THE PURSUIT OF PRIVACY IN A WORLD WHERE INFORMATION CONTROL IS FAILING

ADAM THIERER*

* Senior Research Fellow, Mercatus Center, George Mason University. The author wishes to thank Jerry Brito, Larry Downes, Adam Marcus, and Ryan Radia for helpful feedback on this paper.

INTRODUCTION

Online privacy has become one of the most contentious information policy debates of recent times.[1] Many academics, activist organizations, and average consumers are clamoring for greater privacy protections as they realize it is easier than ever for personal information to be widely shared—whether intended or not.[2] "Targeted" or "behavioral" online advertising and data collection practices are under particularly intense scrutiny.[3] Policymakers at all levels—state, federal, and international—are responding to these concerns with an array of proposals, many of which aim to expand regulation of the Internet, social networking sites, online

1. *See* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 440 (2011). *See generally* Omer Tene, *Privacy: The new generations*, 1 INT'L DATA PRIVACY L. 15 (2011).

2. *See* Nicole A. Ozer, *Putting Online Privacy above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 220–21 (2012) ("Surveys performed over the past decade have consistently shown that a large percentage of the American public is concerned about their online privacy."). Some of these fears may be motivated by ancient animosities toward advertising, which some critics have often decried as manipulative and unnecessary, even though "advertising has an unsuspected power to improve consumer welfare" and "is an efficient and sometimes irreplaceable mechanism for bringing consumers information that would otherwise languish on the sidelines." *See* JOHN E. CALFEE, FEAR OF PERSUASION: A NEW PERSPECTIVE ON ADVERTISING AND REGULATION 96 (1997); Adam Thierer, *Advertising, Commercial Speech, and First Amendment Parity*, 5 CHARLESTON L. REV. 503 (2011).

3. *See generally* Slade Bond, *Doctor Zuckerberg: Or, How I Learned to Stop Worrying and Love Behavioral Advertising*, 20 KAN. J.L. & PUB. POL'Y 129 (2010); Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273 (2012).

advertising and marketing services, data aggregators, and other information technology services.[4]

This Article—which focuses not on privacy rights against the government, but against private actors—cuts against the grain of much modern privacy scholarship by suggesting that expanded regulation is not the most constructive way to go about ensuring greater online privacy. The inherent subjectivity of privacy as a personal and societal value is one reason why expanded regulation is not sensible. Privacy has long been a thorny philosophical and jurisprudential matter; few can agree on its contours or can cite firm constitutional grounding for the rights or restrictions they articulate.[5] Part I discusses some of the normative considerations raised by the debate on privacy right and argues that there may never be a widely accepted, coherent legal standard for privacy rights or harms here in the United States.

This Article does not dwell on that widely acknowledged controversy. Instead, a different complication is introduced here: Legislative and regulatory efforts aimed at protecting privacy must now be seen as an increasingly intractable information control problem. Part II considers the many enforcement challenges that are often ignored when privacy policies are being proposed or formulated. Most of the problems policymakers and average individuals face when it comes to controlling the flow of private information online are similar to the challenges they face when trying to control the free flow of digitalized bits in other information policy contexts, such as online safety, cybersecurity, and digital copyright.

Because it will be exceedingly difficult to devise a fixed legal standard for privacy that will be satisfactory for a diverse citizenry (not all of whom value privacy equally), and because it will be increasingly difficult to enforce that standard even if it can be determined, alternative approaches to privacy protection should be considered. This approach is particularly ap-

---

4. Grant Gross, *US Lawmakers Call for Online, Mobile Privacy Legislation*, PCWORLD, June 19, 2012, http://www.pcworld.com/article/257900/us_lawmakers_call_for_online_mobile_privacy_legislation.html; Edward Wyatt, *F.T.C. and White House Push for Online Privacy Laws*, N.Y. TIMES, May 9, 2012, http://www.nytimes.com/2012/05/10/business/ftc-and-white-house-push-for-online-privacy-laws.html.

5. Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 37 (2002).

propriate here in the United States, which, relative to Europe, places greater significance on both free speech rights and the importance of online commerce and innovation.[6]

This conclusion does not mean that privacy is unimportant or that society is entirely powerless to address it through legal or regulatory means. It does, however, mean that individuals who are highly sensitive about their online privacy will likely need to devise new strategies to shield it as the law will not likely play as great a role due to both normative and practical constraints.

The best way to protect personal privacy in the United States, therefore, is to build on the approach now widely utilized to deal with online child safety concerns, where the role of law has been constrained by similar factors. A so-called "3-E" solution that combines consumer *education*, user *empowerment*, and selective *enforcement* of existing targeted laws and other legal standards (torts, anti-fraud laws, contract law, and so on), has helped society achieve a reasonable balance in terms of addressing online safety while also safeguarding other important values, especially freedom of expression.[7] That does not mean perfect online safety exists, not only because the term means very different things to different people, but because it would be impossible to achieve in the first instance as a result of information control complications. But the "3-E" approach has the advantage of enhancing online safety without sweeping regulations being imposed that could undermine the many benefits information networks and online services offer individuals and society.[8] This same framework can guide online

---

6. TERENCE CRAIG & MARY E. LUDLOFF, PRIVACY AND BIG DATA 17 (2011) ("Put simply, the U.S. system weighs privacy issues through a liberty and free market filter."); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1219 (2004) ("What is at stake are two different core sets of values: On the one hand, a European interest in personal dignity, threatened primarily by the mass media; on the other hand, an American interest in liberty, threatened primarily by the government.").

7. *See* ADAM THIERER, PARENTAL CONTROLS & ONLINE CHILD PROTECTION: A SURVEY OF TOOLS AND METHODS 195 (2009), http://www.pff.org/parentalcontrols/.

8. Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 87–88 (2001) ("Legislating privacy comes at a cost: more notices and forms, higher prices, fewer free services, less convenience, and, often, less security. More broadly, if less tangibly, laws regulating privacy chill the creation of beneficial collective goods and erode social values. Legislated privacy is burdensome for individuals and a dicey proposition for society at large.").

privacy decisions—both at the individual household level and the public policy level.[9]

This Article also discusses the recent actions of the Federal Trade Commission (FTC), which has been increasingly active on privacy issues in recent years.[10] Specifically, in two major recent privacy reports[11] and public statements by agency officials,[12] the FTC has been pushing for industry adoption of a "Do Not Track" mechanism, a browser-based tool that "tells advertisers and other third parties not to follow you around the Internet."[13] Legislative proposals to mandate the creation of "Eraser Buttons" to help users delete their past web histories will also be examined.

The battle over Do Not Track has proven particularly contentious, and its future remains unclear.[14] The struggle over

---

9. *See* Tom W. Bell, *Pornography, Privacy, and Digital Self Help*, 19 J. MARSHALL J. COMPUTER & INFO. L. 133, 133 (2000) ("The same arguments that have helped to strike down statutory limits on Internet speech thought harmful to its readers (because indecent or harmful to minors) argue against enacting new statutory limits on speech thought harmful to its subjects (because within or by commercial entities and about Internet users). In both cases, self help offers Internet users a less restrictive means of preventing the alleged harms caused by free speech than legislation does. In both cases, the alternative offered by digital self help makes regulation by state authorities not only constitutionally suspect but also, from the more general point of view of policy, functionally inferior.").

10. *See, e.g.*, Josh Dreller, *A marketer's guide to the privacy debate*, IMEDIA CONNECTION, Dec. 8, 2011, http://www.imediaconnection.com/content/30629.asp; Alex Howard, *FTC Calls on Congress to enact baseline privacy legislation and more transparency of data brokers*, STRATA, Mar. 27, 2012, http://strata.oreilly.com/2012/03/ftc-calls-on-congress-to-enact.html.

11. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR FOR BUSINESSES AND POLICYMAKERS (2010) [hereinafter FTC PRELIMINARY PRIVACY REPORT], http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter FTC FINAL PRIVACY REPORT], http://ftc.gov/os/2012/03/120326privacyreport.pdf.

12. Sara Forden, *FTC's Leibowitz Foresees Do-Not-Track Privacy Option in 2012*, BLOOMBERG BUSINESSWEEK, Mar. 29, 2012, http://www.businessweek.com/news/2012-03-29/ftc-s-leibowitz-foresees-do-not-track-privacy-option-in-2012; Wyatt, *supra* note 4.

13. Jeff Blagdon, *Do Not Track: an uncertain future for the web's most ambitious privacy initiative*, THE VERGE, Oct. 12, 2012, http://www.theverge.com/2012/10/12/3485590/do-not-track-explained.

14. *See* Kevin J. O'Brien, *Privacy Advocates and Advertisers at Odds Over Web Tracking*, N.Y. TIMES, Oct. 4, 2012, http://www.nytimes.com/2012/10/05/technology/privacy-advocates-and-advertisers-at-odds-over-web-tracking.html?pagewanted=all.

whether to adopt Do Not Track results from both the complex definitional issues pertaining to what constitutes online "tracking,"as well as business-related concerns about how Do Not Track might undermine online sites and services that depend upon advertising and data collection to survive.[15]

This Article will argue that, from a practical enforcement perspective, schemes like Do Not Track and the Eraser Button might have some value at the margin, but neither should be considered a silver-bullet solution to privacy concerns. Only a layered approach built on the "3-E" model can strike a reasonable balance between information sharing, online commerce, and personal privacy in an information marketplace characterized by rapid technological change and constantly evolving social norms.[16]

I. NORMATIVE CONSIDERATIONS: THE CHALLENGE OF DEFINING PRIVACY

A. Privacy and "the Pursuit of Happiness"

Do Americans have a right to privacy, and, if so, what does that right entail? The debate over this question has raged for decades and remains contentious.[17] Most people believe they have *some* privacy rights, even if those rights remain difficult to define and find limited grounding in the plain language of the Constitution. Professor Daniel J. Solove has noted that privacy has long been a "conceptual jungle" and a "concept in disarray."[18] "[T]he attempt to locate the 'essential' or 'core' charac-

15. Berin Szoka, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, FTC PRIVACY ROUNDTABLES, Dec. 7, 2009, http://ftc.gov/os/comments/privacyroundtable/544506-00035.pdf.

16. Rachel O'Connell, *An Evolution in Internet Use*, HUFFPOST TECH, (Oct. 25, 2012, 10:35 AM), http://www.huffingtonpost.co.uk/dr-rachel-oconnell/an-evolution-in-internet-_b_2014499.html?utm_hp_ref=tw ("What is required is a more holistic and balanced approach to educating families as to how to support young children in their use of the Internet—an approach which views the Internet as a positive tool and communicates educational messages to parents, from a parent's perspective, about both the opportunities and challenges that the Internet offers.").

17. *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002).

18. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 196 (2008).

teristics of privacy has led to failure," he says.[19] "Privacy has really ceased to be helpful as a term to guide policy in the United States," argues Professor Woodrow Hartzog, "because privacy means so many different things to so many different people."[20] For these reasons, some scholars, most notably Professor Helen Nissenbaum, have argued that privacy must be thought of in a highly context-specific fashion.[21]

Of course, privacy has always been a highly subjective philosophical concept.[22] It is also a constantly morphing notion that evolves as societal attitudes adjust to new cultural and technological realities.[23] For these reasons, America may never be able to achieve a coherent fixed definition of the term or determine when it constitutes a formal right outside of some narrow contexts.

Even if agreement over the scope of privacy rights proves elusive, however, everyone would likely agree that citizens have the right *to pursue privacy*. In this sense, we might think about the pursuit of privacy the same way we think about the pursuit of happiness. Recall the memorable line from America's Declaration of Independence: "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness."[24]

---

19. *Id.* at 8.

20. Cord Jefferson, *Spies Like Us: We're All Big Brother Now*, GIZMODO, Sept. 27, 2012, http://gizmodo.com/5944980/spies-like-us-were-all-big-brother-now.

21. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); *see also* Cate & Litan, *supra* note 5, at 61 ("A meaningful evaluation of the constitutionality of privacy laws requires that those laws be examined in context—not just the context of other issues and values, but also the specific context in which a constitutional challenge is raised.").

22. *See* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 77 (1998) ("When it comes to privacy, there are many inductive rules, but very few universally accepted axioms."); Cate & Litan, *supra* note 5, at 60 ("[T]he term can mean almost anything to anybody."); Jim Harper, *Understanding Privacy—and the Real Threats to It*, CATO POLICY ANALYSIS, Aug. 4 2004, at 1, www.cato.org/pub_display.php?pub_id=1652 ("Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves."); Betsy Masiello, *Deconstructing the Privacy Experience*, IEEE SECURITY & PRIVACY, July–Aug. 2009, at 678 ("On the social Web, privacy is a global and entirely subjective quality—we each perceive different threats to it.").

23. *See* Cate & Litan, *supra* note 5, at 61 ("The public's expectations of privacy are changing, as are the many influences that shape those expectations, such as technology, law, and experience.").

24. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

Consider the importance of that qualifying phrase—"and the pursuit of"—before the mention of the normative value of happiness. America's Founders obviously felt happiness was an important value, but they did not elevate it to a formal positive right alongside life, liberty, physical property, or even freedom of speech.

This framework provides a useful way of thinking about privacy. Even if we cannot agree whether we have a right to privacy, or what the scope of any particular privacy right should be, the right to pursue it should be as uncontroversial as the right to pursue happiness. In fact, pursing privacy is probably an important element of achieving happiness for most citizens.[25] Almost everyone needs some time and space to be free with their own thoughts or to control personal information or secrets that they value. But that does not make it any easier to define the nature of privacy as a formal legal right, or any easier to enforce it, even if a satisfactory conception of privacy could be crafted to suit every context.

The most stable and widely accepted privacy rights in the United States have long been those that are tethered to unambiguous tangible or physical rights, such as rights in body and property, especially the sanctity of the home.[26] Moreover, these rights have been focused on limiting the power of state actors, not private parties.[27] By contrast, privacy claims premised on intangible or psychological harms have found far less support, and those claims have been particularly limited for private actors relative to the government.[28] All this will likely remain the case for online privacy. Importantly, if privacy is enshrined as a positive right even in narrowly drawn contexts, it imposes obligations on the government to secure that right. These obligations create corre-

25. *See* Harper, *supra* note 22, at 3 ("Only empowered, knowledgeable citizens can formulate and protect true privacy for themselves, just as they individually pursue other conditions, like happiness, piety, or success.").

26. *See* CRAIG & LUDLOFF, *supra* note 6, at 16 ("In general, the American view of privacy is focused on the home and on the person."); Whitman, *supra* note 6, at 1214 ("What matters in America, over the long run, is liberty against the state within the privacy of one's home.").

27. *See* Whitman, *supra* note 6, at 1211 ("Suspicion of the state has always stood at the foundation of American privacy thinking, and American scholarly writing and court doctrine continue to take it for granted that the state is the prime enemy of our privacy.").

28. *See id.* at 1215.

sponding commitments and costs that must be taken into account since government regulation always entails tradeoffs.[29]

Therefore, even as America struggles to reach political consensus over the scope of privacy rights in the information age, it makes sense to find methods and mechanisms—most of which will lie outside of the law—that can help citizens cope with social and technological changes that affect their privacy. Part III will outline some of the ways citizens can pursue and achieve greater personal privacy.

B. On the Problem of "Creepiness" as the Standard of Privacy Harm

Precisely because the scope of privacy rights is so difficult to delimit, defining what constitutes "harm" in the context of information sharing and collection is similarly complicated. Some scholars have attempted to better delineate the nature and scope of privacy harms, but consensus remains elusive.[30] The recent FTC reports offer no clarification on the matter either.[31]

This Part focuses on the problems associated with one particular alleged privacy harm commonly associated with new information technologies and practices: "creepiness." Practically every new information technology launched today is initially labeled "creepy" and creepiness is often the primary (or only) alleged harm that is cited as the basis of much online pri-

---

29. *See* Thomas M. Lenard & Paul H. Rubin, *The FTC and Privacy: We Don't Need No Stinking Data*, THE ANTITRUST SOURCE, Oct. 2012, at 3, http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/oct12_lenard_10_22f.authcheckdam.pdf ("It seems clear that greater privacy protections will involve tradeoffs—costs to Internet businesses, as well as to consumers. The commercial use of online information produces a range of benefits, including advertising targeted to consumers' interests, advertising-supported services (such as email, search engines, and fraud detection), and a reduction in other threats, such as malware and phishing. More privacy, in the current context, means less information available for the marketplace and therefore fewer of these benefits to consumers. Even if the services are still offered, they will be of lower quality as providers will have less money and less data to use in providing services.") (footnotes omitted).

30. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1 (2011); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

31. *See* Lenard & Rubin, *supra* note 29, at 4 ("Neither FTC report contains any data on any harm, however defined. Demonstrating, and to the extent feasible quantifying, harm is important because it can be the starting point for assessing benefits, which are the reduced harms associated with increased privacy protection.").

vacy regulation.[32] Recently, for example, in various filings to the government as well as countless news stories, advocates of expanded privacy regulation have stressed the "creepiness" factor associated with targeted (or behavioral) advertising and the online data collection that makes such ads possible.[33] Concerns about "creepy" uses of wireless geolocation technologies are also increasingly commonplace, even though the public has simultaneously demonstrated an insatiable appetite for these new mobile networks and applications.[34]

Finally, "creepiness" is a common lament heard whenever new social networking sites and services are launched. Jim Adler, Chief Privacy Officer and General Manager of Data Systems at Intelius, notes that "[w]ith increasing volume, 'creepy' has snuck its way in to [sic] the privacy lexicon and become a mainstay in conversations around online sharing and social networking."[35] "How is it possible," he wonders, "that we use the same word to describe Frankenstein and Facebook?"[36]

But why should "creepiness" be the standard by which policymakers judge privacy harms at all? Although there will always be subjective squabbles over what constitutes harm as it

---

32. For example, when "Google Now" was released, the news with greeted with accusations of it being too "creepy." *See* Rebecca Greenfield, *Confirmed: Google's Siri-Esque Personal Assistant Is Creepy*, THE ATLANTIC WIRE, July 2, 2012, http://www.theatlanticwire.com/technology/2012/07/confirmed-googles-siri-esque-personal-assistant-creepy/54117; Evan Selinger, *Why Do We Love To Call New Technologies "Creepy"?*, SLATE, Aug. 22, 2012, http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy_.html. ("Creepy is the go-to term for broadcasting how technology unsettles us."); Jenna Wortham, *Will Google's Personal Assistant Be Creepy or Cool*?, N.Y. TIMES BITS, (June 28, 2012, 8:06 PM), http://bits.blogs.nytimes.com/2012/06/28/will-googles-personal-assistant-be-creepy-or-cool.

33. *See* Peter Suciu, *EPIC Worries Facebook Could Follow You to the Mall*, E-COMMERCE TIMES, Sept. 25, 2012, http://www.ecommercetimes.com/story/EPIC-Worries-Facebook-Could-Follow-You-to-the-Mall-76243.html (noting that many feel that using data from social networking sites like Facebook is "creepy" and makes some feel "uncomfortable").

34. *See* Adam Thierer, *Apple, The iPhone and A Locational Privacy Techno-Panic*, FORBES.COM, May 1, 2011, http://www.forbes.com/sites/adamthierer/2011/05/01/apple-the-iphone-and-a-locational-privacy-techno-panic ("Last week's revelation that Apple iPhones and Google Android-based smart phones were retaining locational information generated howls of protest from privacy advocates and government officials.").

35. Jim Adler, *Creepy Is As Creepy Does*, JIMADLER.ME, Dec. 13, 2011, http://jimadler.me/post/14171086020/creepy-is-as-creepy-does.

36. *Id.*

relates to online privacy, and while many consumers will undoubtedly describe much online marketing and advertising as "creepy,"[37] law must be more concrete than the amorphous "creepiness" standard permits. "Creepiness" is simply too open-ended and subjective, and "creating new privacy rights cannot be justified simply because people feel vague unease."[38] "[C]reepiness isn't necessarily a sign that something is amiss" and "[a]s the history of technology shows, sometimes feelings are out of sync with reasonable responses."[39]

If privacy harm is reduced to "creepiness," or even "annoyance," such an amorphous standard for policy analysis or legal and regulatory action leaves much to the imagination and opens the door to creative theories of harm that may not actually represent true harm at all and could be exploited by those who ignore the complex tradeoffs at work when we attempt to regulate information flows online.[40] "Creepiness" is a hopelessly open-ended, eye-of-the-beholder standard that is no better than an "I-know-it-when-I-see-it" standard for speech regulation: It would provide zero guidance to companies or courts when they are attempting to make privacy determinations. Employing a "creepiness" standard to gauge supposed privacy harm makes economic cost-benefit analysis virtually impossible, as policy considerations become purely about emotion instead of anything empirical.[41] After all, one person's "creepy" could be another's "cool" or "killer" app. Personalized online shopping ex-

---

37. Blase Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising* 5, Carnegie Mellon Univ. CyLab Paper No. CMU-CyLab-12-007, 2012), *available at* http://www.futureofprivacy.org/wp-content/uploads/Smart-Useful-Scary-Creepy.-Perceptions-of-Online-Behavioral-Advertising-.pdf.

38. Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector*, CATO POLICY ANALYSIS, Jan. 22, 1998, at 3, http://www.cato.org/pubs/pas/pa-295.html.

39. Selinger, *supra* note 32.

40. *See* Berin Szoka & Adam Thierer, *Targeted Online Advertising: What's the Harm & Where Are We Heading*?, 16 PROGRESS ON POINT, June 2009, at 3–4.

41. Adam Thierer, *On "Creepiness" as the Standard of Review in Privacy Debates*, TECH. LIBERATION FRONT, Dec. 13, 2011, http://techliberation.com/2011/12/13/0n-creepiness-as-the-standard-of-review-in-privacy-debates/. Here is another way to think about it: There are plenty of people we come in contact with in this world that we might describe as "creepy," but that does not mean they are harmful. Most of us would draw a distinction between creepiness and the potentially harmful nature of various individuals, and likely reserve judgment on the latter question until we had more evidence. That standard is the same one we should use for privacy matters when they are elevated to the level of policy concerns.

periences, for example, might be considered too invasive by some, whereas others might greatly appreciate the benefits associated with tailored recommendations.[42] Indeed, "more often than not, the creepy factor will go away without the need for intervention," notes Larry Downes, because "[o]ver time, consumers either adjust to what is an essentially inert new information use, or act through the market to change the practice."[43]

For example, when Google launched its Gmail service in 2004, it was greeted with hostility by many privacy advocates and some policymakers.[44] Rather than charging some users for more storage or special features, Google paid for the service by showing advertisements next to each email "contextually" targeted to keywords in that email. Some privacy advocates worried that Google was going to "read users' email," however, and pushed for restrictions on such algorithmic contextual targeting.[45] But users enthusiastically embraced Gmail and the service grew rapidly. By the summer of 2012, Google announced that 425 million people were actively using Gmail.[46] Users adapted their privacy expectations to accommodate this new service, which offered them clear benefits (free service, generous storage, and improved search functionality) in exchange for tolerating some targeted advertising.

If creepiness were the standard by which information collection and distribution activities were regulated, it raises the question whether services like Gmail, and the entire commercial Internet for that matter, can continue to exist. Online advertising and data collection are the fuel that powers the modern information economy.[47] If claims of creepiness are converted

---

42. Scott Brave, *Personalization and Privacy*, FORBES.COM, Oct. 22, 2012, http://www.forbes.com/sites/ciocentral/2012/10/22/making-sense-of-online-personalization-and-privacy.

43. Larry Downes, *Customer Intelligence, Privacy, and the 'Creepy Factor,'* HBR BLOG NETWORK (Aug. 15, 2012, 12:00 PM), http://blogs.hbr.org/cs/2012/08/customer_intelligence_privacy.html.

44. *See* Adam Thierer, *Lessons from the Gmail Privacy Scare of 2004*, TECH. LIBERATION FRONT, Mar. 25, 2011, http://techliberation.com/2011/03/25/lessons-from-the-gmail-privacy-scare-of-2004.

45. Letter from Chris Jay Hoofnagle et al. to Bill Lockyer, Att'y Gen. (May 3, 2004), *available at* http://epic.org/privacy/gmail/agltr5_3_04.html.

46. Dante D'Orazio, *Gmail now has 425 million active users*, THE VERGE, June 28, 2012, http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users.

47. *See* Berin Szoka & Adam Thierer, *Online Advertising & User Privacy: Principles to Guide the Debate*, PROGRESS SNAPSHOT, Sept. 2008, at 4.

into actionable legal trumps on commercial online activities, advertising and data collection will no longer be able to sustain online sites and services.[48] As a result, those online services will either need to raise prices significantly (most of them charge nothing today), cut back services, limit further innovation and investment, or go under entirely.[49] Regulation—especially arbitrary regulation of this sort—is not a costless exercise.

C. Increasing Tensions Between Privacy Rights and Online Free Speech

Strong conceptions of privacy rights can also come into conflict with more well-defined and constitutionally protected speech and press rights. This problem will grow more acute if the formal contours of online privacy rights are greatly enhanced, especially if the law comes to treat personal information as property much like copyrighted content.

This tension has long been a fixture of privacy debates. Professor Samuel D. Warren and then-Professor Louis D. Brandeis's famous 1890 *Harvard Law Review* essay *The Right to Privacy*—the law review article that gave birth to modern American privacy law—was heavily influenced by copyright law.[50] Stewart Baker has noted that, "Brandeis wanted to extend common law copyright until it covered everything that can be recorded about an individual. The purpose was to protect the individual from all the new technologies and businesses that had suddenly made it easy to gather and disseminate personal information."[51]

Then-Professor Brandeis and Professor Warren's call for such a regime was driven in part by their desire to control the press. "The press is overstepping in every direction the obvious bounds of propriety and of decency," and "column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle," they argued.[52] So angered

---

48. *See id.*

49. *See* Adam Thierer & Berin Szoka, *The Hidden Benefactor: How Advertising Informs, Educates & Benefits Consumers*, PROGRESS SNAPSHOT, Feb. 2010, at 6.

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

51. STEWART BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 319 (2010).

52. Warren & Brandeis, *supra* note 50, at 196.

were Brandeis and Warren by reports in daily papers of specifics from their own lives[53] that they concluded that, "modern enterprise and invention have, through invasions upon his privacy, subjected [man] to mental pain and distress, far greater than could be inflicted by mere bodily injury."[54] Although it remains unclear how one could have greater "pain and distress" inflicted by words than "by mere bodily injury," as Brandeis and Warren suggested, it follows that they would want fairly draconian controls on free speech and press rights if they felt this strongly about the injury the press could potentially inflict.

Taken to the extreme, however, giving such a notion the force of law would put privacy rights on a direct collision course with the First Amendment, and press rights in particular.[55] For instance, Professor Eugene Volokh has argued that:

> The difficulty is that the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits), whether the communication is "fair" or not.[56]

If privacy rights could trump speech and press rights in the fashion Brandeis and Warren suggested, a journalist would not be allowed to conduct her daily business without fear of running afoul of government regulation. Good reporting requires that journalists gather and report facts, many of a personal nature. If privacy rights were treated like intellectual property, robust privacy rights could trump free speech rights, even when the information being collected or distributed was truthful. Such a situation would raise significant First Amendment

---

53. *See* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 6 (1979).

54. Warren & Brandeis, *supra* note 50, at 196.

55. Cate & Litan, *supra* note 5, at 51 ("[T]o the extent that privacy laws restrict expression, even if that expression is commercial, the First Amendment imposes a considerable burden on the government to demonstrate the need and effectiveness of those laws.").

56. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000) (footnote omitted).

issues,[57] even when mere data collection and dissemination are being undertaken.[58]

This issue may come to the fore if the debate over the so-called "Eraser Button" concept advances here in the United States. In 2011, Representatives Edward Markey and Joe Barton introduced the "Do Not Track Kids Act of 2011," which proposed the expansion of the Children's Online Privacy Protection Act of 1998 (COPPA) and other new regulations aimed at enhancing the privacy of teens online.[59] The Markey-Barton measure also required online operators "to the extent technologically feasible, to implement mechanisms that permit users of the website, service, or application of the operator to erase or otherwise eliminate content that is publicly available through the website, service, or application and contains or displays personal information of children or minors."[60] The hope was that these so-called "Eraser Buttons" could help minors wipe out embarrassing facts they had placed online but later came to regret. The Eraser Button concept was modeled loosely on a similar idea being considered in the European Union, a so-called "right to be forgotten" online.[61]

Though well-intentioned, the Eraser Button concept—like the "right to be forgotten"—raises clear First Amendment issues by limiting the right of others to speak freely or to collect, analyze,

---

57. Others have pushed back against Volokh's assertions and the general argument that the First Amendment poses a significant barrier to expanded privacy regulation. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1506–1523 (2000); Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005); Paul M. Schwartz, Commentary, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000).

58. *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2665–66 (2011) ("An individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way in which the information might be used' or disseminated.") (citing Seattle Times Co. v. Rhinehart, 467 U.S. 20, 32 (1984)).

59. Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong., (2011). The measure also proposed applying Fair Information Practice Principles (FIPPS) to teenagers via a "Digital Marketing Bill of Rights for Teens" and also proposed limits on collection of geolocation information from both children and teens. *Id.* § 5.

60. *Id.* § 7(b).

61. *See* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009); Franz Werro, *The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash*, *in* HAFTUNGSRECHT IM DRITTEN MILLENNIUM [LIABILITY IN THE THIRD MILLENNIUM] 285–300 (Aurelia Colombi Ciacchi et al. eds., 2009).

or redistribute information they find online.[62] For example, individuals might be able to "claim a right to be forgotten or ask to hit the Eraser Button when a journalist or historian pens an article about them," something "[t]hat would be a direct affront to the First Amendment since journalistic freedoms apply even when minors are the subject of reports or histories."[63]

II. ENFORCEMENT COMPLICATIONS: CONTROLLING INFORMATION FLOWS

This Part considers the formidable challenges that await any effort to clamp down on the flow of information on digital networks—even if such regulation is pursued in the name of protecting consumer privacy. The administrative and enforcement burdens associated with modern information control efforts are as important as the normative considerations in play.

Information control has always been complex and costly. That observation was equally true in the era of media and information scarcity, with its physical and analog distribution methods of information dissemination. All things considered, however, the challenge of controlling information in the analog era pales in comparison to the far more formidable challenges governments face in the digital era when they seek to limit information flows.

The movement of binary bits across electronic networks and digital distribution systems creates unique problems for information control efforts, even when that control might be socially desirable.[64] In particular, efforts to control spam, objectionable media content, hate speech, copyrighted content, and even personal information are greatly complicated by five phenomena unique to the Information Age: (1) media and technological

---

62. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten ("[Do Not Track] represents the biggest threat to free speech on the Internet in the coming decade."); Emma Llansó, *Do Not Track for Kids Act: Good Idea Raises Real Challenges*, CTR. FOR DEMOCRACY & TECH., MAY 16, 2011, http://cdt.org/do-not-track-for-kids.

63. Adam Thierer, *Kids, Privacy, Free Speech & the Internet: Finding the Right Balance* 7 (Mercatus Ctr. at George Mason Univ., Working Paper No. 11-32, 2011), *available at* http://mercatus.org/publication/kids-privacy-free-speech-internet.

64. Walker, *supra* note 8, at 88 ("Information flows in subtle and nuanced ways, and well-intentioned regulations can easily go awry. After all, enforcing privacy restricts the free flow of information.").

convergence; (2) decentralized, distributed networking; (3) unprecedented scale of networked communications; (4) an explosion of the overall volume of information; and (5) unprecedented individual information sharing through user-generation of content and self-revelation of data. Each of these phenomena is facilitated by the underlying drivers of the information revolution: digitization, dramatic expansions in computing and processing power (also known as "Moore's Law"[65]), a steady drop in digital storage costs, and the rise of widespread Internet access and ubiquitous mobile devices and access. The ramifications of these practical enforcements considerations for privacy policy are itemized below.[66]

A. Media and Technological Convergence

First, content platforms and information distribution outlets are rapidly converging. Convergence means that information is increasingly being "unbundled" from its traditional distribution platform and can find many paths to consumers.[67] It is now possible to disseminate, retrieve, or consume the same content and information via multiple devices or distribution networks. When copying costs are essentially zero and platforms are abundant, information can flow across communications and media platforms seamlessly and instantly. As such, content flowing over modern digital communication tools and networks can more easily overcome the distribution-based limitations that encumbered content and data dissemination in the past.

For example, a piece of personal information voluntarily uploaded to any site can be reproduced instantaneously on

---

65. "Moore's Law" refers to a statement by Intel co-founder Gordon Moore regarding the rapid pace of semiconductor technology. Moore stated, "The number of transistors and resistors on a chip doubles every 18 months." *Definition of Moore's Law*, PC MAGAZINE ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia_term/0,2542,t=Moores+law&i=47229,00.asp (last visited Jan. 29, 2013).

66. The following Part is adapted from ADAM THIERER, PUBLIC INTEREST COMMENT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, (2011), http://mercatus.org/publication/public-interest-comment-protecting-consumer-privacy-era-rapid-change.

67. HENRY JENKINS, CONVERGENCE CULTURE: WHERE OLD AND NEW MEDIA COLLIDE 2 (2006) (defining convergence as "the flow of content across multiple media platforms, the cooperation between multiple media industries, and the migratory behavior of media audiences who will go almost anywhere in search of the kinds of entertainment experiences they want.").

other blogs, social networking sites (such as Facebook, LinkedIn, or MySpace), and content hosting services, sent to Twitter (where it could be re-Tweeted countless times), or sent directly to many others via e-mail or text messages. The information being transmitted can be reproduced across countless sites in a matter of seconds.

In this way, technological convergence complicates efforts to create effective information control regimes. This has important ramifications for privacy policy, just as it does for other regulatory efforts such as speech controls, copyright policy, and cybersecurity measures.

B. Decentralized, Distributed Networking

Second, information creation, curation, storage, and dissemination are all increasingly highly decentralized and distributed in nature.[68] For example, shutting down a website, blog, or social networking site to control information flows will often be ineffective since the information in question could be hosted in multiple places and might have been copied and reproduced by countless individuals who perpetuate the process by uploading it elsewhere.[69]

By contrast, controlling information in the past could have been accomplished by destroying a printing press, cutting power to a broadcast tower, or confiscating communications devices. While imperfect, such measures—or even less extreme regulatory measures—were often reasonably effective at control-

68. MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 4 (2010) ("[T]he Internet protocols decentralized and distributed participation in and authority over networking and ensured that the decision-making units over network operations are no longer closely aligned with political units.").

69. MANUEL CASTELLS, COMMUNICATION POWER 113 (2009) ("[S]hort of unplugging the Internet, it is difficult to control its networking capabilities because they can always be redirected to a backbone somewhere else on the planet. True, it is possible to block access to some designated sites, but not the trillions of e-mail messages and the millions of web sites in constant process of renewal. . . . [T]he best governments can do to enforce their legislation is to prosecute a few unfortunate culprits who are caught in the act, while millions of others enjoy their merry ride over the web. . . . [W]hile a few of the messengers are punished, the messages go on, most of them surfing the ocean of global, seamless, communication.").

ling information flows.[70] This system, though, was facilitated by the highly centralized nature of those analog-era systems and networks. Because modern digital technologies are far more decentralized and distributed, efforts to centralize information control must necessarily be more complicated than those of the past. Accordingly, hierarchical or top-down regulatory schemes must contend with the atomization of information and its mercurial nature within these modern digital systems.

C. Unprecedented Scale of Networked Communications

Third, in the past, the reach of speech and information was limited by geographic, technological, and cultural or language considerations. Today, by contrast, content and data can flow across the globe at the click of a button as a result of the dramatic expansion of Internet access and broadband connectivity.[71] Commentary and personal information that appears on a blog or social networking site in one corner of the globe is just as visible everywhere else. Offshore hosting of content also makes it harder to know where content originates or is stored.[72] While restrictions by government are certainly still possible, the scale of modern speech and content dissemination greatly complicates government efforts to control information flows.[73]

D. Explosion of the Overall Volume of Information

Fourth, the volume of media and communications activity taking place today also complicates regulatory efforts. There exists vastly more content and communication for regulators to police today than in the past. "Since 1995 the sheer volume of information—personally identifiable and otherwise—that has become digitized and can be cheaply transported around the world has grown by orders of magnitude," notes Larry Dow-

---

70. *See, e.g.*, David Pike, *Censorship in Soviet-Occupied Germany*, *in* THE ESTABLISHMENT OF COMMUNIST REGIMES IN EASTERN EUROPE, 1944–1949, at 217 (Norman Naimark & Leonid Gibianskii eds., 1997).

71. CRAIG & LUDLOFF, *supra* note 6, at 20 ("Data, in and of itself, has no country, respects no law, and travels freely across borders.").

72. HAL ABELSON ET AL., BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 68 (2008) ("The bits are everywhere; there is simply no locking them down, and no one really wants to do that anymore.").

73. TRANSNATIONAL CULTURE IN THE INTERNET AGE 3 (Sean A. Pager & Adam Candeub eds., 2012), ("[T]he Internet has revolutionized scale.").

nes.[74] Professor Milton Mueller concurs, noting: "The sheer volume of transactions and content on the Internet often overwhelms the capacity of traditional governmental processes to respond" to developments in this space.[75]

A February 2011 study by Professors Martin Hilbert and Priscila López of the University of Southern California, calculated "The World's Technological Capacity to Store, Communicate, and Compute Information," and found that in 2007, humankind sent 1.9 zettabytes of information through broadcast technology, such as televisions and GPS.[76] That's equivalent to every person in the world receiving 174 newspapers every day, they claim.[77] A 2010 report by the International Data Corporation also found that "by 2020, our Digital Universe will be 44 times as big as it was in 2009."[78] Finally, the Global Information Industry Center reports that:

> In 2008, Americans consumed information for about 1.3 trillion hours, an average of almost 12 hours per day. Consumption totaled 3.6 zettabytes and 10,845 trillion words, corresponding to 100,500 words and 34 gigabytes for an average person on an average day. A zettabyte is 10 to the 21st power bytes, a million million gigabytes. These estimates are from an analysis of more than 20 different sources of information, from very old (newspapers and books) to very new (portable computer games, satellite radio, and Internet video). Information at work is not included.[79]

This "volume problem" for information control efforts—including privacy controls—will only grow more acute in coming years, especially when the difficulties considered in the next Part are taken into account.

---

74. LARRY DOWNES, THE LAWS OF DISRUPTION: HARNESSING THE NEW FORCES THAT GOVERN LIFE AND BUSINESS IN THE DIGITAL AGE 69 (2009).

75. MUELLER, *supra* note 68, at 4.

76. Martin Hilbert & Priscila López, *The World's Technological Capacity to Store, Communicate, and Compute Information*, SCIENCE, Feb. 10, 2011, at 60, 63 http://annenberg.usc.edu/News%20and%20Events/News/110210Hilbert.aspx.

77. *Id.*

78. JOHN GANTZ & DAVID REINSEL, THE DIGITAL UNIVERSE DECADE–ARE YOU READY? 1 (2010), *available at* http://www.emc.com/collateral/analyst-reports/idc-digital-universe-are-you-ready.pdf.

79. ROGER E. BOHN & JAMES E. SHORT, HOW MUCH INFORMATION? 2009 REPORT ON AMERICAN CONSUMERS 7 (2009, updated 2010), http://hmi.ucsd.edu/howmuchinfo_research_report_consum.php.

E. User-Generated Content and Self-Revelation of Data

Finally, modern digital systems make it increasingly easy for anyone to be a one-person publishing house or self-broadcaster. As such, restrictions on information sharing, aggregation, and reuse will become increasingly difficult to devise and enforce.[80] This phenomenon is particularly relevant to any discussion of privacy regulation, as individuals are currently placing massive volumes of personal information online—both about themselves and others. "We live in what one might call the Peeping Tom society," argues Professor Lawrence M. Friedman, in that "[n]ew technology puts powerful tools for invading privacy into the hands of ordinary people."[81] The rapid rise of data self-revelation leads many scholars to puzzle about the existence of a so-called "privacy paradox," which refers to the fact that "[p]eople value their privacy, but then go out of their way to give it up."[82]

Regardless, slowing such information flows through public policy will be remarkably challenging because many people continue to voluntarily release and widely distribute their personal information. Moreover, because of the highly connected nature of social networks and the sheer volume of information sharing that takes place across them, absolute privacy control becomes an impossible task. For example, in 2011, Facebook reported that its users submitted around 650,000 comments on the 100 million pieces of content served up *every minute* on its site.[83] And Hilbert and López found that humankind shared 65 exabytes of information in 2007,[84] the equivalent of every person in the world sending out the contents of six newspapers every day, they es-

---

80. YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 4 (2006) ("The material requirements for effective information production and communication are now owned by numbers of individuals several orders of magnitude larger than the number of owners of the basic means of information production and exchange a mere two decades ago. . . . Individuals can reach and inform or edify millions around the world. Such a reach was simply unavailable to diversely motivated individuals before . . . .").

81. LAWRENCE M. FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY 259, 269 (2007).

82. DOWNES, *supra note* 74, at 79.

83. Ken Deeter, *Live Commenting: Behind the Scenes*, FACEBOOK ENGINEERING'S NOTES (Feb. 7, 2011, 1:00 PM), http://www.facebook.com/note.php?note_id=496077348919.

84. Hilbert & López, *supra* note 76, at 63.

timate.[85] Not all of that shared information was personal information, of course, but much of it probably was.

This problem will be exacerbated by the increasing ubiquity of mobile computing and communications devices that capture and reproduce information instantaneously.[86] For example, most adults and many teenagers today carry a powerful digital sensor or surveillance technology with them at all times: their mobile phones.[87] Individuals use these technologies to record audio and video of themselves and the world around them and instantaneously share that data with many others. They also use geolocation technologies to pinpoint the movement of themselves and others in real time.[88]

Meanwhile, new digital translation tools and biometric technologies are becoming widely available to consumers. Tools such as Google Goggles, available for many smartphones, let users snap pictures of anything they see and have it identified by Google's search engine, with the results provided almost instantly to the user.[89] Eventually, these technologies will merge with "wearable computing" technologies that will, for example, let the buttons on our shirts feed live streams of our daily movements and interactions into social networking sites and databases.[90] Peo-

---

85. *Id.*

86. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 221 (2008) ("Cheap sensors generatively wired to cheap networks with cheap processors are transforming the nature of privacy.").

87. JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 62 (2008) ("Young people are turning to mobile devices in droves. They use them to post more information about themselves and their friends into the ether."); Jennifer Valentino-DeVries, *The Economics of Surveillance*, WALL ST. J. DIGITS BLOG (Sept. 28, 2012, 10:30 PM), http://blogs.wsj.com/digits/2012/09/28/the-economics-of=surveillance/?mod=WSJBlog (quoting Col. Lisa Shay, a professor of electrical engineering at the U.S. Military Academy at West Point, who notes that "nowadays cellphones are sensors," and "you're now carrying a personal sensor with you at all times").

88. *See, e.g.*, *About Foursquare*, FOURSQUARE.COM, https://foursquare.com/about/ (last visited Jan. 30, 2013) ("Foursquare is a free app that helps you and your friends make the most of where you are. When you're out and about, use Foursquare to share and save the places you visit. And, when you're looking for inspiration for what to do next, we'll give you personalized recommendations and deals based on where you, your friends, and people with your tastes have been.").

89. *Google Goggles*, GOOGLE, http://www.google.com/mobile/goggles/#text (last visited Jan. 30, 2013).

90. *See, e.g.*, *Memoto Lifelogging Camera*, MEMOTO, http://memoto.com (last visited Jan. 30, 2013) ("The Memoto camera is a tiny camera and GPS that you clip on and wear. It's an entirely new kind of digital camera with no controls. Instead, it

ple will use such tools to record their lives and play them back later, or perhaps just to instantly scan and recognize faces, items, and places in case they want to remember them later.

Such technologies and ubiquitous information-sharing activities are growing rapidly and will become increasingly commonplace throughout society. As a result, mountains of intimate data will be created, collected, collated, and cataloged about us, and by us, on a daily basis.[91] In other words, "[i]t's not the government spying on all the citizens, it's the citizens themselves."[92]

When combined with the other four factors discussed above, the unprecedented individual information sharing and user-generation of content makes information control efforts—especially privacy control efforts—significantly more difficult. Digital marketing professional Bhavishya Kanjhan notes that increasingly it is "the action of a user rendering . . . privacy controls ineffective. The human element is the weakest link in the chain."[93]

F. Synthesis: Information Wants to Be Free (Even When We Don't Want it to Be)

Taken together, the end result of these five phenomena is that "[o]nce information is out there, it is very hard to keep track of who has it and what he has done with it."[94] The unsettling reality for privacy in the information age is that, as Steward Brand once famously said, "information wants to be free"

---

automatically takes photos as you go. The Memoto app then seamlessly and effortlessly organizes them for you. . . . As long as you wear the camera, it is constantly taking pictures. It takes two geotagged photos a minute with recorded orientation so that the app can show them upright no matter how you are wearing the camera. . . . The camera and the app work together to give you pictures of every single moment of your life, complete with information on when you took it and where you were. This means that you can revisit any moment of your past.").

91. ZITTRAIN, *supra* note 84, at 221. ("The central problem is that the organizations creating, maintaining, using, and disseminating records of identifiable personal data are no longer just 'organizations'—they are people who take pictures and stream them online, who blog about their reactions to a lecture or a class or a meal, and who share on social sites rich descriptions of their friends and interactions. These databases are becoming as powerful as the ones large institutions populate and centrally define.").

92. Jefferson, *supra* note 20.

93. Bhavishya Kanjhan, *Online privacy is dead and it is a good thing*, SOC. MEDIA TODAY, June 14, 2010, http://socialmediatoday.com/index.php?q=SMC/206725.

94. DAVID D. FRIEDMAN, FUTURE IMPERFECT: TECHNOLOGY AND FREEDOM IN AN UNCERTAIN WORLD 62 (2008).

and that is at least partly due to the fact that "the cost of getting it out is getting lower and lower all the time."[95]

Only recently have individuals begun to realize that this insight applies to *all* types of information flows. Though they might have appreciated the implications of this truism in other contexts, where many wanted digitized data to flow freely, they are only beginning to understand the uncomfortable reality of what it means for efforts to control their own information. "When this idea was applied to online music sharing, it was cool in a 'fight the man!' kind of way," says computer scientist Ben Adida.[96] "Unfortunately, information replication doesn't discriminate: your *personal data*, credit cards and medical problems alike, also want to be free. Keeping it secret is really, really hard," he notes.[97] Again, this observation holds for all classes of information—intellectual property, pornography, hate speech, state secrets, and even personal information.

As Konstantinos Stylianou argues, "there are indeed technologies so disruptive that by their very nature they cause a certain change *regardless* of other factors," and the Internet is one of them.[98] Compared to previous communications technologies, the Internet is qualitatively different from the telegraph, the telephone, the radio, and the television. It is innately resistant to control in a way that those previous technologies were not, and that reality must be factored into public policy considerations. "As a result, the cat-and-mouse chase game between the law and technology will probably always tip in favor of technology. It may thus be a wise choice for the law to stop underestimating the dynamics of technology, and instead adapt to embrace it."[99] Observes science journalist Matt Ridley, "[t]he implication is

95. Roger Clarke, *Information Wants to be Free*, ROGERCLARKE.COM, http://www.rogerclarke.com/II/IWtbF.html (last visited Jan. 30, 2013).

96. Ben Adida, *(your) information wants to be free*, BENLOG (Apr. 28, 2011, 12:46 AM), http://benlog.com/articles/2011/04/28/your-information-wants-to-be-free.

97. *Id.*

98. Konstantinos K. Stylianou, *Hasta La Vista Privacy, or How Technology Terminated Privacy*, *in* PERSONAL DATA PRIVACY AND PROTECTION IN A SURVEILLANCE ERA: TECHNOLOGIES AND PRACTICES 44, 46 (Christina Akrivopoulou & Athanasios-Efstratios Psygkas eds., 2011).

99. *Id*. at 54.

that, short of arresting half the planet's people, we could not stop the march of technology even if we wanted to."[100]

G. Corollary: "Silver-Bullet" Solutions Won't Work

In light of these information control considerations, seeking a simple solution to a complex problem such as online privacy protection is quixotic. In this sense, the Do Not Track and Eraser Button schemes fall into a long line of proposed silver-bullet or "universal" solutions to complicated technological problems.

When it comes to such information control efforts, there are not many good examples of simple fixes or silver-bullet solutions that have been effective, at least not for very long. Consider the elusive search for a universal solution to controlling access to online pornography. The experience of the World Wide Web Consortium's (W3C) Platform for Internet Content Selection (PICS)[101] and the Internet Content Rating Association (ICRA)[102] is instructive in this regard. Around the turn of the century, there was hope that voluntary metadata tagging and content labeling could be used to screen objectionable content on the Internet,[103] but the sheer volume of material to be dealt with made that task almost impossible.[104] The effort was eventually abandoned.[105] Of course, the effort did not have a government mandate behind it to encourage more widespread adoption, but even if it had, it is hard to believe that all pornog-

---

100. Matt Ridley, *Why Can't Things Get Better Faster (or Slower)?*, WALL ST. J., Oct. 19, 2012, http://online.wsj.com/article/SB10000872396390443854204578058720488396776.html.

101. *PICS Frequently Asked Questions (FAQ)*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/2000/03/PICS-FAQ/ (last visited Jan. 30, 2013).

102. *About ICRA*, FAMILY ONLINE SAFETY INST., http://www.fosi.org/icra (last visited Jan. 30, 2013).

103. *See, e.g.*, Joris Evers, *Net labels mean choice, not censorship*, PC ADVISOR, Oct. 23, 2001, http://www.pcadvisor.co.uk/news/desktop-pc/1646/net-labels-mean-choice-not-censorship/.

104. *See* PHIL ARCHER, ICRAFAIL: A LESSON FOR THE FUTURE 9 (2009), philarcher.org/icra/ICRAfail.pdf ("The problem with a safety system that has a label at one end and a filter at the other is that unlabelled sites can only be treated as a single group, i.e. you either block them all or allow them all. Since the number of labelled sites was very small, blocking all unlabelled sites would effectively shut off most of the Web.").

105. FAMILY ONLINE SAFETY INST., http://www.icra.org (last visited Nov. 30, 2012).

raphy or other objectionable content would have properly been labeled and screened.

In a similar way, the CAN-SPAM Act[106] aimed to curtail the flow of unsolicited email across digital systems, yet failed to do so. Private filtering efforts have helped stem the flow to some extent, but have not eliminated the problem altogether. Royal Pingdom estimates that in 2010, 89.1% of all e-mails were spam.[107] "Spam pages" are also a growing concern.[108] In January 2011, Blekko, a new search engine provider, created a "Spam Clock" to track new spam pages and found one million new spam pages were being created *every hour*.[109]

Similar problems await information control efforts in the privacy realm, even if a mandated Do Not Track mechanism required the reengineering of web browser architecture or standards or both.[110] Also, Do Not Track "does not address mobile or app data, nor any data created outside a traditional web browser," notes Michael Fertik, CEO of Reputation.com.[111] "At the same time, the growth in technology and understanding can render current solutions inadequate. A privacy rule to limit behavioral advertising today might not work in the future when more data is available and there are more powerful algorithms to process it," he says.[112] "There is no reliable way of ensuring this technology is being used," says Sidney Hill of *Tech*

106. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at various sections of 15 and 18 U.S.C.).

107. *Internet 2010 in Numbers*, ROYAL PINGDOM, Jan. 12, 2011, http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers.

108. Spam pages are "useless pages that contain only a nugget of relevancy to your query and are slathered in ads." Caleb Johnson, *Spam Clock Claims 1 Million Spam Pages are Created Every Hour*, Jan. 10, 2011, SWITCHED.COM, http://switched.com/2011/01/10/blekko-spam-clock-1-million-pages-an-hour/.

109. SPAMCLOCK, http://www.spamclock.com (last visited Jan. 30, 2013); *see also* Danny Sullivan, *Blekko Launches Spam Clock To Keep Pressure On Google*, SEARCH ENGINE LAND.COM, Jan. 7, 2011, http://searchengineland.com/blekko-launches-spam-clock-to-keep-pressure-on-google-60634.

110. Steve DelBianco & Braden Cox, *NetChoice Reply Comments on Department of Commerce Green Paper* (Jan. 28, 2011), *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=1EA98542-23A4-4822-BECD-143CD23BB5E9 ("It's a single response to an overly-simplified set of choices we encounter on the web.").

111. Michael Fertik, *Comments of Reputation.com, Inc. to the U.S. Department of Commerce* (Jan. 28, 2011), *available at* http://www.reputation.com/blog/2011/01/31/reputation-com-comments-commerce-department-privacy-green-paper.

112. *Id.*

News World.[113] "Ensuring compliance with antitracking rules will become even more difficult as more users turn to mobile devices as their primary means of connecting to the Web."[114]

Importantly, Do Not Track would not slow the "arms race" in this arena as some have suggested.[115] If anything, a Do Not Track mandate will speed up that arms race and have many other unintended consequences.[116] Complex definitional questions also remain unanswered, such as how to define and then limit "tracking" in various contexts.[117]

In sum, in light of the global, borderless nature of online speech and data flows, the Do Not Track and Eraser Button schemes likely will not be effective.[118] The regulatory experience with spam, objectionable content, and copyrighted content suggests serious challenges lie ahead for top-down regulatory efforts.

---

113. Sidney Hill, *Internet Tracking May Not Be Worth the Headaches*, TECH NEWS WORLD, Dec. 29, 2010, http://www.technewsworld.com/story/Internet-Tracking-May-Not-Be-Worth-the-Headaches-71543.html.

114. *Id.*

115. *See* Rainey Reitman, *Mozilla Leads the Way on Do Not Track*, ELEC. FRONTIER FUND, Jan. 24, 2011, https://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track ("The header-based Do Not Track system appeals because it calls for an armistice in the arms race of online tracking."); Christopher Soghoian, *What the US government can do to encourage Do Not Track*, SLIGHT PARANOIA, Jan. 27, 2011, http://paranoia.dubfire.net/2011/01/what-us-government-can-do-to-encourage.html. ("[O]pt out mechanisms . . . [could] finally free us from this cycle of arms races, in which advertising networks innovate around the latest browser privacy control.").

116. ABELSON ET AL., *supra* note 72, at 159 ("Too often, well-intentioned efforts to regulate technology are far worse than the imagined evils they were intended to prevent.").

117. Lauren Weinstein, *Risks in Mozilla's Proposed Firefox "Do Not Track" Header Thingy*, LAUREN WEINSTEIN'S BLOG (Jan. 24, 2010, 12:09 AM), http://lauren.vortex.com/archive/000803.html.

118. "Many behavioral targeting companies are based outside the US—making legislation ineffective," says Doug Wolfgram, CEO of IntelliProtect, an online privacy management company. Tony Bradley, *Why Browser 'Do Not Track' Features Will Not Work*, COMPUTERWORLD, Feb. 10, 2011, http://news.idg.no/cw/art.cfm?id=ACE91A0E-1A64-6A71-CE2572C981C0204A; DANIEL CASTRO, POLICYMAKERS SHOULD OPT OUT OF "DO NOT TRACK" 1, 3 (2010), www.itif.org/files/2010-do-not-track.pdf ("Another problem with Do Not Track is that it does not scale well on the global Internet. . . . [T]o be effective, the proposal would require a federal mandate calling for substantive modifications to networking protocols, web browsers, software applications and other Internet devices. Besides raising costs for consumers, it is unclear how effective such a mandate would be outside of the U.S. borders or how well the proposal would be received by international standard bodies.").

III. CONSTRUCTIVE SOLUTIONS

If the effectiveness of law and regulation is limited by the normative considerations discussed in Part I and the practical enforcement complications discussed in Part II, what alternatives remain to assist privacy-sensitive individuals? The approach America has adopted to deal with concerns about objectionable online speech and child safety offers a path forward.

The current debate over protecting online privacy shares much in common with the debate that has taken place over the past two decades about ensuring greater child safety online. First, the same debates over the scope of rights and harms have raged for decades in the child safety context.[119] Specifically, the definitions of indecency, obscenity, hate speech, harassment, and excessively violent content have been bogged down in subjective political squabbles[120] and endless First Amendment-related court battles over the constitutionality of regulatory enactments.[121] At the same time, enforcement challenges in the online safety context have multiplied rapidly.[122] Because of these two factors, legal and regulatory efforts aimed at limiting the flow of objectionable content have proven largely futile.[123]

Lacking solutions that were practical or could achieve political or judicial consensus, a variety of less restrictive alternatives have developed both on the child safety and privacy fronts. These alternatives can be labeled the "3-E Approach," which refers to *education*, *empowerment*, and targeted *enforcement* of existing legal standards. In the online safety context, I have documented how this framework works at much greater length elsewhere.[124]

Compared to the more top-down regulatory proposals being considered today, the 3-E Approach is more bottom-up, multi-

---

119. *See* Robert Corn-Revere, *Moral Panics, the First Amendment, and the Limits of Social Science*, 28 COMM. LAW. 1 (2011).

120. *See* Margaret A. Blanchard, *The American Urge to Censor: Freedom of Expression Versus the Desire to Sanitize Society—From Anthony Comstock to 2 Live Crew*, 33 WM. & MARY L. REV. 741, 848 (1992).

121. *See* Adam Thierer, *Why Regulate Broadcasting? Toward a Consistent First Amendment Standard for the Information Age*, 15 COMMLAW CONSPECTUS 431 (2007).

122. COMPUTER SCI. AND TELECOMM. BD., NAT'L RESEARCH COUNCIL, YOUTH, PORNOGRAPHY, AND THE INTERNET 47 (2002).

123. THIERER, *supra* note 7, at 18–20.

124. *Id.*

faceted, and evolutionary in nature.[125] It does not imagine it is possible to craft a single, universal solution to online safety or privacy concerns. It aims instead to create a flexible framework that can help individuals cope with a world of rapidly evolving technological change and constantly shifting social and market norms as they pertain to information sharing.

Importantly, this approach assumes and depends upon a certain amount of personal and parental responsibility in order to be effective. It is not unreasonable to expect privacy-sensitive consumers to exercise some degree of personal responsibility to avoid unwanted content or communications for themselves and their families, just as they must in the context of objectionable content or online child safety.[126] This Part discusses the "3-E" approach in more detail.

A. Education, Awareness and Digital Literacy

As with online child safety, education and media literacy must be the first line of defense in ongoing efforts to better protect personal privacy in the information age. In recent years, many child safety scholars and child development experts have worked to expand traditional online education and media literacy strategies to place the notion of "digital citizenship" at the core of their lessons.[127] Online safety expert Anne Collier defines digital citizenship as "[c]ritical thinking and ethical choices

---

125. ONLINE SAFETY & TECH. WORKING GRP., YOUTH SAFETY ON A LIVING INTERNET 7 (2010) ("Government should avoid rigid, top-down technological mandates and instead enhance funding and encourage collaborative, multifaceted, and multi-stakeholder initiatives and approaches to enhance online safety via innovation and cooperation.").

126. PALFREY & GASSER, *supra* note 87, at 70 ("The person who can do the most to protect her privacy over the long run is the Digital Native herself. She is not in a position to solve the problem completely, but she can sharply mitigate any potential harm through her own behavior. Common sense is the most important aspect of any solution to the privacy problem."); Harper, *supra* note 22, at 5 ("Privacy is not a gift from politicians or an entitlement that can be demanded from government. Privacy is a product of personal responsibility.").

127. Anne Collier, *From users to citizens: How to make digital citizenship relevant*, NET FAMILY NEWS, (Nov. 16, 2009, 2:23 PM), www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html; Larry Magid, *We Need to Rethink Online Safety*, HUFFINGTON POST, Jan. 22, 2010, www.huffingtonpost.com/larry-magid/we-need-to-rethink-online_b_433421.html; Nancy Willard, *Comprehensive Layered Approach to Address Digital Citizenship and Youth Risk Online*, CTR. FOR SAFE & RESPONSIBLE INTERNET USE (2008), *available at* http://digitalcitizen.wikispaces.com/file/view/yrocomprehensiveapproach.pdf.

about the content and impact on oneself, others, and one's community of what one sees, says, and produces with media, devices, and technologies."[128] Common Sense Media, a prominent U.S.-based online safety organization, notes that "[d]igital literacy programs are an essential element of media education and involve basic learning tools and a curriculum in critical thinking and creativity."[129] "Digital Citizenship," the group notes:

> means that kids appreciate their responsibility for their content as well as their actions when using the Internet, cell phones, and other digital media. All of us need to develop and practice safe, legal, and ethical behaviors in the digital media age. Digital Citizenship programs involve educational tools and a basic curriculum for kids, parents, and teachers.[130]

Digital citizenship education can also alleviate anxieties among parents and policymakers about new information technologies.[131]

These same principles and strategies can help us address privacy concerns for both kids and adults. "Again, the solution is critical thinking and digital citizenship," argues online safety expert Larry Magid.[132] "We need educational campaigns that teach kids how to use whatever controls are built-in to the browsers, how to distinguish between advertising and editorial content and how to evaluate whatever information they come across to be able to make informed choices."[133] Teaching kids smarter online hygiene (sensible personal data use) and "Netiquette" (proper behavior toward others) is vital.[134] Children

---

128. Anne Collier, *A definition of digital literacy & citizenship*, NET FAMILY NEWS, (Sept. 15, 2009, 8:04 AM), www.netfamilynews.org/2009/09/definition-of-digital-literacy.html; *see also* Anne Collier, *Literacy for a digital age: Transliteracy or what?*, NET FAMILY NEWS, (Sept. 20, 2012, 4:52 PM), http://www.netfamilynews.org/?p=31427.

129. COMMON SENSE MEDIA, DIGITAL LITERACY AND CITIZENSHIP IN THE 21ST CENTURY: EDUCATING, EMPOWERING, AND PROTECTING AMERICA'S KIDS 1 (2009), www.commonsensemedia.org/sites/default/files/CSM_digital_policy.pdf.

130. *Id.*

131. STEPHEN BALKAM & NANCY GIFFORD, CALMING PARENTAL ANXIETY WHILE EMPOWERING OUR DIGITAL YOUTH (2012), http://www.fosi.org/images/stories/resources/calming-parental-anxiety-while-empowering-our-digital-youth.pdf.

132. Larry Magid, *Digital citizenship & media literacy beat tracking laws & monitoring*, SAFEKIDS.COM, Aug. 29, 2011, http://www.safekids.com/2011/08/29/digital-literacy-critical-thinking-accomplish-more-than-monitoring-tracking-laws.

133. *Id.*

134. Willard, *supra* note 127, at 1–2 (specifying that responsible digital citizens: (1) understand the risks: they know how to avoid getting into risk, detect if they

must be taught the dangers of over-sharing personal information about themselves and others. They can also be encouraged to delete unnecessary online information occasionally.[135]

Corporations and governments can help facilitate digital citizenship. The FTC's "OnGuard Online," a collaborative effort with other federal agencies, represents a savvy approach to raising awareness about various legitimate online threats, including spyware, phishing, laptop security, and identity theft.[136] The agency also has many other data security education initiatives underway.[137] Many companies and trade associations are also taking steps to raise awareness among their users about how they can better protect their privacy and security.[138] Other nonprofit organizations—such as Privacy Rights Clearinghouse[139] and the ACLU of Northern California[140]—offer instructional websites and tips for how privacy-sensitive consumers can take steps to protect their personal information online.

While much of this mentoring will be conducted within schools, digital citizenship ultimately begins at home with parental guidance and mentoring.[141] The empowerment strategies

---

are at risk, and respond effectively, including asking for help; (2) are responsible and ethical: they do not harm others, and they respect the privacy and property of others; (3) pay attention to the wellbeing of others: they make sure their friends and others are safe, and they report concerns to an appropriate adult or site; and, (4) promote online civility and respect).

135. Anne Collier, *'Delete Day': Students putting messages that matter online*, NET FAMILY NEWS, (May 6, 2011, 2:41 PM), http://www.netfamilynews.org/?p=30376.

136. ONGUARDONLINE, http://www.onguardonline.gov (last visited Jan. 20, 2013).

137. *See, e.g.*, *Prepared Statement of the Federal Trade Commission on Data Security Before the H. Comm. on Energy & Commerce, H. Subcomm. on Commerce, Mfg. & Trade*, 112th Cong. 5–7 (2011) (statement of Edith Ramirez, Comm'r, Fed. Trade Comm'n), http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf (describing the agency's educational efforts to address data security concerns.).

138. *Trustworthy Computing Initiative,* MICROSOFT, http://www.microsoft.com/about/twc/en/us/default.aspx (last visited Jan. 30, 2013); *Yahoo! Privacy Center*, YAHOO!, http://info.yahoo.com/privacy/us/yahoo (last visited Jan. 30, 2013); *Privacy Policy*, GOOGLE, http://www.google.com/privacy (last visited Jan. 30, 2013).

139. *Fact Sheets,* PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/privacy-rights-fact-sheets. (last visited Jan. 30, 2013).

140. *It's Time to Demand Your dotRights!*, ACLU OF N. CAL., https://www.aclunc.org/issues/technology/it's_time_to_demand_your_dotrights.shtml (last visited Jan. 30, 2013).

141. O'Connell, *supra* note 16 ("Fostering communication between parents about their children's use of the Internet is an important strategy that will help to normalise [sic] discussion about how to reconcile the conflicting views about the value and the risks associated with Internet use. Empowering parents to educate their children to be able to navigate the Internet in a way that's fun and safe is

discussed in the next Part can supplement, but not replace, those efforts.[142]

B. Empowerment and Self-Regulation

The market for digital "self-help" tools and privacy enhancing technologies (PET) continues to expand rapidly to meet new challenges. These tools can help users block or limit various types of advertising and data collection and also ensure a more anonymous browsing experience. What follows is a brief inventory of the PETs and consumer information already available on the market today:

- The major online search and advertising providers offer "ad preference managers" to help users manage their advertising preferences. Google,[143] Microsoft,[144] and Yahoo![145] all offer easy-to-use opt-out tools and educational webpages that clearly explain to consumers how digital advertising works.[146] Meanwhile, a relatively new search engine, DuckDuckGo, offers an alternative search experience that blocks data collection altogether.[147]

- Major browser providers also offer variations of a "private browsing" mode, which allows users to turn on a stealth browsing mode to avoid data collection and other forms of tracking. This functionality is available as a menu option in Microsoft's Inter-

---

key, as is ensuring they are keeping pace with the rapidly changing patterns of use of technology.").

142. ONLINE SAFETY & TECH. WORKING GRP., *supra* note 125, at 7.

143. *Ads Preferences*, GOOGLE, http://www.google.com/ads/preferences (last visited Jan. 30, 2013).

144. *Ad Choices*, MICROSOFT, http://choice.live.com/Default.aspx and (last visited Jan. 30, 2013); *Personalized Advertising*, MICROSOFT, https://choice.live.com/AdvertisementChoice/Default.aspx. (last visited Jan. 30, 2013).

145. *Ad Interest Manager*, YAHOO!, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html. (last visited Jan. 30, 2013).

146. *Privacy*, MICROSOFT, http://www.microsoft.com/privacy/default.aspx; (last visited Jan. 30, 2013); *Yahoo! Privacy Center*, YAHOO!, http://info.yahoo.com/privacy/us/yahoo; (last visited Jan. 30, 2013); *Privacy Policy*, GOOGLE, http://www.google.com/privacy/ads. (last visited Jan. 30, 2013).

147. *Privacy*, DUCKDUCKGO, http://duckduckgo.com/privacy.html. (last visited Jan. 30, 2013); *see also*, Jennifer Valentino-DeVries, *Can Search Engines Compete on Privacy?*, WALL ST. J. DIGITS BLOG (Jan. 25, 2011, 4:02 PM), http://blogs.wsj.com/digits/2011/01/25/can-search-engines-compete-on-privacy.

net Explorer ("InPrivate Browsing"),[148] Google's Chrome ("Incognito")[149] and Mozilla's Firefox ("Private Browsing").[150] Firefox also has many add-ons available that provide additional privacy-enhancing functionality.[151] "With just a little effort," notes Dennis O'Reilly of *CNET News.com*, "you can set Mozilla Firefox, Microsoft Internet Explorer, and Google Chrome to clear out and block the cookies most online ad networks and other Web trackers rely on to build their valuable user profiles."[152]

- There are also many supplemental tools and add-ons that users can take advantage of to better protect their privacy online by managing cookies, blocking web scripts, and so on. Like the marketplace for parental control technologies, a remarkable amount of innovation continues in the market for privacy empowerment tools, so much so that it is impossible to document all of them here. However, some of the more notable privacy-enhancing tools and services include: Ghostery,[153] NoScript,[154] Cookie Monster,[155] Better Privacy,[156] Track Me Not,[157] Collusion,[158] and the Targeted Advertising Cookie Opt-Out or

148. *InPrivate Browsing*, MICROSOFT, http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/in-private (last visited Jan. 30, 2013).

149. *Incognito mode (browse in private)*, GOOGLE, http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95464 (last visited Jan. 30, 2013).

150. *Private Browsing—Browse the web without saving information about the sites you visit*, MOZILLA, http://support.mozilla.com/en-US/kb/Private%20Browsing (last visited Jan. 30, 2013).

151. *Add-Ons*, MOZILLA, https://addons.mozilla.org/en-US/firefox/tag/incognito (last visited Jan. 30, 2013).

152. Dennis O'Reilly, *Add 'do not track' to Firefox, IE, Google Chrome*, CNETNEWS.COM, Dec. 7, 2010, http://news.cnet.com/8301-13880_3-20024815-68.html.

153. *Ghostery Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/ghostery (last visited Jan. 30, 2013).

154. *No Script Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/noscript (last visited Jan. 30, 2013).

155. *Cookie Monster Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/cookie-monster (last visited Jan. 30, 2013).

156. *BetterPrivacy Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/betterprivacy (last visited Jan. 30, 2013).

157. *TrackMeNot Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/trackmenot (last visited Jan. 30, 2013).

158. *Collusion Add-On*, MOZILLA, http://www.mozilla.org/en-US/collusion (last visited Jan. 30, 2013).

"TACO"[159] (all for Firefox); No More Cookies[160] (for Internet Explorer); Disconnect (for Chrome);[161] AdSweep (for Chrome and Opera);[162] CCleaner[163] (for PCs); and Flush[164] (for Mac). New empowerment solutions are constantly turning up.[165] Many of these tools build around the Do Not Track notion and functionality that the FTC has been encouraging. For example, Reputation.com's new "MyPrivacy" service lets users remove their information from various sites and helps them create the equivalent of a Do Not Track list for over 100 online networks.[166] New tools from Priveazy[167] and Privacyfix[168] offer similar functionality and allow users to adjust privacy settings for several sites and services at once. Finally, online privacy company Abine offers a "Do Not Track Plus," which it claims blocks more than 600 trackers.[169] Abine also sells a "PrivacyWatch" service, which alerts Facebook users to privacy policy changes on the site,[170] as well as a "DeleteMe" service that helps

159. *Targeted Advertising Cookie Opt-Out (TACO) Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/targeted-advertising-cookie-op/ (last visited Jan. 30, 2013).

160. *No More Cookies*, CNET.COM, http://download.cnet.com/No-More-Cookies/3000-2144_4-10449885.html (last visited Jan. 30, 2013).

161. DISCONNECT, https://disconnect.me (last visited Jan. 30, 2013).

162. *AdSweep Add-On*, OPERA, https://addons.opera.com/addons/extensions/details/adsweep/2.0.3-3/?display=en (last visited Jan. 30, 2013).

163. *CCleaner*, PIRIFORM, http://www.piriform.com/ccleaner (last visited Jan. 30, 2013).

164. *Flush*, MACUPDATE, http://www.macupdate.com/app/mac/32994/flush (last visited Jan. 30, 2013).

165. David Gorodyansky, *Web Privacy: Consumers Have More Control Than They Think*, HUFFINGTON POST, Dec. 30, 2010, http://www.huffingtonpost.com/david-gorodyansky/web-privacy-consumers-hav_b_799881.html.

166. *My Privacy*, REPUTATION.COM, http://www.reputation.com/myprivacy (last visited Jan. 30, 2013).

167. PRIVEAZY, https://www.priveazy.com (last visited Jan. 30, 2013).

168. PRIVACYFIX, https://privacyfix.com (last visited Jan. 30, 2013).

169. *Do Not Track Plus*, ABINE, http://www.abine.com/dntdetail.php (last visited Jan. 30, 2013).

170. *PrivacyWatch*, ABINE, http://www.abine.com/privacywatchdetail.php (last visited Jan. 30, 2013).

users erase personal information from various other online sites and services.[171]

- The success of one particular tool, AdBlockPlus, deserves special mention. AdBlockPlus, which lets users blocks advertising on most websites, is the most-downloaded add-on for both the Firefox and Chrome web browsers.[172] As of October 2012, roughly 175 million people had downloaded the Adblock Plus add-on for the Firefox web browser.[173] Incidentally, both Adblock Plus and NoScript, another of the most popular privacy-enhancing downloads for Firefox, support the Do Not Track protocol.[174]

- Finally, pressured by policymakers and privacy advocates, all three of those browser makers (Microsoft,[175] Google,[176] and Mozilla[177]) have now agreed to include some variant of a Do Not Track mechanism or an opt-out registry in their browsers to complement the cookie controls they had already offered. Microsoft has even decided to turn on Do Not Track by default, although it has been a controver-

---

171. *DeleteMe*, ABINE, http://www.abine.com/marketing/landing/index.php (last visited Jan. 30, 2013).

172. ADBLOCKPLUS, https://adblockplus.org/en (last visited Jan. 30, 2013).

173. *Statistics for Adblock Plus Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/adblock-plus./statistics/?last=30 (last visited Jan. 30, 2013).

174. *X-Do-Not-Track support in NoScript*, HACKADEMIX, http://hackademix.net/2010/12/28/x-do-not-track-support-in-noscript (Dec. 28, 2010, 5:31 PM).

175. Dean Hachamovitch, *IE9 and Privacy: Introducing Tracking Protection*, MICROSOFT IE BLOG (Dec. 7, 2010, 1:10 PM), http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx; Dean Hachamovitch, *Update: Effectively Protecting Consumers from Online Tracking*, MICROSOFT IE BLOG (Jan. 25, 2011, 2:43 PM), http://blogs.msdn.com/b/ie/archive/2011/01/25/update-effectively-protecting-consumers-from-online-tracking.aspx.

176. Peter Bright, *Do Not Track support added to Chrome, arriving by the end of the year*, ARS TECHNICA, Sept. 14, 2012, http://arstechnica.com/information-technology/2012/09/do-not-track-support-added-to-chrome-arriving-by-the-end-of-the-year; Sean Harvey & Rajas Moonka, *Keeping your opt-outs*, GOOGLE PUB. POL'Y BLOG (Jan. 24, 2010, 12:00 PM), http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

177. *See* Julia Angwin, *Web Tool On Firefox To Deter Tracking*, WALL ST. J., Jan. 24, 2011, http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html; Stephen Shankland, *Mozilla offers do-not-track tool to thwart ads*, CNET NEWS DEEP TECH, Jan. 24, 2011, http://news.cnet.com/8301-30685_3-20029284-264.html.

> sial move.[178] These developments build on industry-wide efforts by the Network Advertising Initiative and the "Self-Regulatory Program for Online Behavioral Advertising"[179] to make opting out of targeted advertising simpler. The resulting Digital Advertising Alliance is a collaboration among the leading trade associations in the field, including: American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Better Business Bureau, Digital Marketing Association, Interactive Advertising Bureau, and Network Advertising Initiative.[180] Their program uses an "Advertising Option Icon" to highlight a company's use of targeted advertising and gives consumers an easy-to-use opt-out option.[181] It was accompanied by an educational initiative, www.AboutAds.info, which offers consumers information about online advertising.[182] The independent Council of Better Business Bureaus will enforce compliance with the system.[183] Self-regulatory efforts such as these have the added advantage of being more flexible than government regulation, which tends to lock in sub-optimal policies and stifle ongoing innovation.

Again, this survey only scratches the surface of what is available to privacy-sensitive web surfers today.[184] Importantly, this

---

178. Natasha Singer, *Do Not Track? Advertisers Say 'Don't Tread on Us'*, N.Y. TIMES, Oct. 13, 2012, http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html?_r=1&.

179. *Self-Regulatory Program for Online Behavioral Advertising*, DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info (last visited Jan. 30, 2013).

180. Press Release, Network Advertising Initiative, Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data For Online Behavioral Advertising (Oct. 4, 2010) [hereinafter Major Marketing], www.networkadvertising.org/pdfs/Associations104release.pdf.

181. *Id.*

182. *Self-Regulatory Principles*, DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info/principles (last visited Jan. 30, 2013).

183. Major Marketing, *supra* note 180, at 2.

184. There are many other mundane steps that users can take to protect their privacy. *See, e.g.*, Kashmir Hill, *10 Incredibly Simple Things You Should Be Doing To Protect Your Privacy*, FORBES, Aug. 23, 2012, http://www.forbes.com/sites/kashmirhill/2012/08/23/10-incredibly-simple-things-you-should-be-doing-to-protect-your-privacy.

inventory does not include the many different types of digital security tools that exist today.[185]

What these tools and efforts illustrate is a well-functioning marketplace that is constantly evolving to offer consumers greater control over their privacy without upending online markets through onerous top-down regulatory schemes. Policymakers would be hard-pressed to claim any sort of "market failure" exists when such a robust marketplace of empowerment tools exists to serve the needs of privacy-sensitive web surfers.[186]

Importantly, it is vital to realize that most consumers will never take advantage of these empowerment tools, just as the vast majority of parental control technologies go untapped by most families.[187] This is due to a number of factors, most notably that not every individual or household will have the same needs and values as they pertain to either online safety and digital privacy.

Therefore, the fact that not every individual or household uses empowerment tools should not be used as determination of "market failure" or the need for government regulation. Nor should the effort or inconvenience associated with using such tools be viewed as a market failure.[188] What matters is that these tools exist for those who wish to use them, not the actual uptake or usage of those tools or the inconvenience they might pose to daily online activities.

Government officials can take steps to encourage the use of PETs, but it is even more essential that they do not block or

185. Online security and digital privacy are related, but are also distinct in some ways. For example, technically speaking, anti-virus and other anti-malware technologies are considered security tools, but they can also help protect a user's privacy by guarding information she wishes to keep private.

186. Lenard & Rubin, *supra* note 29, at 2 ("The Commission and Staff Reports do not provide a rigorous analysis of whether market failures exist with respect to privacy.").

187. Adam Thierer, *Who Needs Parental Controls? Assessing the Relevant Market for Parental Control Technologies*, PROGRESS ON POINT, Feb. 2009, at 4–6, http://www.pff.org/issuespubs/pops/2009/pop16.5parentalcontrolsmarket.pdf.

188. The Supreme Court has held as much in the context of child safety. *See* United States v. Playboy Entm't Grp., 529 U.S. 803, 824 (2000) ("It is no response that voluntary blocking requires a consumer to take action, or may be inconvenient, or may not go perfectly every time. A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act.").

discourage their use.[189] For example, limitations on encryption technologies or mandates requiring that web surfers use online age verification or identify authentication technologies would undermine user efforts to shield their privacy.[190]

C. On "Simplified" Privacy Policies and Enhanced Notice

Many privacy advocates[191] and the FTC[192] have stressed the benefits of "simplified" privacy policies. The FTC has also complained that "the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[193]

No doubt, more clearly worded privacy and data use policies would be a welcome development. As Google has noted in a filing to the Department of Commerce, "[c]onsumers are ill-served by a regulatory regime that values rote compliance over innovation, or pressures companies to 'overlawyer' their privacy policies and notices or lock in litigation-tested messaging and delivery mechanisms rather than experimenting with new content or new ways to inform and empower consumers."[194] There are other considerations that must also be taken into account when debating privacy policies, however.

First, simply because consumers do not necessarily read or understand every word of a company's privacy policy does not mean a market failure exists. Consider how other disclosure policies or labeling systems work. It is unlikely that consumers read or fully understand every proviso contained in the stacks

---

189. Froomkin, *supra* note 57, at 1529 ("Sometimes overlooked, however, are the ways in which existing law can impose obstacles to PETs. Laws and regulations designed to discourage the spread of cryptography are only the most obvious examples of impediments to privacy-enhancing technology.").

190. Adam Thierer, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, PROGRESS ON POINT, Mar. 2007, at 3, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976936.

191. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543 (2008); Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J. L. SCI. & TECH. 281, 342–47 (2012).

192. FTC PRELIMINARY PRIVACY REPORT, *supra* note 11, at 19, 26, 70.

193. *Id.* at iii.

194. Pablo L. Chavez, *Comments of Google, Inc. to the U.S. Department of Commerce* 7 (Jan. 28, 2010), http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=10FE3003-691B-4E2E-9685-87D7DB413C1D.

of paper placed in front of them when they sign a home mortgage (even with Truth in Lending Act[195] disclosure requirements in place). The same is true for life insurance policies, which are full of incomprehensible provisions and stipulations, even though regulations govern those policies as well. It is also unlikely that consumers read and understand every provision of their car loan or warranty. The same is also true of mandatory Food and Drug Administration disclosures on pharmaceuticals. In each of these cases, far more is at stake for consumers than whatever "risk" they face by not fully comprehending online privacy policies. Accordingly, a certain amount of "rational ignorance" about privacy policies should be expected. Consumers will never be perfectly informed.[196] Although increased notice and transparency should always be encouraged, users value their time and often ignore data collection and privacy policies for a variety of reasons. Increased "simplification" of privacy policies is not going to magically make consumers start reading them or care any more than they currently do about their privacy.

Second, the highly litigious nature of America's legal culture will likely not permit companies to radically simplify their privacy policies. By its very nature, simplification likely entails less specificity about the legal duties and obligations of either party. Consequently, some companies will rightly fear that a move toward more "simplified" privacy policies could open them up to greater legal liability. If policymakers persist in the effort to force the simplification of privacy policies, therefore, they may need to extend some sort of safe harbor provision to site operators for a clearly worded privacy policy that is later subject to litigation because of its lack of specificity. If not, site operators will find themselves in a "damned if you do, damned if you don't" position: Satisfying regulators' desire for simplicity will open them up to attacks by those eager to exploit the lack of specificity inherent in a simplified privacy policy.

Nonetheless, efforts to make privacy policies more comprehensible will continue, as will efforts to institute "privacy by de-

195. Pub. L. 90-321, 82 Stat. 146 (1968).

196. Harper, *supra* note 22, at 4 ("Unfortunately, there is no horn that sounds when consumers are sufficiently aware, or when their preferences are being honored.").

sign."[197] This term refers to efforts by organizations to "embed privacy into the architecture of technologies and practices."[198] There already have been amazing strides made in this regard, and progress—though slow—will continue. "The signs are already beginning to appear," says Ann Cavoukian, who is widely credited with coining the term, that "market leaders are embracing *Privacy by Design*, and are, in turn, reaping the benefits."[199]

The growth of privacy by design efforts reflect a renewed focus on evolving industry self-regulation and codes of conduct, as was discussed in the previous Part. Policymakers and the general public are increasingly demanding that privacy professionals be present in information-gathering institutions and take steps to better safeguard private information flows. The rapidly expanding ranks of the International Association for Privacy Professionals (IAPP) reflects that fact.[200] The IAPP was formed in 2000 and has rapidly grown from just a few hundred members to almost 10,000 members in 70 countries by 2012.[201] Membership was expected to reach 12,000 by the end of 2012.[202] As a result, a growing class of privacy professionals exists throughout the corporate world, as Professors Kenneth A. Bamberger & Deirdre K. Mulligan summarize:

> The individuals managing corporate privacy have an applicant pool of trained professionals to draw from. There is ongoing training, certification, and networking. A community

197. Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L. J. 1409 (2011); Peter Schaar, *Privacy by Design*, 3 IDENTITY INFO. SOC'Y 267 (2010).

198. Ann Cavoukian, *2011: The Decade of Privacy by Design starts now*, ITBUSINESS (Jan. 15, 2011, 6:00 AM), http://blogs.itbusiness.ca/2011/01/2011-the-decade-of-privacy-by-design-starts-now.

199. *Id.*

200. Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 L. & POL'Y 477 (2011); Tene & Polonetsky, *supra* note 191, at 348–49.

201. *About the IAPP*, INT'L ASS'N OF PRIVACY PROF'LS, https://www.privacyassociation.org/about_iapp (last visited Jan. 20, 2013).

202. Deborah M. Todd, *CMU introduces new masters program for technological privacy certification*, PITTSBURGH POST-GAZETTE, Oct. 16, 2012, http://www.post-gazette.com/stories/business/news/cmu-introduces-new-masters-program-for-technological-privacy-certification-657737.

> of corporate privacy managers has emerged. Ready evidence suggests that substantial effort is made to manage privacy.[203]

D. Increased Section 5 Enforcement, Targeted Statutes, and the Common Law

Despite the challenges of enforcing privacy law that were summarized in Part II, regulators and courts will continue to play a role at the margin of this debate.

As noted above, policymakers can encourage the continuous improvement of corporate privacy policies, ensuring that they are accompanied by clearer notice about specific data collection practices, and then hold companies to the promises they make to their customers.[204] As former FTC Commissioner J. Thomas Rosch has argued, "if there is anything wrong with the 'notice' model, it is that we do not enforce it stringently enough."[205] He argues that, "to the extent that privacy notices have been buried, incomplete, or otherwise ineffective—and they have been—the answer is to enhance efforts to enforce the 'notice' model, not to replace it with a new framework."[206]

The agency's broad powers under Section 5 of the Federal Trade Commission Act should be more than adequate to accomplish that task.[207] The FTC's authority to police "unfair and deceptive practices" under Section 5 provides the agency with a remarkably sweeping consumer protection tool to address privacy and data security matters.[208] The FTC has noted that it

---

203. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 260 (2011).

204. PALFREY & GASSER, *supra* note 87, at 73–74. ("The state does need to provide a crucial backstop, and in the United States it already does. If a company says it will do one thing, and it does another, then the Federal Trade Commission can hold the company responsible for its actions.").

205. FTC PRELIMINARY PRIVACY REPORT, *supra* note 11, app. E, at E-6–E-7 (Concurring Statement of Comm'r J. Thomas Rosch).

206. *Id.* app. E, at E-2.

207. Section 5 of the Federal Trade Commission Act prohibits businesses from engaging in "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a); *see also* J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM'N (June 2003), http://www.ftc.gov/speeches/beales/unfair0603.shtm (last visited Oct. 30, 2012).

208. Bamberger & Mulligan, *supra* note 198, at 273 ("[T]he Federal Trade Commission has actively used its broad authority under Section 5 of the FTC Act, which prohibits 'unfair or deceptive practices,' to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices

has already brought and settled many cases involving its Section 5 authority to police privacy and data security matters.[209] In its March 2012 *Protecting Consumer Privacy in an Era of Rapid Change* report, the FTC noted that, using its Section 5 authority and other powers, the agency has carried out many privacy and data security-related actions just since December 2010.[210] Specifically, the Commission reported that it had:

- Brought enforcement actions against Google and Facebook. The orders obtained in these cases require the companies to obtain consumers' affirmative express consent before materially changing certain of their data practices and to adopt strong, company-wide privacy programs that outside auditors will assess for 20 years. These orders will protect the more than one billion Google and Facebook users worldwide.

- Brought enforcement actions against online advertising networks that failed to honor opt outs. The orders in these cases are designed to ensure that when consumers choose to opt out of tracking by advertisers, their choice is effective.

- Brought enforcement actions against mobile applications that violated the Children's Online Privacy Protection Act as well as applications that set default privacy settings in a way that caused consumers to unwittingly share their personal data.

- Brought enforcement actions against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act.

- Brought actions against companies for failure to maintain reasonable data security.[211]

The FTC brought several other privacy and data security-related cases using its Section 5 powers after the 2012 report

---

for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury.").

209. FTC FINAL PRIVACY REPORT, *supra* note 11, at i.

210. *Id.* at ii.

211. *Id.*

was released.[212] In essence, the agency is using its Section 5 powers to hold companies to the privacy and data security promises they make to their consumers. "The net effect of these privacy enforcement actions has been to create a 'common law' of consent decrees that dictates what privacy violations, including data security lapses, constitute a violation of the FTC Act," concludes privacy attorney Christopher Wolf.[213] This has "produc[ed] a set of data protection rules for businesses to follow."[214] The FTC has also issued industry guidance for mobile app data collection and privacy practices[215] as well as facial recognition technologies.[216]

Tort,[217] property,[218] and contract law[219] will also continue to play a role in privacy enforcement and data security. The four privacy torts are public disclosure of private facts, intrusion upon seclusion, false light, and appropriation of name or likeness.[220] Although privacy torts evolved fairly recently com-

---

212. *FTC Finalizes Privacy Settlement with Myspace*, FED. TRADE COMM'N, (Sept. 11, 2012), http://www.ftc.gov/opa/2012/09/myspace.shtm; *FTC Halts Computer Spying*, FED. TRADE COMM'N, (Sept. 25, 2012), http://www.ftc.gov/opa/2012/09/designware.shtm; *Tracking Software Company Settles FTC Charges That it Deceived Consumers and Failed to Safeguard Sensitive Data it Collected*, FED. TRADE COMM'N, (Oct. 22, 2012), http://www.ftc.gov/opa/2012/10/compete.shtm.

213. CHRISTOPHER WOLF, TARGETED ENFORCEMENT AND SHARED LAWMAKING AUTHORITY AS CATALYSTS FOR DATA PROTECTION 7 (2010), http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf.

214. *Id.* at 2.

215. *FTC Publishes Guide to Help Mobile App Developers Observe Truth-in-Advertising, Privacy Principles*, FEDERAL TRADE COMMISSION, (Sept. 5, 2012), http://www.ftc.gov/opa/2012/09/mobileapps.shtm.

216. *FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies*, FEDERAL TRADE COMMISSION, (Oct. 22, 2012), http://www.ftc.gov/opa/2012/10/facialrecognition.shtm.

217. *See* JIM HARPER, THE PRIVACY TORTS: HOW U.S. STATE LAW QUIETLY LEADS THE WAY IN PRIVACY PROTECTION (2002), http://www.privacilla.org/releases/Torts_Report.html.

218. *See* Harper, *supra* note 22, at 3. ("Real property law and the law of trespass mean that people have legal backing when they retreat into their homes, close their doors, and pull their curtains to prevent others from seeing what goes on within.").

219. *See id.* ("Contract law, for example, allows consumers to enter into enforceable agreements that restrict the sharing of information involved in or derived from transactions. Thanks to contract, one person may buy foot powder from another and elicit as part of the deal an enforceable promise never to tell another soul about the purchase.") (footnote omitted).

220. PALFREY & GASSER, *supra* note 87, at 79 ("The law should make it clear what it means for an actor who collects personally identifiable information to be negligent in terms of computer security. Lawyers call this area of the law torts. Com-

pared to other common law torts, it is possible that these privacy torts will continue to evolve in response to technological change in ways that will provide more avenues of recourse to plaintiffs seeking to protect their privacy rights.

State governments and state attorneys general also continue to advance their own privacy policies, and those enforcement efforts are often more stringent than federal law.[221] For example, in July 2012, California Attorney General Kamala D. Harris announced the creation of the Privacy Enforcement and Protection Unit to expand privacy enforcement through civil prosecution of privacy laws.[222] States also have a variety of targeted privacy laws such as data security breach notification rules, "Peeping Tom" statutes, confidentiality laws, and anti-blackmail laws.[223] Again, the effectiveness of many of these laws and regulations are limited by new enforcement challenges, but they continue to play a backstop role that, if nothing else, puts companies on notice about their data policies. There are strong reputational incentives at work here since data breaches or privacy violations can be a major public relations setback for companies handling consumer information.

Not to be forgotten is that fact that the United States, "has a vibrant privacy litigation industry, led by privacy class ac-

---

panies that store information about users should be held to a reasonable standard, under the law, for maintaining the security of their data collection and storage systems. In the event of a data breach, an individual or class of persons should be able to hold companies accountable for the breach. If companies do not meet this reasonable standard for security, they should be held liable."); *see also* FTC PRELIMINARY PRIVACY REPORT, *supra* note 11, app. D, at D-1 (Concurring Statement of Comm'r William E. Kovacic).

221. WOLF, *supra* note 213, at 3. ("At the state level, legislatures have become the proving grounds for new statutory approaches to privacy regulation. Some of these developments include the enactment of data security breach notification laws . . . as well as highly detailed data security laws, enacted largely in response to data breaches. This partnership has resulted in a set of robust standards for the protection of personal data.").

222. Press Release, Cal. Dep't of Justice, Office of the Att'y Gen., Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit (July 19, 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

223. *See, e.g.*, Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, NEB. REV. STAT. ANN. § 87-801 (LexisNexis 2012); Peeping Toms, GA. CODE ANN., § 16-11-61; Confidential communications between husband and wife, W. VA. CODE ANN., § 57-3-4 (LexisNexis 2012); Blackmail; aggravated blackmail; penalties, WYO. STAT. ANN. § 6-2-402 (2012).

tions."[224] Class action lawsuit activity is remarkably intense following major privacy violations or data breaches[225] and there is evidence that "[h]ow federal courts define the damages people suffer from data breaches is broadening dramatically, leaving unprepared companies at greater risk of big payouts in class-action lawsuits."[226] This disciplines firms that violate privacy and data security norms while sending a signal to other online operators about their data policies and procedures.[227]

Meanwhile, other targeted statutes and regulations already exist to address specific privacy or data security concerns. On its website, the FTC itemizes the many privacy laws and consumer protection regulations it already enforces.[228] They include: the Truth in Lending Act,[229] the Fair Credit Billing Act,[230] the Fair Credit Reporting Act of 1970,[231] the Electronic Fund Transfer Act of 1978,[232] the Children's Online Privacy Protection Act (COPPA) of 1998,[233] and the Health Breach Notification Rule (2009),[234]

---

224. Peter Fleischer, *Privacy-litigation: get ready for an avalanche in Europe*, PETER FLEISCHER: PRIVACY . . . ? (Oct. 26, 2012, 10:00 AM), http://peterfleischer.blogspot.com/2012/10/privacy-litigation-get-ready-for.html?m=1.

225. *Id.* ("Within hours of any newspaper headline (accurate or not) alleging any sort of privacy mistake, a race begins among privacy class action lawyers to find a plaintiff and file a class action. Most of these class actions are soon dismissed, or settled as nuisance suits, because most of them fail to be able to demonstrate any 'harm' from the alleged privacy breach. But a small percentage of privacy class actions do result in large transfers of money, first and foremost to the class action lawyers themselves, which is enough to keep the wheels of the litigation-machine turning.").

226. Antone Gonsalves, *Courts widening view of data breach damages, lawyers say*, CSO ONLINE, Oct. 29, 2012, http://www.csoonline.com/article/720128/courts-widening-view-of-data-breach-damages-lawyers-say.

227. For example, in October 2012, the web analytics company KISSmetrics agreed to settle a class-action lawsuit associated with its use of "supercookies," which tracked users online without sufficient notice or choice being given beforehand. The firm agreed to pay each consumer who was part of the suit $2,500. *See* Wendy Davis, *KISSmetrics Settles Supercookies Lawsuit*, ONLINE MEDIA DAILY, Oct. 19, 2012, http://www.mediapost.com/publications/article/185581/kissmetrics-settles-supercookies-lawsuit.html#ixzz2A306a5mq.

228. *See* FED. TRADE COMM'N, ADVERTISING AND MARKETING ON THE INTERNET: RULES OF THE ROAD, (2000), http://business.ftc.gov/documents/bus28-advertising-and-marketing-internet-rules-road; *Legal Resources - Statutes Relating to Consumer Protection Mission*, FED. TRADE COMM'N, http://www.ftc.gov/ogc/stat3.shtm (June 28, 2012).

229. 15 U.S.C. §§ 1601–1667(f) (2006).

230. 15 U.S.C. §§ 1666–1666(j) (2006).

231. 15 U.S.C. §§ 1681–1681(u) (2006).

232. 15 U.S.C. § 1693 (2006).

233. 15 U.S.C. § 6501 (2006).

234. 16 C.F.R. § 318.1 (2012).

among others. Many other federal consumer protection and privacy laws exist and are enforced by other agencies or courts, such as the Cable Communications Policy Act of 1984,[235] the Video Privacy Protection Act of 1998,[236] and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[237]

In sum, a plethora of privacy laws, data security-related statutes, and other consumer protection policies already exist. Before adding new laws and regulations, more focused enforcement efforts should be pursued using existing legal authority, which is already extremely broad in scope. Of course, all of these legal efforts will be encumbered by the enforcement challenges detailed in Part II, meaning that ultimately they will be no substitute for a more educated, empowered, and responsible citizenry.

CONCLUSION

Not every complex social problem can be solved by state action. Many of the thorniest social problems citizens encounter in the information age will be better addressed through efforts that are bottom-up, evolutionary, education-based, empowerment-focused, and resiliency-centered. That framework is the best approach to address personal privacy protection. Evolving social and market norms will also play a role as citizens incorporate new technologies into their lives and business practices. What may seem like a privacy-invasive practice or technology one year might be considered an essential information resource the next.[238] Public policy should embrace—or at least not unnecessarily disrupt—the highly dynamic nature of the modern digital economy.

This approach is even more relevant today when it comes to protecting privacy in an age of ubiquitous sharing and quicksilver information flows. To some extent, the technological genie is out of the bottle and, as uncomfortable as it may be, individuals will need to adjust some of their privacy expectations to account for these new realities. Attempting to put the information genie back in the bottle is impossible absent extreme

---

235. 47 U.S.C. § 551 (2006).

236. 18 U.S.C. § 2710 (2006).

237. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).

238. Downes, *supra* note 43.

steps that would entail massive costs on the free flow of information and technological freedom.[239]

America's privacy regime must, therefore, be flexible and evolutionary—especially if we hope to preserve the many benefits of an economy built on the free flow of information.[240] Regulation—even well-intentioned regulation aimed at preserving privacy—is not a costless exercise.[241]

Whether it is online child safety or online privacy protection, the consistent and principled position can be simply stated: Personal responsibility and user empowerment should be the first-order solution for both these issues. "The state ought not help those who can better help themselves."[242] Governments should only intervene when clear harm can be demonstrated and user empowerment truly proves ineffective. Conjectural fears and hypothetical harms should not drive Internet regulation.[243] Although there are many legitimate online safety privacy concerns today, less restrictive means of dealing with them can be tapped before policymakers consider greatly expanded controls for cyberspace and the information economy.

---

239. L. Gordon Crovitz, *Optimism and the Digital World*, WALL ST. J., Apr. 21, 2008, http://online.wsj.com/article/SB120873501564529841.html ("The uncertainties and dislocations from new technology can be wrenching, but genies don't go back into bottles."); Adam Thierer, *Copyright, Privacy, Property Rights & Information Control: Common Themes, Common Challenges*, TECH. LIBERATION FRONT, Apr. 10, 2012, http://techliberation.com/2012/04/10/copyright-privacy-property-rights-information-control.

240. HOWARD BEALES, THE VALUE OF BEHAVIORAL TARGETING (2011), http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

241. Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, 50 (2000) ("A premature insistence on regulatory control over market approaches to the problem may distort or prevent the evolution of initiatives that produce lower prices, increase convenience, provide more secure records, and foster new and widely beneficial civic and political interchange.").

242. Tom W. Bell, *Free Speech, Strict Scrutiny, and Self-Help: How Technology Upgrades Constitutional Jurisprudence*, 87 MINN. L. REV. 743, 743 (2003).

243. Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309 (2013).