Pepperdine Law Review

Volume 47 | Issue 4 Article 2

5-30-2020

When Considering Federal Privacy Legislation

Neil Chilson

When Considering Federal Privacy Legislation

Neil Chilson*

Abstract

Legislators, advocates, and business interests are proposing federal privacy legislation with new urgency. The United States has a long-established federal framework for addressing commercial privacy concerns, including general consumer protection law and sector-specific legislation. 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.

Should we create a U.S. federal privacy law, and if so, how? When considering any kind of privacy regulation, three concepts are fundamental. First, no one can control all information about them. Second, all privacy laws are government-enforced constraints 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.

This Article defines privacy as the combined effect of two different types of constraints on information: perception and use. When

* Neil Chilson is a lawyer, computer scientist, and senior research fellow for tech and innovation at the Charles Koch Institute. He guides CKI's ongoing efforts to understand and promote the legal and cultural frameworks that best enable people to discover, innovate, and improve all of our lives. Before joining CKI, he was Chief Technologist at the Federal Trade Commission and an attorney advisor to acting FTC Chairman Maureen K. Ohlhausen. This Article originally appeared on the website of the Federalist Society's Regulatory Transparency Project.

perception constraints are weakened, privacy debates ensue about how to restore privacy, presumably by replacing those weakening perception constraints with use constraints. Different kinds of constraints can be used to protect online privacy, including technology, social norms, private agreements, common law, and legislation.

Six principles can guide policymakers in choosing among these constraints. These principles are to: maximize permissionlessness, avoid data ownership metaphors, distinguish between privacy and data security, focus on uses that injure consumers, clarify FTC authority, and avoid giving the FTC broad rulemaking authority.

In short, 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 and preserving the permissionless environment that has made the U.S. a leader in online innovation.

TABLE OF CONTENTS

I. INTRODUCTION

Legislators, advocates, and business interests are proposing federal privacy legislation with new urgency.[1] The United States has a long-established federal framework for addressing commercial privacy concerns, including general consumer protection laws and legislation for specific sectors, such as health care or financial services.[2] 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.[3]

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.[4] Second, all privacy laws are government-enforced restrictions on how one party can use information about another party.[5] Third, over-restricting

1. *See*, *e.g.*, *Examining Legislative Proposals to Protect Consumer Data Privacy Before the S. Comm. on Commerce, Sci., & Transp.* (Dec. 4, 2019), https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy (discussing separate legislative draft proposals by the Committee Chairman and a Ranking Member, among others); Press Release, Ron Wyden, U.S. Senator for Or., Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy, (Nov. 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy; Wendy Davis, *AT&T Calls for National Privacy Law*, DIGITAL NEWS DAILY (Nov. 13, 2018), https://www.mediapost.com/publications/article/327984/att-calls-for-national-privacy-law.html (arguing for various types of privacy legislation); Harper Neidig, *Advocates Draw Battle Lines on National Privacy Law*, HILL (Nov. 13, 2018), https://thehill.com/policy/technology/416341-advocates-draw-battle-lines-over-national-privacy-law.

2. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585–86 (2014).

3. Jennifer Huddleston, *The Problem of Patchwork Privacy*, BRIDGE (Aug. 23, 2018), https://www.mercatus.org/bridge/commentary/problem-patchwork-privacy (discussing the issues arising from a multitude of state privacy laws).

4. *See* CESAR HIDALGO, WHY INFORMATION GROWS: THE EVOLUTION OF ORDER, FROM ATOMS TO ECONOMIES xix (2018) (describing information as the arrangement of physical things, which is why "[i]t is the *only* thing we produce"); Solove & Hartzog, *supra* note 2, at 589–99 (explaining the history of federal privacy laws).

5. *See* Press Release, Ron Wyden, *supra* note 1 (detailing ways in which corporations exploit users' data); *see also* Carole Piovesan, *How Privacy Laws Are Changing to Protect Personal Information*, FORBES (Apr. 5, 2019), https://www.forbes.com/sites/cognitiveworld/2019/04/05/how-privacy-laws-are-changing-to-protect-personal-information; Wesley Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16, 30–32 (1913) (explaining legal rights as a constraint on others' actions).

the use of information about individuals can harm individuals by limiting beneficial innovation.[6]

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 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.[7]

In the following pages, I will first explain what information is and then define privacy as the result of 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 weakened 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 United States can address privacy concerns through government action while preserving the permissionless environment that has made the United States a leader in online innovation. In short, I argue that federal legislation should enhance the ability of the Federal Trade Commission (FTC) 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.[8] The signal could be light reflecting off an object, soundwaves coming off an object, light or electrons moving through a conduit, or any other change in the physical world that can

6. *See* Neidig, *supra* note 1 (highlighting the harm of over-restricting individuals' privacy); *see also* ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA, (2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.

7. *See* Solove & Hartzog, *supra* note 2, at 666–67 (discussing the necessary balance between access to information and privacy protection).

8. C. E. Shannon, *A Mathematical Theory of Communication*, 27 (3) BELL SYS. TECH. J. 379, 379–423 (1948) (distinguishing between signal and information). Shannon acknowledges that information conveyed thus often has meaning, although such meaning is irrelevant to his particular engineering problem. *Id.* at 379.

be sensed.[9] Signals can carry information enabling the receiver to determine something about the state of the transmitter.[10]

As physical beings in a physical world, information flows off us constantly and we cannot control all of it.[11] 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.[12] 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.[13] 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.[14] Defined thus, privacy is a concept that only makes sense with respect

9. *Id.* at 380 (providing examples of information submitted through signals); *see also* Peter Kinget, *The World is Analog*, CIRCUIT CELLULAR (2014), http://www.ee.columbia.edu/~kinget/WhyAnalog/circuitcellar_The_World_Is_Analog_201410.pdf.

10. Shannon*, supra* note 8, at 379. Note that "transmission" need not be intentional. There is no intentionality in the transmission of the light that enables us to see the world around us.

11. HIDALGO, *supra* note 4, at xix (describing information as the arrangement of physical things, which is why "[i]t is the *only* thing we produce").

12. *Id.*; *see also The Neuroscience of Decision Making*, BRAINFACTS.ORG (Aug. 1, 2011), https://www.brainfacts.org/archives/2011/the-neuroscience-of-decision-making. 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. *Id.*

13. Adam Thierer, *Are Benefit-Cost Analysis and Privacy Protection Efforts Incompatible?*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 561, 564 (Evan Selinger et al. eds., 2018) ("Legal scholars have observed that attempts to define privacy are 'notoriously contentious' and can quickly become a 'conceptual jungle.'"); *see* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1–8 (2008) (discussing the multitude of privacy definitions and describing privacy as "a concept in disarray").

14. *See* Daniel Benoliel, *Law, Geography and Cyberspace: The Case of On-Line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125, 130 (2005).

to at least one other party.[15] Thus, we can think of privacy as the relative state of a system 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.

This broad, descriptive definition lacks the specificity of some other definitions.[16] But abstractly describing a state of privacy highlights some important principles that might be missed if one jumps directly to delineating the boundaries of privacy rights or privacy harms.[17] In particular, the distinction between the perception of information and the use of information is important.[18] 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.[19]

A. Perception Constraints

One type of information constraint—a "perception constraint"—exists when B cannot even perceive certain information about A.[20] This can occur when B cannot perceive the signal carrying information, as when a closed door hides A from view. In other instances, even though B might be able to perceive the signal, B cannot extract the information carried in the signal. For example, B might be able to see a skyscraper many blocks away, but with her unaided eye, cannot see into the windows of A's apartment in that skyscraper, even though the light reflected from A's apartment reaches B's eye. Perception constraints rely on the world's physical properties to block observers from accessing information.[21]

15. *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 429 (1980) (noting that certain common-sense scenarios make sense only if "the amount of information others have about an individual is considered at least partly determinative of the degree of privacy he has").

16. *See* Benoliel, *supra* note 14, at 127–28; Gavison, *supra* note 15, at 424 (explaining "privacy" is a term with many meanings).

17. *See* Harry Surden, *Structural Rights in Privacy*, 60 S.M.U. L. REV. 1605, 1605–06 (2007) (discussing non-obvious privacy principles and the different constraints of information).

18. *Id.* at 1607.

19. *Id.* at 1607–08 (discussing the differences between structural constraints and latent structural constraints, and their interactions with technology).

20. *Id.* at 1606 n.3, 1607, 1612 (discussing a similar concept he calls "latent structural constraints").

21. Surden, *supra* note 17, at 1607; *see also* Jamuna D. Kelley, *Computer with a View: Progress, Privacy and Google*, 74 BROOK. L. REV. 187, 188 (2008) ("Physical protections are the logistical

In the physical world most of our privacy relies on such perception constraints.[22] Although there are massive 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 increase I might cause when walking through a room, for example, will not linger long.[23]

We learn at a very early age that there are 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.[24] Devices like microscopes and telescopes enable us to gather information from signals we could not previously detect.[25] 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.[26] Each of

obstacles that prevent society from gathering information about an individual, such as locked doors or password-protected hard drives.").

22. *See* Richard Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1, 7 (1978) ("Doors, private apartments, unattached single-family houses, and private automobiles facilitate privacy in the less tangible senses of seclusion or secrecy.").

23. *See, e.g.*, James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 321 (2002); *cf.* Kelley, *supra* note 21, at 194 ("Furthermore, the fact that Street View publicizes moments in time that might otherwise go completely unnoticed also contradicts Google's position that Street View reveals nothing more than does a stroll around town.").

24. *See* HIDALGO, *supra* note 4, at xx ("[I]t is the accumulation of information and of our ability to process information that defines the arrow of growth encompassing the physical, the biological, the social, and the economic, and which extends from the origin of the universe to our modern economy."); NAT'L ACADS. OF SCI., ENG'G, & MED., INFORMATION TECHNOLOGY AND THE U.S. WORKFORCE (2017), https://www.nap.edu/24649 (reviewing how technological innovations transform aspects of society).

25. *See* Tomkovicz, *supra* note 23, at 320–21; Lawrence Kaiser Marks, *Telescopes, Binoculars, and the Fourth Amendment*, 67 CORNELL L. REV. 379, 379–80 (1982) (examining "the reasonable expectation of privacy standard as applied to evidence obtained through telescope and binocular surveillance," and "suggest[ing] that police use of telescopes and binoculars to observe activities or objects unobservable from a proper location by the 'naked eye' violates an individual's expectation of privacy").

26. *See* Craig Timberg, *A Flaw in the Design*, WASH. POST (May 30, 2015), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.0c866

these technologies expand our ability to perceive information about the world around us, including information about other people.[27]

B. Use Constraints

Sometimes it is not possible, practical, or desirable to stop other people's perception of information about us.[28] In these cases, social norms, private rules, and law often constrain how others can use the information they gather.[29] Thus, B may perceive information about A, but social pressure, private agreements, or government commands restrict how B can use that information.[30] Use constraints can vary in degree, from complete bans on any use to broad allowance of uses except for certain restricted uses.[31]

Perception constraints rely on natural properties of physics or mathematics to control information flows.[32] In contrast, use constraints control information flows based on the strength of the underlying social norms, or the abilities of private or government enforcers.[33]

C. The Privacy Challenge

Every privacy policy debate is over whether and how use constraints should supplement perception constraints.[34] Such debates often erupt when a new technology increases the amount of information available, usually by

3583583 [http://wapo.st/1J9UYJy] (examining the historical development of the Internet, which "allowed virtually any computer network in the world to communicate directly with any other, no matter what hardware, software or underlying computer language the systems used").

27. *See* Tomkovicz, *supra* note 23, at 320–21.

28. *See* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM 69–70 (rev. and expanded ed. 2016) (arguing that the growing concerns over privacy should not curtail data collection because "innovative services, devices, and applications might be lost in the future").

29. *Id*. (describing how social norms evolved after the introduction of the camera).

30. *See* Surden, *supra* note 17, at 1610.

31. *Id.*

32. *See* Kelley, *supra* note 21, at 188.

33. *See* Jisuk-Woo & Jae-Hyup Lee, *The Limitations of Information Privacy in the Network Environment*, 7 PITT. J. TECH. L. & POL'Y 1, 12 (2006) (explaining that the general policy "in the United States has placed heavy reliance on individuals policing their own records and protecting their own information from unintended use" (citing James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 6 (2003))).

34. *See* David Annecharico, *Online Transactions: Squaring the Gramm-Leach-Bliley Act Privacy Provisions with the FTC Fair Information Practice Principles*, 6 N.C. BANKING INST. 637, 640 (2002).

generating entirely new types of information, but also by weakening or eliminating certain perception constraints.[35] Those debates often resolve as individuals and society adapt to the change, including at times by adopting new perception or use constraints.[36]

Consider the advent of popular portable cameras in the late 1800s, which made it possible and common to capture permanent information about individuals in public places.[37] This new technology prompted calls for legal privacy protections in the United States.[38] But laws are only one type of tool to control information flow.[39] Although people had concerns, they also saw many benefits, and society adapted to this new technology.[40] Individuals learned what to expect from photographs and photographers, and how to mitigate or avoid photos.[41] People developed social norms and private rules about where and how cameras may be used.[42] And the legal system adopted common law torts and, in some cases, statutes to prevent or remedy harms caused by the technology.[43]

Privacy debates are increasingly frequent today because the physical and online worlds have very different perception constraints.[44] Because humans

35. *See* Surden, *supra* note 17, at 1608.

36. *See* DANIEL CASTRO & ALAN MCQUINN, INFO. TECH. & INNOVATION FOUND., THE PRIVACY PANIC CYCLE: A GUIDE TO PUBLIC FEARS ABOUT NEW TECHNOLOGIES 5–6, 25 (2015), http://www2.itif.org/2015-privacy-panic.pdf (urging lawmakers to consider how society adapts over time when deciding whether to regulate new technology).

37. *Id.* at 2 (describing the initial panic over privacy concerns with the portable Kodak camera); *see also Original Kodak Camera*, *Serial No. 540*, NAT'L MUSEUM OF AM. HIST. (last visited Feb. 26, 2020), https://americanhistory.si.edu/collections/search/object/nmah_760118 (discussing the invention of the Kodak portable camera).

38. *See* Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (arguing that common law protects a right to privacy in the wake of the popularization of the portable camera).

39. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, YALE L.J. & TECH. 59, 75 (2013) (noting that individuals choose what to share).

40. *See* CASTRO & MCQUINN, *supra* note 36, at 2 (explaining how people were aghast at the idea of taking public photos in the early 1900s, yet everyone now carries a powerful camera in their pocket).

41. *See id.* at 12 (discussing the bans implemented against cameras at beaches and the Washington monument).

42. *Id.* at 2; *see also* Tene & Polonetsky, *supra* note 39, at 71–72 (noting how people adjusted their expectations and norms after cellphones with cameras became widely used in gym locker rooms).

43. *See* Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 703–04 (1990) (describing the adoption of common law torts protecting privacy as a result of the Warren and Brandeis article).

44. *See* BROOKE AUXIER ET. AL, PEW RESEARCH CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 12–15 (Nov. 15,

have deep experiences 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.[45]

But the Internet has always had fewer and weaker perception constraints than the physical world, by design and by necessity.[46] Online interactions can be tracked and stored much more efficiently and effectively than physical interactions.[47] Indeed, digital communications are so powerful precisely because they are easy to observe, collect, store, and use in a relatively comprehensive manner.[48]

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.[49] Furthermore,

---

2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (providing empirical research about Americans' concerns and fears about online privacy); Emily Steel, *Protecting Offline Privacy*, WALL STREET J. (Nov. 19, 2009), https://www.wsj.com/articles/SB10001424052748704533904574543400320693232 (overviewing how policymakers and consumer advocates worry about digital companies' use of consumer data to sell and market products).

45. *See* Jonathan Shaw, *Exposed: The Erosion of Privacy in the Internet Era*, HARV. MAG. 38 (2009), http://www.harvardmag.com/pdf/2009/09-pdfs/0909-38.pdf (Internet has eroded many of the essential aspects of privacy); *cf*. CASTRO & MCQUINN, *supra* note 36, at 3 (analyzing the privacy panic cycle and finding that the general public panics when a new technology emerges because the public understands little about the technology and "privacy fundamentalists" exaggerate the privacy issues of the technology).

46. *See TCP Definition*, LINUX INFO. PROJECT, http://www.linfo.org/tcp.html (last visited Feb. 26, 2020) (explaining the transmission control protocol, a trait of the digital world). As a system dedicated to accurately transferring information, the Internet is designed to avoid information degradation that occurs in the physical world. *Id*. ("[Fundamental Internet protocol] TCP uses error correction and data stream control techniques to ensure that packets to arrive at their intended destinations uncorrupted and in the correct sequence, thereby making the point-to-point connection virtually error-free."); *see also* Timberg, *supra* note 26 (describing how the Internet "developed into a communication system that operated mostly in the clear—meaning anyone with access to the network could monitor transmissions").

47. *See* FED. TRADE COMM'N, CROSS-DEVICE TRACKING 1–5 (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (describing online tracking technologies).

48. *See* Tene & Polonetsky, *supra* note 39, at 84; Shaw, *supra* note 45 ("People can collect data and never throw anything away. Policies on data sharing are not very good, and the result is that data tend to flow around and get linked to other data.").

49. Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 290–91 (2003) (arguing that digital technology makes past legal conceptions of privacy difficult to enforce).

as "Internet of Things" technologies increase the number of online sensors, more of the previously offline world will be digitally legible.[50] This will be extremely beneficial, and will enable software-driven solutions to address a wider range of real-world problems.[51] But it also reduces perception constraints in a way that some find unsettling.[52]

In response to these technology changes, many seek to impose new use constraints on Internet information flows.[53] This is the policy challenge we face today.[54]

IV. TOOLS TO PROTECT PRIVACY

How might we address this challenge?[55] There are many kinds of perception and use constraints, including several I have already mentioned.[56] Let's take a deeper look at the various tools that are available to protect online privacy.

50. Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 1, 6–7 (2014).

51. *The Sensor-Based Economy*, WIRED, https://www.wired.com/brandlab/2017/01/sensor-based-economy/ (last visited Feb. 26, 2020) (describing how new sensors and Internet-connected devices will proliferate and become common to individuals' daily routines).

52. *See* AUXIER ET. AL, *supra* note 44, at 2 ("Some 81% of the public say that the potential risks they face because of data collection by companies outweighs the benefits, and . . . a majority of Americans report being concerned about the way their data is being used by companies (79%) or the government (64%)."); *see also* Amadou Diallo, *Do Smart Devices Need Regulation? FTC Examines Internet of Things*, FORBES (Nov. 23, 2013), https://www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/#772ddb838015 (discussing how Internet-connected devices offer convenience but raise privacy issues). *But see* CASTRO & MCQUINN, *supra* note 36, at 7 (noting that the practice of entering credit card information into a computer spread quickly once people understood that it produced a lower risk of fraud than physical use of the credit card).

53. *See* Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. 49, 52 (2013) ("If we intend for our economic and legal frameworks to shift from data collection to use, it is essential to begin the conversation about what sort of uses we want to take off the table."); Cristiano Lima, *A Cornucopia of Privacy Proposals*, POLITICO (Nov. 27, 2019, 10:00 A.M.), https://www.politico.com/newsletters/morning-tech/2019/11/27/a-cornucopia-of-privacy-proposals-783154 (describing dueling Senate privacy bills).

54. *See* Jerome, *supra* note 53; Lima, *supra* note 53; Tene & Polonetsky, *supra* note 39, at 73.

55. *See* Tene & Polonetsky, *supra* note 39, at 73 (implying that social norms might be a better tool than the law to impose use constraints).

56. *See supra* notes 36–41 and accompanying text.

A. Technological Tools

Self-help software tools could help control information flows online, similarly to how doors, clothes, and blinds help control information flows in the physical world.[57] If effective, such online perception constraints would be preferable to almost any other approach.[58] 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.[59]

Encryption technologies are the best online analog to privacy-protecting physical barriers.[60] These technologies enable us to safely transmit sensitive information in financial and other transactions.[61] Encrypting information helps ensure that only the intended recipient will receive that information.[62] Other examples of online perception constraints include tools such as ad blockers and VPNs.[63]

However, technology-driven perception constraints cannot address all privacy concerns.[64] Consumers willingly engage in online transactions that generate information.[65] Indeed, in many cases a service *requires* information to operate.[66] If encryption is analogous to window blinds that prevent a

57. *See* Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 440–45 (2013).

58. *See* Tene & Polonetsky, *supra* note 39, at 92–93 (describing the "significant challenges in providing easy-to-use tools that give users meaningful control without interfering with their use of the web" (citation omitted)); Thierer, *supra* note 57, at 445.

59. *See* Tene & Polonetsky, *supra* note 39, at 84–85 (providing examples of popular services that provide users with the opportunity to balance autonomy and privacy); Thierer, *supra* note 57, at 445.

60. Vindu Goel, *Encryption Is More Important, and Easier, Than Ever*, N.Y. TIMES (Oct. 14, 2015, 4:35 P.M.), https://bits.blogs.nytimes.com/2015/10/14/encryption-is-more-important-and-easier-than-ever/.

61. *Id.* ("[E]ncryption essentially creates a private connection . . . an unencrypted connection also opens the possibility of a hacker[] . . . steal[ing] personal information.").

62. *Id.*

63. *See generally* FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015) (outlining other technological tools including obfuscation techniques). Obfuscation techniques have strengths and weaknesses of their own. *Id.* at 92–93; *see also* Neil Chilson, *Hiding in Plain Sight*, 34 ISSUES SCI. & TECH. 88 (2018) (reviewing BRUNTON & NISSENBAUM, *supra*).

64. *See* Thierer, *supra* note 57, at 454–55.

65. *Id.* at 431–32 ("[I]nformation wants to be free . . . .").

66. *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-

stranger on the sidewalk from observing me in my house, most online interactions are more like inviting a guest inside.[67] We invite guests inside specifically so that the doors and blinds won't stop us from communicating.[68] But once the guest is inside (or when we're directly communicating with an online service), we can no longer use those perception constraints to restrict information flows.[69]

B. Evolving Social Norms

Social norms also control information flows.[70] Society adapts to new technology over time, creating new norms around its use.[71] As individuals use a new technology, they can evaluate the results as well as consider any criticism or praise from others.[72] This feedback loop organically generates a shared sense across members of a community about the proper and improper uses of a technology.[73]

Consider, for example, how social norms around Caller ID evolved.[74] When it first launched, many considered it a privacy invasion for the phone company to share your number with the person you were calling.[75] Some

era-rapid-change-recommendations/120326privacyreport.pdf. For example, ordering from online retailers requires providing your shipping address and payment information. *Id.* at 44. Privacy concerns about information inherent to a transaction usually revolve around unexpected uses or sharing with third parties. *Id.* at 26–27, 47 (recommending that "companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business" and that uses inconsistent with what a consumer might expect should be accompanied by additional disclosure).

67. *Id.* at 7–8 (articulating the harm caused by intrusive data collection practices).

68. *See* Louis Menand, *Why Do We Care So Much About Privacy?*, NEW YORKER (June 11, 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy (highlighting the contrast that we "store more in the cloud than in lockboxes," and thus we trade the efficiency of operating online for "a society whose citizens have nowhere to hide").

69. *Id.*

70. *See* Thierer, *supra* note 28, at 74.

71. *Id.*; *see also* Adam Thierer, *Privacy and Security Implications of the Internet of Things*, 1, 5–8 (June 1, 2013), https://ssrn.com/abstract=2273031 (providing examples of social adaption to six different technologies and a description of how norms can regulate use).

72. *See* Thierer, *supra* note 28, at 74–77.

73. *Id.*

74. *Id.* at 70.

75. States News Service, *'Caller ID' Stirs Debate on Phone Privacy*, N.Y. TIMES (Feb. 11, 1990), https://www.nytimes.com/1990/02/11/nyregion/caller-id-stirs-debate-on-phone-privacy.html [https://nyti.ms/29uyuJa] (describing a wide range of privacy concerns with Caller ID).

states even regulated it.[76] Today, many people consider Caller ID—which is a standard feature on every mobile phone—to be an improvement to their privacy because it allows them to screen calls, and many people won't answer calls from numbers they don't recognize.[77]

Such norms can restrict behavior even when perception constraints are removed.[78] 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.[79]

C. Private Agreements

Two parties might also address concerns about information flows by agreeing how such information will be used.[80] These agreements can take many forms and, unlike regulation, can be specifically tailored to the needs of the parties.[81] Such agreements could be formal contracts enforceable by either party under standard contract law.[82] 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.[83] Or the agreements could be implied or explicit promises in advertising or other documents to the consumer.[84]

---

76. Laurie Thomas Lee, *U.S. Telecommunications Privacy Policy and Caller ID*, 30 CAL. W. L. REV. 1, 5–7 (1993) (discussing the history of government regulation around Caller ID).

77. *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 118 (2014); *see also* Thierer, *supra* note 28, at 70.

78. Thierer, *supra* note 28, at 74–77 (stating that social norms are "the grammar of society").

79. *Id.* (noting that Edmund Burke stated that "[m]anners are more important than laws" in shaping behavior).

80. *Id.* at 123–24.

81. Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J. L. & PUB. POL'Y 591, 609 (1994).

82. *Id*. at 605–08.

83. *See, e.g.*, Comment Letter from Council of Better Bus. Bureaus to Nat'l Telecomm. & Info. Admin. on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/cbbb_comment_to_ntia_on_consumer_privacy_-_11.09.18.pdf (describing three privacy-related self-regulatory programs run by the BBB).

84. *See* Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n, Speech Before the Hudson Institute: The Government's Role in Privacy (Oct. 16, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/governments-role-privacy-getting-it-right/121016governmentrole.pdf. These types of "agreements" are more likely to be enforced by government consumer protection agencies. *Id.* (describing how the FTC can and has brought cases against companies that break their promises to consumers).

D. Legal Remedies

Thus far, the remedies to privacy concerns I have discussed involve only private parties. Legal remedies add another entity—government.[85] When one party can legitimately force another party to act in a specific way, we say the first party has a legal right.[86] All rights imply the power to force another to act, or to not act.[87]

People disagree over how to define privacy rights.[88] In the United States, for commercial uses of data, our privacy rights are generally operationalized as a consumer protection right to not be harmed by the collection or use of information about us.[89] In Europe, privacy rights focus instead on protecting individuals' decisions about how information about them is collected and used.[90] As such, the U.S. and the EU use different legal tools to advance these different goals.[91] And these are just two of many differing goals that are often described as privacy.[92]

Even if one settles on a specific privacy goal, there are a variety of legal

85. *See, e.g.*, Ohlhausen, *supra* note 84, at 2 (explaining how the Federal Trade Commission, a government agency, "often uses its deception authority in cases where a company makes a representation to consumers about the collection and/or use of their personal data but it fails to keep that promise and consumer injury results"); *see* Donald H. Zeigler, *Rights Require Remedies: A New Approach to the Enforcement of Rights in the Federal Courts*, 38 HASTINGS L.J. 665, 681 (1987).

86. *See* ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 154, 155 (1995) (discussing the legal right to privacy); *see also* Zeigler, *supra* note 85, at 665.

87. *See* Ziegler, *supra* note 85, at 678–80; *see also* ALDERMAN & KENNEDY, *supra* note 86, at 155.

88. Judith Jarvis Tomson, *The Right To Privacy*, 4 PHIL. & PUB. AFF. 295, 295 (1975) ("Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."); *see also* Deirdre K. Mulligan, Colin Koopman & Nick Doty, *Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy*, 374 PHIL. TRANS. R. SOC. A 1, 1 (2016), https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2016.0118 (describing privacy rights as an essentially contested concept that cannot be resolved but can be productively explored).

89. Mark MacCarthy, *Privacy Is Not A Property Right In Personal Information*, FORBES (Nov. 2, 2018, 12:36 P.M.), https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/#5873a902280f (arguing against treating online privacy as a property right).

90. Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius*, The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 66, 76 (2019) (describing the conditions and approach laid out by the European Union's General Data Protection Rules).

91. *Id.* (discussing the U.S. and EU approaches to privacy); *see also Comparison of European and American Privacy Law*, HIPAA J. (Apr. 25, 2018), https://www.hipaajournal.com/comparison-of-european-and-american-privacy-law/.

92. *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 479 (2006) (discussing the various definitions of privacy).

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.[93]

1. Common Law

Common law is characterized by a judge's or other neutral decisionmaker's application of general principles to individual situations.[94] Each case a judge hears and decides subsequently informs future cases.[95] Each decision in a case also helps the public understand what behaviors and situations are likely to violate the law.[96] The law therefore evolves incrementally through private litigation or government enforcement in specific cases.[97]

The United States provides most consumer privacy protections through a common-law-like enforcement system.[98] When commercial actions cause

93. *See* Simon Dawes, *Press Freedom, Privacy and the Public Sphere*, 15 JOURNALISM STUD. 17, 19 (2014) (discussing common law and legislation as two approaches for providing "remedies for breaches of privacy").

94. *See* Arthur L. Corbin, *What is the Common Law?*, 3 AM. L. SCH. REV. 73, 75 (1912).

95. *See* Morris L. Cohen, *The Common Law in the American Legal System: The Challenge of Conceptual Research*, 81 L. LIBR. J. 13, 23 (explaining that doctrines of precedent are one of "the main features of common law in America").

96. Corbin, *supra* note 94, at 75; *see, e.g.*, Gordon Tullock, *Public Decisions as Public Goods*, 79 J. POL. ECON. 913, 913 (explaining that a judge's decision in a case "is a direct generation of externalities by him—the externalities falling on the participants in the case" and that "[i]n addition to these rather restricted externalities, he . . . participat[es] in the production of a public good: law enforcement").

97. *See* Cohen, *supra* note 95, at 20 (explaining that jurisdictions respond to "the common law by charter, subsequent legislation, or constitutional provision").

98. Solove & Hartzog, *supra* note 2, at 585 (discussing the FTC's role in "polic[ing] unfair and deceptive trade practices" since the late 1990s); *see, e.g.*, Charles M. Horn, *Financial Services Privacy at the Start of the 21st Century: A Conceptual Perspective*, 5 N.C. BANKING INST. 89 (2001). The U.S. does have specific legislation for certain segments of the data ecosystem. *Id.* at 93–94, 100. 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. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1936 (1996); Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (1998). The U.S. also provides citizens with rights vis-à-vis the government use of information under the Fourth Amendment and certain statutes. Kevin Emas & Tamara Pallas, *United States v. Jones: Does Katz Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116, 137–38 (2012) (discussing Fourth Amendment privacy protection from the government); *see also* Harold J. Kent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 71 n.109 (1995) ("Additional statutes limit what the government can do with information generated under its directives."). In addition, there is also private enforcement under several common law or statutory torts.

privacy problems, the FTC brings cases to address those problems.[99] In fact, the FTC has brought more than 500 privacy- and data security-related cases.[100] Most of the FTC's privacy cases are based on its authority to stop unfair or deceptive acts or practices.[101] That means the FTC holds companies to their privacy promises, serving as a backstop to private agreements.[102] The FTC has also brought unfairness cases where consumers are substantially injured, could not have reasonably avoided the injury, and their injury isn't outweighed by benefits to consumers or competition.[103] The FTC further details its deception and unfairness enforcement through several "soft law" mechanisms such as guidance documents, reports, and letters.[104]

2. Legislation

The most prescriptive approach is the statutory or legislative approach, in which a governing body sets forth detailed rules.[105] These rules are specific

See Solove & Hartzog, *supra* note 2, at 587 (discussing statutory law and common law torts concerning privacy).

99. *See* Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Vera Jourova, Comm'r, Justice, Consumers & Gender Equality, European Comm'n (Feb. 23, 2016), https://www.ftc.gov/system/files/documents/public_statements/927423/160229ftc_privacyshieldletter.pdf [hereinafter Ramirez Letter]; *see also* Ohlhausen, *supra* note 84, at 2 ("In the areas of privacy and data security, the Commission most often uses its deception authority in cases where a company makes a representation to consumers about the collection and/or use of their personal data but it fails to keep that promise and consumer injury results.").

100. Ramirez Letter, *supra* note 99.

101. *See* Olhausen, *supra* note 84, at 2 (discussing the FTC's deception authority).

102. *Id.*

103. *Id.* ("[T]he Commission's unfairness authority . . . focuses on the consumer harm that an act or practice may cause. The Commission's unfairness statement requires that for the Commission to find an act or practice unfair the harm it causes must be substantial, it must not be outweighed by an offsetting consumer or competitive benefits, and the consumer could not have reasonably avoided harm.").

104. *See* Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 44 (2018) (discussing the FTC and "soft law").

105. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117, 1124 (2017); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 495 (2013) ("Fifty years of federal legislative interest in privacy has resulted in one commonly recognized and often lamented fact: American privacy law is extraordinarily piecemeal . . . 'it is unusual in the United States to find any comprehensive privacy laws.'").

to the problem being tackled.[106] They often are focused on a single industry.[107] Such rules often set forth exacting obligations, responsibilities, and standards for judging compliance, and punishments and remedies for non-compliance.[108] Once established, legislative rules can be difficult to change even if circumstances, such as new technology, require change.[109] At best, this rigidity creates ambiguity, and at worst, roadblocks to innovation.[110] Legislation can also entrench incumbent companies and business models, giving them a regulatory advantage over would-be competitors.[111]

The EU has taken a legislative approach to privacy, most recently in its General Data Protection Regulation (GDPR).[112] The GDPR focuses on protecting the judgment of individuals on how information about them should be collected and used.[113] The GDPR creates specific and detailed legal obligations that commercial data collectors and processors must follow.[114] The

106. *See* Murphy, *supra* note 105, at 495 (explaining that U.S. legislation "largely relie[s] on independent enactments tailored to particular sectors or interests").

107. *Id.* at 496 (explaining that "[t]he word 'patch-work' is often used to describe . . . statutory protections" because they are tailored to specific issues without "a single guiding principle or theory").

108. *See* Kerr, *supra* note 105, at 1153–54; *see also* Frank H. Easterbrook, *What Does Legislative History Tell Us?*, 66 CHI. KENT L. REV. 441, 447 (1990).

109. *See* Kerr, *supra* note 105, at 1155; PRISCILLA M. REGAN, LEGISLATING PRIVACY 174 (1995) (explaining that "issues were placed on the congressional agenda in response to technological changes perceived as threatening privacy" and yet, "the issues were on the congressional agenda for years, if not decades, before Congress passed legislation").

110. *See, e.g.*, Lawrence D. Drexler, *Privacy in Financial Services: "A Hard Rain's Gonna Fall"*, 18 DEL. L. 9, 11–12 (2000); Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J. L. TECH. & POL'Y 239, 239 (2007) ("It is often stated that the law lags behind technology. As technology changes and creates new possibilities, lawyers and legal scholars struggle to deal with the implications.").

111. *See* Moses, *supra* note 110, at 274 ("Thus, while it may be possible to avoid discriminating among known technologies, it will not always be possible to avoid discriminating against future, unknown technologies.").

112. *What Is GDPR?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited Feb. 26, 2020); *see* Hoofnagle et al., *supra* note 90, at 71 (discussing the EU's approach to privacy).

113. *See* Hoofnagle et al., *supra* note 90, at 77 (explaining that the GDPR's "purpose limitation principle entails that personal data should only be collected for a purpose that is specified in advance, and that those data should not be used for incompatible purposes"); *General Data Protection Regulation (GDPR)*, EUROPEAN CAMPUS CARD ASS'N, https://ecca.eu/index.php/news/180-general-data-protection-regulation-gdpr (last visited Feb. 26, 2020).

114. *See* Hoofnagle et al., *supra* note 90, at 85, 88 ("The GDPR reaffirms the role of the data controller as the party responsible for the data, and imposes stricter controls, duties, and even liability on processors . . . these responsibilities require controllers and processors to document compliance, noncompliance, and failures in the form of data breaches."); EUROPEAN COMM'N, THE GDPR: NEW OPPORTUNITIES, NEW OBLIGATIONS 1, 8 (2018), https://ec.europa.eu/info/sites/info/files/data-

GDPR restricts what companies can do with information about users, including how they can collect information.[115] The GDPR also specifies what users can force companies to do with information about them.[116] (Interestingly, EU residents have less protection from data use by their own government than United States residents.)[117]

The above categories often form a set of overlapping constraints on information.[118] Cultural norms, private agreements, and soft law will continue to affect behavior, with or without legislation. Furthermore, general privacy principles that have 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, below are six key recommendations for those considering legislative privacy proposals.

Preserve permissionless approaches to the maximum extent possible.[119] Historically, market-tested technological innovation has been the most successful means to advance consumer welfare.[120] And, as discussed earlier,

protection-factsheet-sme-obligations_en.pdf (highlighting the obligations companies have under the GDPR).

115. *See* Hoofnagle et al., *supra* note 90, at 79 (explaining the six legal justifications for processing personal data).

116. *GDPR Compliance Checklist for US Companies*, GDPR.EU, https://gdpr.eu/compliance-checklist-us-companies/ (last visited Feb. 26, 2020) (specifying the conditions that American companies must follow when operating in the EU and handling individuals' personal data).

117. Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. Are "Stricter" Than Each Other for the Privacy of Government Requests for Information*, 66 EMORY L.J. 617, 619 (2017) (discussing how American privacy laws provide greater privacy protection against government actors than do European privacy laws).

118. *See GDPR Compliance Checklist for US Companies*, *supra* note 116 (describing the EU's GDPR restrictions on United States companies operating inside the EU); *see also* MacCarthy, *supra* note *89* (describing privacy rights for commercial uses of data in the United States).

119. *See* Adam Thierer, *Embracing a Culture of Permissionless Innovation*, CATO INST. (Nov. 17, 2014), https://www.cato.org/publications/cato-online-forum/embracing-culture-permissionless-innovation ("[I]f there was one thing every policymaker could do to help advance long-term growth, it is to first commit themselves to advancing [permissionless innovation].").

120. *See generally* DEIRDRE MCCLOSKEY, BOURGEOIS EQUALITY: HOW IDEAS, NOT CAPITAL OR INSTITUTIONS, ENRICHED THE WORLD xxxiv (2016) (describing the significant impact technological

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 prefer privacy approaches that permit greater information flows and more innovation.[121] And in any case, we ought to consider the impact of any approach on innovation.[122]

We can best compare the different privacy approaches' effects on innovation by estimating where they fall on the spectrum between perfectly permissionless and perfectly permissioned.[123] A permissionless approach is one where the developer of the product or service does not have to seek permission, certification, or other authorization.[124] Regulators evaluate the service by the outcome or likely outcome, not by the process used to produce the result.[125]

By contrast, a permissioned approach is one where innovators must seek and receive government approval to pursue an innovation, or where the government sets out a specific process that innovators must follow.[126] If a company fails to follow the specified procedures, it may be found to violate the law even if its practices benefit consumers.[127] Furthermore, a company that follows the specified procedure can escape liability even if consumers are injured.[128]

Permissionless approaches enable a wider range of potential innovations, including completely unforeseen approaches.[129] Permissioned approaches narrow innovation options, often requiring innovators to fit a new service into a pre-existing framework and established processes.[130] This narrowing does the greatest harm in fields where innovation would otherwise be rapid,

innovation has on the development of modern society).

121. *See* Thierer, *supra* note 28, at 33.

122. *Id.* at 20.

123. *See* Thierer, *supra* note 119 (describing the significance of a permissionless innovation system promoted by the government).

124. *Id.* For an expanded definition of "permissionless" versus "permissioned" approaches, see *id.* In that article, Thierer distinguishes between precautionary and permissionless regulatory approaches and describes how a permissionless approach drove enormous innovation in the U.S. information technology sector. *Id.*

125. *See* Thierer, *supra* note 28, at 87.

126. *Id.* at 106.

127. *Id.*

128. *Id.* at 14, 122.

129. *Id.* at 9, 106 (describing the freedom of creativity that stems from permissionless innovation).

130. *Id.* at 28, 106 (defining the precautionary principle).

unpredictable, and disruptive.[131]

The types of tools that could address privacy concerns rank from "most permissionless" to "least permissionless" as follows[132]:

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

Again, many of these restrictions overlap and interact.[133] For example, some legislative actions are more permissionless than others, depending on how much space they leave or create for higher-level solutions.[134] 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 agreements.[135]

Avoid approaches or language that reinforce the idea that consumers *own* all data about them.[136] The ownership/property metaphor does not work well for much information about a consumer—such as their interaction with a company website, their path through a retail store, or their conversation with a clerk.[137] In such cases, the information, if "owned" at all, is arguably jointly

131. *Id.* at 26, 34 (contrasting the precautionary principle's structured and control-centered approach against permissionless innovation's rapid and unpredictable approach).

132. *Id.* at 107.

133. *See id.*

134. *See id.* (finding guidance documents as a more permissionless leaning legislative action as opposed to censorship, information suppression, and product bans, which are more precautionary).

135. *See* Solove & Hartzog, *supra* note 2, at 619, 626.

136. *See* J. Howard Beales III & Timothy J. Muris, *Privacy and Consumer Control* 1–11 (George Mason Univ. Law & Econ. Research Paper Series No. 19–27, 2019), https://ssrn.com/abstract=3449242.

137. Larry Downes, *A Rational Response to the Privacy "Crisis,"* CATO INST. (Jan. 7, 2013), https://www.cato.org/publications/policy-analysis/rational-response-privacy-crisis (arguing that treating jointly created information as the property of one party would create inherent issues).

or publicly owned.[138] Assigning sole ownership rights to jointly produced or public information is inefficient, impractical, and in tension with the First Amendment rights of others.[139]

Maintain a clear distinction between privacy and data security.[140] These are very different problems that need different solutions.[141] In many ways, data security is the narrower and simpler problem.[142] For example, people generally agree that we do not want consumer information lost or stolen in a breach, although people disagree over how to best avoid or deter that negative outcome.[143] But in privacy, there isn't an outcome that everyone agrees is good or bad.[144] 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.[145] Others believe consumers will be better off if companies have broad freedom to collect and use data.[146] To best tackle these problems, privacy and data security ought to

138. *See id.*

139. Bambauer, *supra* note 77, at 118; Beales & Muris, *supra* note 136, at 1–5 (arguing against property rights for personal information.).

140. *See The Difference Between Security and Privacy and Why it Matters to Your Program*, HIV.GOV (Apr. 26, 2018), https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program.

141. *See* Rick Robinson, *Data Privacy vs. Data Protection*, IPSWITCH (Jan. 30, 2020), https://blog.ipswitch.com/data-privacy-vs-data-protection ("In a nutshell, data protection is about securing data against unauthorized access. Data privacy is about authorized access—who has it and who defines it.").

142. *See id.* (explaining that data security is the protection one puts in place to protect against others' unauthorized access of data while data privacy is more broadly concerned with the extent to which the public can access data).

143. *See* Jeff Sovern, *Opting In, Opting Out, or No Options At All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1057–60 (1999); *see also* Robinson, *supra* note 141 ("The only mode of protection that personal data in transit (not in an armored car) can rely on is encryption, [but] . . . many protection officers in the file transfer security community would tell you that it is a privacy security risk.").

144. *See* Robinson, *supra* note 141 ("With end-to-end encryption, however, the only 'authorized users' . . . with known IP addresses can get through the privacy shield and gain access to the data. That's about as far as technology's services can provide you when it comes to data privacy vs. data protection.").

145. *Online Tracking and Behavioral Profiling*, ELECTRONIC PRIVACY INFO. CTR. https://epic.org/privacy/consumer/online-tracking/ (last visited Feb. 26, 2020) (arguing that current online tracking practices allow companies to gather unnecessary amounts of data on consumers and exploit them for information).

146. Alan McQuinn, *The Detractors are Wrong, Online Ads Add Value*, INFO. TECH. & INNOVATION FOUND. (Dec. 8, 2016), https://itif.org/publications/2016/12/08/detractors-are-wrong-online-ads-add-value (discussing how online tracking benefits consumers in multiple ways).

be addressed separately.[147]

Focus on regulating uses that injure consumers, rather than on restricting collection.[148] Preventing consumer injury is the proper goal of privacy legislation, and legislation should directly pursue that goal.[149] Legislation should set general expectations for outcomes followed by active enforcement.[150] 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.[151]

Focusing on consumer injury also better addresses the cases where sensitive inferences, drawn from non-sensitive data, are used to a consumer's detriment.[152]

Legislation should generally avoid regulating collection practices.[153] Collection itself, unless done deceptively, does not harm consumers.[154] Indeed, much data cannot benefit consumers unless it is collected.[155] Access and collection 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

147. *See* Mark E. Heckman, *The Difference Between Data Security and Privacy*, U.S. CYBERSECURITY MAG. (2017) ("Without a clear understanding of the difference, data security and privacy is often conflated in ambiguous and imprecise policies.").

148. *See* Mark MacCarthy, *It's Time For A Uniform National Privacy Law*, CIO (Aug. 23, 2018), https://www.cio.com/article/3300106/it-s-time-for-a-uniform-national-privacy-law.html.

149. *Id.*; *see also 2019 Consumer Data Privacy Legislation*, NAT'L CONF. OF ST. LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx# (last updated Jan. 3, 2020) [hereinafter *Consumer Data*] (indicating that in 2019, twenty-five states and Puerto Rico introduced bills aimed at regulating the privacy practices of commercial cyber entities).

150. *See* MacCarthy, *supra* note 148; *see also Consumer Data*, *supra* note 149 (identifying twenty-two bills, either signed or pending in California, that delineate data privacy protection standards or proscribed usages of data privacy by commercial cyber entities).

151. *See* MacCarthy, *supra* note 148.

152. Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Opening Keynote at the ABA 2017 Consumer Protection Conference (Feb. 2, 2017), https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf (describing how focusing on harms can address consumer injury in cases where non-sensitive information about a consumer is assembled into a sensitive mosaic about that consumer).

153. *See id.* (suggesting the FTC focus on regulating "matters where consumers are actually injured" as opposed to "speculative injury"); *see also* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 501–03 (2018).

154. *See* Ohlhausen, *supra* note 152.

155. *See* Elvy, *supra* note 153, at 501–03.

employment decisions.[156]

Liability should require a showing of actual or likely consumer injury, with material deception as a *per se* injury.[157] If liability hinges on injury, many of the other details of privacy legislation become less important.[158] 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.[159] If companies can be liable for other unquantifiable "harms," it will be impossible to judge whether the law improves the lives of consumers on balance, even as it imposes costs on businesses and their customers.[160]

Clarify the application of the FTC's unfairness and deception authority, rather than mandate best practices.[161] 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 occur.[162] Penalties ought to be proportional to the harm caused or

156. *See id.* at 487.

157. *See, e.g.*, Aspinall v. Philip Morris Co., 813 N.E.2d 476, 492 (Mass. 2004) (finding that deceptive advertising constituted a per se injury if the deception caused consumers to purchase the product).

158. *See* Ohlhausen, *supra* note 152 ("By focusing on practices that are actually harming or likely to harm consumers, the FTC can best use its limited resources.").

159. Maureen K. Ohlhausen, Former Comm'r, Fed. Trade. Comm'n, Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf (explaining the various types of harm and injury that the Federal Trade Commission can address).

160. *See, e.g.*, Alec Stapp, *GDPR After One Year: Costs and Unintended Consequences*, TRUTH ON MKT. (May 24, 2019), https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/ (summarizing news stories of unintended consequences and compliance costs of the European privacy law); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 754–55, 769 (2018) (acknowledging that "intangible" injuries in the case of data breaches remain difficult to quantify).

161. *See* J. Thomas Rosch, Former Comm'r, Fed. Trade Comm'n, Speech Before the Cal. State Bar: Deceptive and Unfair Acts and Practices Principles: Evolution and Convergence (May 18, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/deceptive-and-unfair-acts-and-practices-principles-evolution-and-convergence/070518evolutionandconvergence_0.pdf.

162. *Id.*; *see also* BECKY CHAO, ERIC NULL & CLAIRE PARK, ENFORCING A NEW PRIVACY LAW 9 (2019), newamerica.org/oti/reports/enforcing-new-privacy-law/ ("The FTC's core Section 5 authority does not define standards for unfairness and deception.").

likely to be caused, but also sufficiently high to deter problematic behavior.[163]

Some might wish to simply mandate the FTC's existing recommended privacy best practices.[164] But doing so would lose the current focus on consumer injury that directs enforcement where it matters most.[165] 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.[166]

Do not give the FTC broad rulemaking authority.[167] Because privacy is such a multi-faceted concept, general rulemaking authority around privacy would be a broad delegation of legislative power that could result in administrative abuses.[168] Rulemaking is a permissioned approach, like legislation—but with less political accountability.[169] To avoid potential abuse, any rulemaking authority should be targeted to specific areas, such as defining substantial consumer injury or sensitive personal information.[170]

163. *See generally* Ginger Zhe Jin & Andrew Stivers, Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics (May 22, 2017) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3006172 (particularly the discussion in Section 5 entitled "Policy Tools and their Economic Consideration").

164. Jessica Rich, *Give the F.T.C. Some Teeth to Guard Our Privacy*, N.Y. TIMES (Aug. 12, 2019), https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html [https://nyti.ms/31FRbzP] (arguing that Congress should allow the FTC to set normative privacy standards for all companies regarding online data use and collection).

165. *See* Ohlhausen, *supra* note 152 ("The FTC should focus enforcement on matters where consumers are injured.").

166. Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57(1) MGMT. SCI. 57, 58 (2011) (arguing that regulations restricting companies' use of consumers' data hinders the ability to create effective online ad campaigns).

167. *See* John Hendel & Christiana Lima, *FTC Chairman Tells Congress: Don't Give Me Too Much Power*, POLITICO (May 8, 2019), https://www.politico.com/story/2019/05/08/ftc-chairman-congress-rulemaking-authority-1418237.

168. *See* Cameron F. Kerry & Daniel J. Weitzner, *Rulemaking and its Discontents: Moving From Principle to Practice in Federal Privacy Legislation*, BROOKINGS (June 5, 2019), https://www.brookings.edu/blog/techtank/2019/06/05/rulemaking-and-its-discontents-moving-from-principle-to-practice-in-federal-privacy-legislation/; *see also* Ohlhausen, *supra* note 152 (acknowledging that although the "FTC must remain able to collect the information we need to enforce the law," they must do so "while reducing the burden on businesses, particularly third parties who are not under investigation").

169. *See* Kerry & Weitzner, *supra* note 168; *see also* Ohlhausen, *supra* note 159 (stating that case-by-case enforcement by the FTC under Section 5 "has worked very well").

170. *See* Ohlhausen, *supra* note 152 (suggesting a "harms-based" approach to privacy).

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.[171] 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.

171. *See Consumer Data*, *supra* note 149 ("Online commerce sites, social media, and mobile devices and applications are becoming an integral part of consumers' lives. They improve consumer access to information and make shopping and purchases faster and easier. Smart home speakers, intelligent personal assistants[,] and other connected devices extend computer networks to everyday items.").

***