



**Regulatory
Transparency
Project**
Unlocking Innovation & Opportunity

When Considering Federal Privacy Legislation

Cyber & Privacy

Neil Chilson

The views expressed are those of the author in his personal capacity and not in his official/professional capacities.

To cite this paper: Neil Chilson, “When Considering Federal Privacy Legislation”, released by the Regulatory Transparency Project of the Federalist Society, December 4, 2018 (<https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper-Privacy-Legislation.pdf>).

4 December 2018

Table of Contents

Introduction	3
What is Information?	3-4
What is Privacy?	4-6
Tools to Protect Privacy	6-9
Criteria for Privacy Legislation	9-12
Conclusion	12

I. Introduction

Legislators, advocates, and business interests are proposing federal privacy legislation with new urgency.¹ The U.S. has a long-established federal framework for addressing commercial privacy concerns, including general consumer protection law and legislation for specific sectors, such as health care or financial services. But the calls to expand or replace this approach have grown louder since Europe's General Data Protection Regulation went into effect and since California adopted detailed and prescriptive privacy legislation.

So, do we need federal privacy legislation, and if so, what should it look like?

I believe three often-overlooked concepts can help us answer these questions. First, for practical reasons, no one can control all information about them. Second, all privacy laws are government-enforced restrictions on how one party can use information about another party. Third, over-restricting the use of information about individuals can harm individuals by limiting beneficial innovation.

Taking these concepts into account, I argue that we should prefer case-by-case enforcement frameworks where company practices are judged based on consumer outcomes. Such frameworks serve consumers better than do detailed legislation and prescriptive mandatory privacy practices. Outcome-based case-by-case enforcement approaches better resolve real consumer injuries while maintaining the information flows that ultimately benefit consumers.

In the following pages, I will first explain what information is and then define privacy as a combination of two different types of constraints on information: perception and use. I argue that privacy policy issues arise when advocates seek to impose use constraints where information faces weaker perception constraints. I then describe the different constraints available to protect online privacy and their strengths and weaknesses. Ultimately, I offer six recommendations for how the U.S. can address privacy concerns through government action while preserving the permissionless environment that has made the U.S. a leader in online innovation. In short, I argue that U.S. federal legislation should enhance the FTC's ability to address harmful unfair or deceptive uses of information about consumers.

II. What is Information?

Information, abstractly defined, is the content of a signal or signals that conveys something about the state of the world.² The signal could be light reflecting off an object, soundwaves coming off an

¹ See, e.g., Press Release, "Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy," <https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy>; Harper Neidig, "Advocates draw battle lines on national privacy law," <https://thehill.com/policy/technology/416341-advocates-draw-battle-lines-over-national-privacy-law>; Wendy Davis, "AT&T Calls For National Privacy Law," <https://www.mediapost.com/publications/article/327984/att-calls-for-national-privacy-law.html>.

² Claude E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*. 27 (3): 379–423 (1948).

object, light or electrons moving through a conduit, or any other change in the physical world that can be sensed. Signals can carry information enabling the receiver to determine something about the state of the transmitter.³

Information flows off us constantly and we cannot control all of it. As we interact with our environment, our interactions change the state of the world. These changes create signals that can often be observed, directly or indirectly, by others. We cannot halt or fully control this information flow unless we stop interacting with reality.⁴ In fact, actions to control information flows themselves generate information. To be able to fully control these flows would require godlike ability to control reality, including how others perceive it. If you somehow were able to eliminate the information flowing off you, you would quite literally disappear from the universe.

III. What is Privacy

Privacy is a complicated concept which many people have attempted to define, often in conflicting or incompatible ways.⁵ For the purposes of this paper, and building upon my definition of information, I define privacy as the result of a limitation on the collection or use of information. More specifically, a person has a degree of privacy when certain information – “private” information – about that person cannot be *perceived* or *used* by another entity. Privacy is a concept that only makes sense with respect to at least one other party. Thus, we can think of privacy as having three components: Entity A, information about Entity A, and Entity B. The less information about A that B can *perceive* or *use*, the more privacy A has from B.

We can better understand the genesis and resolution of privacy debates if we understand the difference between constraints on perceiving information and constraints on using information, and how these different constraints interact with new technology.

A. Perception Constraints

One type of information constraint – a “perception constraint” – exists when B cannot even perceive certain information about A. That might mean that B cannot perceive the signal carrying information (as when a closed door hides A from view) or that B cannot perceive the information carried in the signal (as when B cannot see with the unaided eye into the windows of A’s skyscraper apartment blocks away). Perception constraints rely on the world’s physical properties to block observers from accessing information.

³ Note that “transmission” need not be intentional. There is no intentionality in the transmission of the light that enable us to see the world around us.

⁴ At the level of neurons, even purely mental effort still affects physical reality, although we generally lack the technical means to sense such signals or fully understand their meaning.

⁵ See *generally*, Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008; GWU Legal Studies Research Paper No. 420; GWU Law School Public Law Research Paper No. 420. Available at SSRN: <https://ssrn.com/abstract=1127888>.

In the physical world most of our privacy relies on such perception constraints. Although there are nearly infinite amounts of information streaming off us in the physical world, other people face practical limits on their ability to capture such information. And most such signals quickly dissipate below the sensing threshold – the slight temperature rise I might cause when walking through a room, for example, will not linger long.

We learn at a very early age that there are the limits to our own control over information flows in the physical world. For example, because we cannot directly control the light that reflects off our bodies, we wear clothes, build doors, and install blinds to physically block such signals. Used this way, clothes, doors, and blinds become technological barriers to information flows.

On the other hand, much of human progress has been due to scientists and innovators removing barriers to information flows so that we can better understand and connect with the world around us. Devices like microscopes and telescopes enable us to gather information from signals we couldn't previously detect. Cameras allow us to share a representation of a scene with others who are not physically present. Communications networks enable us to speak to others far beyond the distance our voices can carry. Each of these technologies expand our ability to perceive information about the world around us, including information about other people.

B. Use Constraints

Sometimes it is not possible, practical, or desirable to stop other peoples' perception of information about us. In these cases, social norms, private rules, and law often constrain how others can use the information they gather. Thus, B may perceive information about A, but social pressure, private agreements, or government commands restrict how B can use that information. Use constraints can vary in degree from complete bans on any use to broad allowance of uses except for certain restricted uses.

Perception constraints rely on natural properties of physics or mathematics to control information flows. In contrast, use constraints control information flows based on the strength of the underlying social norms or the abilities of private or government enforcers.

C. The Privacy Challenge

Every privacy policy debate is over whether and how use constraints should supplement perception constraints. Such debates often erupt when a new technology increases the amount of information available, usually by generating entirely new types of information but also by weakening or eliminating certain perception constraints. Those debates often resolve as individuals and society adapt to the change, including at times by adopting new perception or use constraints.

Consider advent of popular portable cameras in the late 1800's, which made it possible and common to capture permanent information about individuals in public places. This new technology prompted

calls for legal privacy protections in the United States.⁶ But laws are only one type of tool to control information flow. Although people had concerns, they also saw many benefits, and society adapted to this new technology. Individuals learned what to expect from photographs and photographers, and how to mitigate or avoid photos. People developed social norms and private rules about where and how cameras may be used. And the legal system adapted common law torts and in some cases statutes to prevent or remedy harms caused by the technology.

Privacy debates are increasingly frequent today because the physical and online worlds have very different perception constraints. Because humans have deep experience with the physical world, we generally have accurate intuitions about how to block others' perception of information about us (e.g. close the door, whisper to your friend), and generally understand the vulnerabilities of such barriers.

But the internet has always had fewer and weaker perception constraints than the physical world, by design and by necessity. Online interactions can be tracked and stored much more efficiently and effectively than physical interactions. Indeed, digital communications are so powerful precisely because they are easy to observe, collect, store, and use in a relatively comprehensive manner.

Thus, as individuals increase their activities in this new online space where information is more observable, recordable, and usable, the relative lack of perception constraints creates new privacy challenges. Furthermore, as Internet of Things technologies increase the number of online sensors, more of the previously offline world will be digitally legible. This will be extremely beneficial, enabling software-driven solutions to a wider range of real-world problems. But it also reduces perception constraints in a way that some find unsettling.

In response to these technology changes, many seek to impose new use constraints on internet information flows. This is the policy challenge we face today.

IV. Tools to Protect Privacy

How might we address this challenge? There are many kinds of perception and use constraints, including several I have already mentioned. Let's take a deeper look at the various tools that are available to protect online privacy.

A. Technological Tools

Self-help software tools could help control information flows online, similar to how doors, clothes, and blinds help control information flows in the physical world. If effective, such online perception constraints would be preferable to almost any other approach. They would be self-executing, chosen by users, and would provide feedback into the information ecosystem that would maximize consumer autonomy – allowing those who want to protect information to do so without impeding others' desire to share.

⁶ See Louis Brandeis and Samuel Warren, "The Right To Privacy," 4 HARV. L. REV. 193 (1890).

Encryption technologies are the best online analog to privacy-protecting physical barriers. These technologies enable us to safely transmit sensitive information in financial and other transactions. Encrypting information helps ensure that only the intended recipient will receive that information. Other examples of online perception constraints include tools such as ad blockers or VPNs.⁷

However, technology-driven perception constraints cannot address all privacy concerns. Consumers willingly engage in online transactions that generate information. Indeed, in many cases a service *requires* information to operate. If encryption is analogous to window blinds that prevents a stranger on the sidewalk from observing me, most online interactions are more like inviting a guest into my house. We invite guests inside specifically so that the doors and blinds won't stop us from communicating. But once the guest is inside (or we're directly communicating with an online service), we cannot use those perception constraints to restrict information flows.

B. Evolving Social Norms

Social norms also control information flows. Society adapts to new technology over time, creating new norms around its use. As individuals use a new technology, they can evaluate the results as well as consider any criticism or praise from others. This feedback loop organically generates a shared sense across a community about the proper and improper uses of a technology.

Consider, for example, how social norms around Caller ID evolved. When first launched, many considered it a privacy invasion for the phone company to share your number with the person you were calling.⁸ Some states even regulated it. Today, people consider Caller ID to be a privacy benefit because it allows them to screen calls, and many people won't answer calls from numbers they don't recognize.

Such norms can restrict behavior even when perception constraints are removed. Returning to the house guest analogy, it is primarily manners and other norms that constrain snooping by guests, although hosts might also lock away specific sensitive items.

C. Private Agreements

Two parties might also address concerns about information flows by agreeing how such information will be used. These agreements can take many forms and, unlike regulation, can be specifically tailored to the needs of the parties. Such agreements could be formal contracts enforceable by either party under standard contract law. They could be pledges to comply with industry standards or self-regulatory standards, with those pledges enforced by the industry or the self-regulatory body. Or the

⁷ Other technological tools may include obfuscation techniques such as those outlined in *Obfuscation: A User's Guide for Privacy and Protest* by Finn Brunton and Helen Nissenbaum, Cambridge MA: MIT Press, 2015. Those tools have strengths and weaknesses of their own. See Neil Chilson, *Hiding in Plain Sight*, <https://issues.org/book-review-hiding-in-plain-sight/> (reviewing *Obfuscation*).

⁸ Omar Tene and Jules Polonetsky, "A Theory of Creepy: Technology, Privacy and Shifting Social Norms," 16 YALE J. L. & TECH 59, 72-73 (2013).

agreements could be implied or explicit promises in advertising or other documents to the consumer.

D. Legal Remedies

Thus far, the remedies to privacy concerns I have discussed involve only private parties. Legal remedies add another entity – government. When one party can legitimately force another party to act in a specific way, we say the first party has a legal right. All rights imply the power to force another to act, or to not act.

People disagree over how to define privacy rights. In the U.S., for commercial uses of data, our privacy rights are generally operationalized as a consumer protection right to not be harmed from the collection or use of information about us.⁹ In Europe, privacy rights focus on protecting the individual's decisions about how information about them is collected and used. As such, the U.S. and the E.U. use different legal tools to advance these different goals. And these are just two of many differing goals that are often described as privacy.¹⁰

Even if one settles on a specific privacy goal, there are a variety of legal designs one might use to advance that goal. These can be divided into two general categories, common law and legislation, although a continuum exists between the two.

E. Common Law

Common law is characterized by a judge's or other neutral decisionmaker's application of general principles to individual situations. Each case a judge hears and decides subsequently informs future cases. Each decision in a case also helps the public understand what behaviors and situations are likely to violate the law. The law therefore evolves incrementally through private litigation or government enforcement in specific cases.

The U.S. provides most consumer privacy protections through a common-law-like enforcement system.¹¹ When commercial actions cause privacy problems, the FTC brings cases to address those problems. In fact, the FTC has brought more than 500 privacy and data security related cases. Most of the FTC's privacy cases are based on its authority to stop unfair or deceptive acts or practices. That means the FTC holds companies to their privacy promises, serving as a backstop to private agreements. The FTC has also brought unfairness cases where consumers are substantially injured,

⁹ Mark MacCarthy, "Privacy Is Not A Property Right In Personal Information,"

<https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/#5873a902280f>.

¹⁰ See generally, Daniel J. Solove, "A Taxonomy of Privacy," 154 U. PENN. L. REV. 477 (2006), avail. at SSRN: <https://ssrn.com/abstract=667622>.

¹¹ The U.S. does have specific legislation for certain segments of the data ecosystem. For example, the health industry is governed by the Health Insurance Portability and Accountability Act; the financial industry by the Gramm-Leach-Bliley Act, and data about children by the Children's Online Privacy Protection Act. The U.S. also provides citizens with rights vis-à-vis the government use of information under the Fourth Amendment and certain statutes. In addition, there is also private enforcement under several common law or statutory torts.

could not reasonably avoid the injury, and this injury isn't outweighed by benefits to consumers or competition. The FTC further details its deception and unfairness enforcement through several "soft law" mechanisms such as guidance documents, reports, and letters.¹²

F. Legislation

The most prescriptive approach is the statutory or legislative approach in which a governing body sets forth detailed rules. These rules are specific to the problem being tackled. They often are focused on a single industry. Such rules often set forth exacting obligations, responsibilities, standards for judging compliance, and punishments and remedies for non-compliance. Once established, legislative rules can be difficult to change even if circumstances, such as new technology, require change. At best, this rigidity creates ambiguity, and at worst, roadblocks to innovation. Legislation can also entrench incumbent companies and business models, giving them a regulatory advantage over would-be competitors.

The EU has taken a legislative approach to privacy, most recently in its General Data Protection Regulation. The GDPR focuses on protecting the judgment of individuals on how information about them should be collected and used. The GDPR creates specific and detailed legal obligations that commercial data collectors and processors must follow. The GDPR restricts what companies can do with information about users, including how they can collect information. The GDPR also specifies what users can force companies to do with information about them. (Interestingly, EU residents have less protection from data use by their own government than do U.S. residents.)

The above categories often form a set of overlapping constraints on information. Cultural norms, private agreements, and soft law will continue to affect behavior, with or without legislation. Furthermore, general privacy principles built up over time through common law case-by-case evaluations are sometimes codified into specific rules. And privacy legislation still requires enforcement against violators, the results of which often require judges to interpret the rules in a way that affects future enforcement and popular understanding.

V. Criteria for Privacy Legislation

Building on the framework established above, here are six key recommendations for those considering legislative privacy proposals.

Preserve permissionless to the maximum extent possible. Historically, technological innovation has been the most successful means to advance consumer welfare.¹³ And, as discussed earlier, much of technological innovation has been the result of removing barriers to information flows so that we can better understand and connect with the world around us. Thus, all else being equal, we ought to

¹² See R. Hagemann, J. Skees, and A. Thierer, "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539 (forthcoming in Col. Tech. L. J.).

¹³ See generally, Deirdre McCloskey, *BOURGEOIS EQUALITY: HOW IDEA, NOT CAPITAL OR INSTITUTIONS, ENRICHED THE WORLD*, University of Chicago Press (2016).

prefer privacy approaches that permit greater information flows and more innovation. And in any case, we ought to consider the impact of any approach on innovation.

We can best compare privacy approaches' effect on innovation by estimating where they fall on the spectrum between perfectly permissionless and perfectly permissioned. A permissionless approach is one where the developer of the product or service doesn't have to seek permission, certification, or other authorization. Regulators evaluate the service by the outcome or likely outcome, not by the process used to produce the result.

By contrast, a permissioned approach is one where innovators must seek and receive government approval to pursue an innovation, or where government sets out a specific process that any innovator must follow. Companies might violate the law even if the ultimate outcome is neutral or beneficial for consumers by failing to follow the specified procedure. Furthermore, a company that follows the specified procedure might escape liability even if consumers are injured.

Permissionless approaches enable a wider range of potential innovations, including completely unforeseen approaches. Permissioned approaches narrow innovation options, often requiring innovators to fit a new service into a pre-existing framework and established processes. This narrowing does the greatest harm in fields where innovation would otherwise be rapid, unpredictable, and disruptive.

The types of tools that could address privacy concerns rank from “most permissionless” to “least permissionless” as follows:

- technological change
- social norms
- private contracts
- soft law
- common law
- legislation¹⁴

Again, many of these restrictions overlap and interact. For example, some legislative actions are more permissionless than others, depending on how much space they leave or create for higher-level solutions. The FTC Act Section 5 unfairness and deception standard, for example, was legislation that created a common law and soft law approach and provides an enforcement backstop for private contracts.

Avoid approaches or language that reinforce the idea that consumers *own* all data about them. The ownership/property metaphor doesn't work well for much information about a consumer – such as their interaction with a company website, or their path through a retail store, or

¹⁴ See, Adam Thierer, PERMISSIONLESS INNOVATION at 107, available at <http://permissionlessinnovation.org/book/>.

their conversation with a clerk.¹⁵ In such cases, the information, if “owned” at all, is arguably jointly or publicly owned. Assigning sole ownership rights to jointly produced or public information is inefficient, impractical, and in tension with the First Amendment rights of others.

Maintain a clear distinction between privacy and data security. These are very different problems that need different solutions. In many ways, data security is the narrower and simpler problem. For example, people generally agree that we don’t want consumer information lost or stolen in a breach, although people disagree over how to best avoid or deter that negative outcome. But in privacy, there isn’t an outcome that everyone agrees is good or bad. There is no universally agreed upon ideal world. Some believe consumers will be better off with minimal data collection even if it means banning or restricting certain business models. Others believe consumers will be better off if companies have broad freedom to collect and use data. To best tackle these problems, privacy and data security ought to be addressed separately.

Focus on regulating uses that injure consumers, rather than on restricting collection. Preventing consumer injury is the proper goal of privacy legislation, and legislation should directly pursue that goal. Legislation should set general expectations for outcomes followed by active enforcement. This ends-oriented approach better preserves permissionless innovation, because companies can try something novel and unanticipated, provided they are willing to face consequences – including making consumers whole – if things go wrong.

A focus on consumer injury also better addresses the cases where sensitive inferences drawn from non-sensitive data are used to a consumer’s detriment.

Legislation should generally avoid regulating collection practices. Collection itself, unless done deceptively, does not harm consumers. Indeed, much data is of no benefit to consumers until it is collected. Access and correction rights, if adopted at all, ought to be limited to the narrow set of sensitive uses where tangible consumer injury is more likely, such as credit or employment decisions.

Liability should require showing actual or likely consumer injury, with material deception as *per se* injury. If liability hinges on injury, many of the other details of privacy legislation become less important. Consumer injury should include the types of objective injury cognizable under an FTC unfairness analysis – primarily financial or physical harm or quantifiable increased risk of harm, but also potentially extreme mental duress that results in tangible harms. Critics who argue that injury ought to include unquantifiable harms are admitting that it will be impossible to judge whether their approach improves the lives of consumers on balance, even as it will certainly impose costs on businesses and their customers.

Clarify the application of the FTC’s unfairness and deception authority, rather than mandate best practices. Any legislation ought to further detail the Section 5 approach to privacy by specifying the criteria for consumer privacy injury in terms of deception and unfairness and empowering the FTC to bring enforcement actions in cases where such injury occurs or is likely to

¹⁵ Larry Downes, “A Rational Response to the Privacy ‘Crisis,’” <https://www.cato.org/publications/policy-analysis/rational-response-privacy-crisis>.

occur. Penalties ought to be proportional to the harm caused or likely to be caused, but sufficiently high to deter problematic behavior.

Some might wish to simply mandate the FTC's existing recommended privacy best practices. But doing so would lose the current focus on consumer injury that directs enforcement where it matters most. For example, if legislation mandates FTC recommendations such as "opt-out consent for unexpected uses of non-sensitive data" or "data minimization," practices that benefit consumers could still violate the law. Such an approach would deter useful data-driven services and products without benefiting consumers.

Do not give the FTC broad rulemaking authority. Because privacy is such a multi-faceted concept, general rulemaking authority around privacy would be broad delegation of legislative power that could result in administrative abuses. Rulemaking is a permissioned approach, like legislation – but with less political accountability. To avoid potential abuse, any rulemaking authority ought to be targeted to specific areas, such as defining substantial consumer injury or sensitive personal information.

VI. Conclusion

As Congress grapples with the increasing digital legibility of our world, it should not attempt to freeze this evolution through legislation. Doing so would sacrifice the benefits of technological innovation and hinder the creation of information that helps us better understand and interact with the world around us. American privacy protections continue to evolve through technology, social norms, private arrangements, and common law. If Congress seeks to legislate further privacy protections, it should preserve the environment of permissionless innovation that has made the internet such a vital tool for all Americans.