the person is assault even if the attacker leaves no bruises, the law should recognize that collection of personal information without permission is a violation of my right to privacy.[59]

### *Principle 2: Recognize that context and service matters*

Recognizing that a universal principle of privacy applies does not mean mindless mechanical refusal to recognize that context matters. While we should not depend upon the sensitivity of the information to dictate whether or not it is worthy of protection, the sensitivity of the information is certainly important in assessing damages, remedies, and precautions appropriate to the potential or actual harm. Privacy law has long recognized the difference between the sensitivity of information and the context in which a service is provided. For example, in the analog age, we allowed mail order catalog companies to keep track of the information from purchasers and sell that information to others, but we never permitted UPS or other delivery companies to track information about the packages or the individuals to whom they delivered these packages for any purpose other than to facilitate delivery and ensure proper billing. We allowed the mail order giants of the analog age such as Sears and Lands' End more freedom than we allowed to much smaller medical practices and financial advisers, because we recognized that context and sensitivity were more important for privacy than market share.

Similarly, any bill that addresses privacy in the digital age needs to recognize the differences between lines of business and services and ensure that application of the basic principles of privacy reflect these differences. Amazon, Facebook, and Google, with their massive information gathering and analysis, are utterly different from analog age businesses and require rules that reflect these differences. But they are also different from the carriers that deliver the information to and from consumers. Device manufacturers used to simply sell us television sets and telephones, and now they continue to monitor us in utterly unexpected ways.

Finally, as is recognized in existing sector-specific privacy laws, the right of privacy requires certain exceptions in order to function. This includes not merely the usual exceptions for life and safety, or for law enforcement (subject to due process). In the digital age, it is often necessary to provide personal information to a provider, and for that provider to share the information with third parties, for the service to work. Sometimes overriding public policy concerns require that individuals give up some control over their information. For example, for enhanced 911 geolocation to work, manufacturers must build the capacity into every phone. For smart grid to work

---

[58] *Brandeis supra* note 30.

[59] *Id*. at 205 (As Brandies further elaborated, however, that information which a person has already made public, or matters genuinely related to the public interest, or information of the kind that has always been available to the public, is not included in the right of privacy.).

effectively, we cannot allow individual homes to "opt out." Future driving safety systems, particularly for self-driving cars, may require that all cars share information with each to avoid accidents and maximize traffic efficiency. But just as past sector-specific regulations have recognized the need for exceptions, so too can generally applicable laws of privacy protection.

Federal privacy law should empower consumers to genuinely control their personal information. But the law must recognize that application of this overriding principle requires considerable flexibility and nuance, just as it did in the analog world.

### *Principle 3: First do not harm; Avoid preemption*

One would think it axiomatic that any genuine effort to protect personal privacy would not actually *reduce* privacy protections. But an astonishing number of "privacy" bills propose to do just that. For example, Rep. Marsha Blackburn's proposed replacement to the FCC privacy rules, which she eliminated by introducing a Congressional resolution of disapproval, would preempt the states, as well as eliminate the FCC's privacy jurisdiction over all communications, including traditional telephone and cable services.[60]

Concerns about personal information and privacy arise at every level of our daily lives. Our federal system relies not on a single, federal agency to protect consumer privacy, but on the combination of numerous state and federal laws that reflect the complex nature of protecting consumer privacy while enabling commerce and innovation. Certainly Congress needs to vastly expand the authority and resources available to the FTC to protect privacy. But the FTC cannot displace the states (or other federal agencies with complementary privacy jurisdiction) if Congress intends to provide adequate privacy protection to the American people.

Proposals to preempt state jurisdiction, while long sought by the same special interests responsible for eliminating the FCC's privacy rules, cannot seriously be considered a benefit to consumers. Even if Congress were to dramatically expand the resources available to federal privacy agencies – a proposal not even on the table – the federal government could not hope to provide adequate protection to consumers on its own. Congress has long recognized the vital role played by the states in consumer protection, both in terms of providing an additional "cop on the beat" and as leaders in consumer protection. No bill that purports to modernize privacy for the digital age should preempt the states from continuing to act in their necessary and traditional role as the first line of protection for consumers.

---

[60] *See* BROWSER Act of 2017, H.R. 2520, 115th Congress, https://www.congress.gov/bill/115th-congress/house-bill/2520

### *Principle 4: New federal laws must be compatible and complement existing federal privacy protections*

Similar to the principle above, Congress should resist lobbying by special interests to modify existing federal privacy protections. In particular, Congress should reject the long-standing efforts of the cable and telecommunications industries to repeal the highly successful and consumer friendly privacy rules governing cable and traditional telephone service. Again, any response to the current inadequacy of existing privacy law should not be used to do favors for special interests and reward industry lobbyists.

The existing sector-specific privacy laws in communications, healthcare, finance, and other business sectors are generally aligned with the principle of consumer control at the core of traditional American privacy law. They cover sectors of the economy that require individuals to have the highest degree of confidence in their ability to control the information. Health information and financial information, for example, are considered "sensitive" information under the FTC's existing privacy regime. Communications is not only often highly sensitive in its own right, but is also the means by which all other sensitive communications are communicated. A failure of privacy protection in communications compromises the privacy of all other information sent through the network.

Weakening or eliminating well-established federal privacy regulations where they do exist is a recipe for unintended consequences and uncertainty. As Congress works to provide Americans with the necessary privacy protections for the digital age, it should adopt a pragmatic, incremental approach rather than seek to "harmonize" all privacy law without regard to the differences in industry and consumer expectations.

## CONCLUSION

For far too long, Americans have seen their basic right to control their personal information erode away in the digital age. The Equifax data breach appears to have finally broken the paralysis that has gripped Congress on the question of digital privacy and data breach notification.