Maine Law Review

Volume 66 | Number 2 Article 6

June 2014

Privacy Law's Precautionary Principle Problem

Adam Thierer

PRIVACY LAW'S PRECAUTIONARY PRINCIPLE PROBLEM

Adam Thierer

I. INTRODUCTION
II. DEALING WITH NEW REALITIES
III. THE PROBLEM WITH PRECAUTIONARY REGULATION
IV. TOWARD SERIOUS BENEFIT-COST ANALYSIS
V. NEW APPROACHES
VI. THE ROLE OF PRIVACY PROFESSIONALS AND THE DIGITAL DESIGNERS OF THE FUTURE
VII. RELIANCE ON NORMS AND SOCIAL PRESSURE WILL EXPAND
VIII. CONCLUSION

PRIVACY LAW'S PRECAUTIONARY PRINCIPLE PROBLEM

Adam Thierer[*]

I. INTRODUCTION

Privacy law today faces two interrelated problems. The first is an *information control problem*. Like so many other fields of modern cyberlaw—intellectual property, online safety, cybersecurity, etc.—privacy law is being challenged by intractable Information Age realities.[1] Specifically, it is easier than ever before for information to circulate freely and harder than ever to bottle it up once it is released.[2]

This has not slowed efforts to fashion new rules aimed at bottling up those information flows. If anything, the pace of privacy-related regulatory proposals has been steadily increasing in recent years even as these information control challenges multiply.[3]

This has led to privacy law's second major problem: *the precautionary principle problem*. The precautionary principle generally holds that new innovations should be curbed or even forbidden until they are proven safe. Fashioning privacy rules based on precautionary principle reasoning necessitates prophylactic regulation that makes new forms of digital innovation guilty until proven innocent.

This puts privacy law on a collision course with the general freedom to innovate that has thus far powered the Internet revolution, and privacy law threatens to limit innovations consumers have come to expect or even raise prices for services consumers currently receive free of charge.[4] As a result, even if new regulations are pursued or imposed, there will likely be formidable push-back not just from affected industries but also from their consumers.

In light of both these information control and precautionary principle problems, new approaches to privacy protection are necessary. We need to invert the process of how we go about protecting privacy by focusing more on practical "bottom-up" solutions—education, empowerment, public and media pressure, social norms and etiquette, industry self-regulation and best practices, and an enhanced role for privacy professionals within organizations—instead of "top-

* Senior Research Fellow, Mercatus Center, George Mason University.

1. 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.

2. Adam Thierer, *When It Comes to Information Control, Everybody Has a Pet Issue & Everyone Will Be Disappointed*, TECH. LIBERATION FRONT (Apr. 29, 2011), http://techliberation.com/2011/04/29/when-it-comes-to-information-control-everybody-has-a-pet-issue-everyone-will-be-disappointed.

3. *See* Kate Kaye, *Privacy Bills: Which One Would Ad Industry Choose*? CLICKZ (May 18, 2011), http://www.clickz.com/clickz/news/2072092/privacy-bills-industry-choose.

4. ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (Arlington, VA: Mercatus Ctr. at George Mason Univ., forthcoming 2014).

down" legalistic solutions and regulatory techno-fixes.[5] Resources expended on top-down regulatory pursuits should instead be put into bottom-up efforts to help citizens better prepare for an uncertain future.

In this regard, policymakers can draw important lessons from the debate over how best to protect children from objectionable online content. In a sense, there is nothing new under the sun; the current debate over privacy protection has many parallels with earlier debates about how best to protect online child safety. Most notably, just as top-down regulatory constraints came to be viewed as constitutionally-suspect and economically inefficient, and also highly unlikely to even be workable in the long-run for protecting online child safety, the same will likely be true for most privacy related regulatory enactments.

This article sketches out some general lessons from those online safety debates and discusses their implications for privacy policy going forward.

II. DEALING WITH NEW REALITIES

Lawmakers and policy advocates who worry about how best to protect online privacy today must contend with the fact that, for better or worse, we now live in a world that is ruthlessly governed by two famous Internet aphorisms.[6] First, "*information wants to be free*."[7] Sometimes that fact is worth celebrating; other times not so much. "Unfortunately," notes computer scientist Ben Adida, "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 correctly notes.[8]

A second well-known Internet aphorism explains why this is the case: "*The Net interprets censorship as damage and routes around it*," as Electronic Frontier Foundation co-founder John Gilmore once noted.[9] Importantly, this insight applies to *all* classes of information and efforts to control information flows, including: copyright policy, cybersecurity, state secrets, pornography, hate speech, or even personal information. In each case, the reality is always the same: any effort to control information flows will be resisted by many other forces or actors throughout the online ecosystem. Moreover, once the genie is out of the bottle, it is incredibly hard to get it back in, and in most cases it is simply impossible.

These two realities are the byproduct of the Internet's decentralized, distributed nature; the unprecedented scale of modern networked communications; the combination of dramatic expansions in computing and processing power (also

5. Adam Thierer, *Let's Not Place All Our Eggs in the Do Not Track Basket*, IAPP: PRIVACY PERSPS. (May 2, 2013), https://www.privacyassociation.org/privacy_perspectives/post/lets_not_place_all_our_eggs_in_the_do_not_track_basket.

6. Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 454 (2013).

7. *Id.* at 431.

8. Ben Adida, *(Your) Information Wants to Be Free*, BENLOG (Apr. 28, 2011), http://benlog.com/articles/2011/04/28/your-information-wants-to-be-free.

9. Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, *available at* http://www.chemie.fu-berlin.de/outerspace/internet-article.html (emphasis added).

known as "Moore's Law")[10] alongside a steady drop in digital storage costs; and the rise of widespread Internet access and ubiquitous mobile devices and service.[11]

Compounding matters further still—especially for efforts to protect privacy—is the fact that we are our own worst enemies when it comes to information containment. Ours is a world of unprecedented individual information sharing through user-generation of content and self-revelation of data.[12] Moreover, decentralized peer-to-peer sharing and surveillance capabilities now exist that make it easier than ever for us to release information not only about ourselves but also about all those around us.[13] Traditional information control mechanisms are being strained to the breaking point in this new environment.[14]

Taken together, the combined effect of these factors should be abundantly clear: law will typically lag well behind both technological and social developments. Technology lawyer and consultant Larry Downes has shown how lawmaking in the information age is inexorably governed by the "law of disruption" or the fact that "technology changes exponentially, but social, economic, and legal systems change incrementally."[15] This law is "a simple but unavoidable principle of modern life," he said, and it will have profound implications for the way businesses, government, and culture evolve. "As the gap between the old world and the new gets wider," he argues, "conflicts between social, economic, political, and legal systems" will intensify and "nothing can stop the chaos that will follow."[16]

---

10. "Moore's Law" refers to a statement by Intel co-founder Gordon Moore regarding the rapid pace of semiconductor technology growth. Moore stated, "[t]he number of transistors and resistors on a chip doubles every 18 months." *Definition of Moore's Law*, PC MAG. ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/47229/moore-s-law (last visited Jan. 17, 2014).

11. I have discussed these factors and their impact on information control efforts at greater length elsewhere. *See, e.g.*, Thierer, *supra* note 6, at 424-35.

12. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1895 (2013) ("[P]eople appear to be sharing data with increasing frequency and magnitude. Most people are not opting out as companies gather and use data. They are exposing the intimate minutiae of their lives on sites like Facebook and Twitter."); Jenna Wortham, *Instagram Direct and the Fracturing of Privacy*, N.Y. TIMES BITS BLOG (Dec. 17, 2013, 8:00 AM), http://bits.blogs.nytimes.com/2013/12/17/instagram-direct-and-the-evolution-of-privacy ("[P]eople spend the vast majority of their time talking to each other through a screen — and it is fun to have new and interesting ways to get in touch with them. At the same time, our notions of privacy are constantly evolving and in many cases, being eroded altogether. As a result, we're learning how to cope by adapting ourselves and our sharing behavior by deciding which version of ourselves to present based on the number of people who will be able to see it.").

13. Francesca Musiani, *Privacy as Invisibility: Pervasive Surveillance and the Privatization of Peer-to-Peer Systems*, 9 TRIPLEC 126, 138 (2011), *available at* http://www.academia.edu/1470476/Privacy_as_Invisibility_Pervasive_Surveillance_and_the_Privatization_of_Peer-to-Peer_Systems.

14. Adam Thierer, *Privacy as an Information Control Regime: The Challenges Ahead*, TECH. LIBERATION FRONT (Nov. 13, 2010), http://techliberation.com/2010/11/13/privacy-as-an-information-control-regime-the-challenges-ahead.

15. LARRY DOWNES, THE LAWS OF DISRUPTION: HARNESSING THE NEW FORCES THAT GOVERN LIFE AND BUSINESS IN THE DIGITAL AGE 2 (2009).

16. *Id.* at 2-3. In a similar sense, Andy Grove, former CEO of Intel, once reportedly said that "[h]igh tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap." Lillian Cunningham, *Google's Eric Schmidt Expounds on His Senate Testimony*, WASH. POST, Oct. 1, 2011, *available at*

III. THE PROBLEM WITH PRECAUTIONARY REGULATION[17]

Despite these new realities, private advocates have stepped up their calls for legislative and regulatory action to address alleged privacy violations.[18] Many of their well-intentioned proposals are premised on "precautionary principle" logic. That is, the privacy and data security-related proposals often rest on the precautionary assumption that "since every technology and technological advance could pose some theoretical danger or risk, public policies should prevent people from using innovations until their developers can prove that they won't cause any harms."[19]

The problem with letting such precautionary thinking guide policy is that it poses a serious threat to technological progress, economic entrepreneurialism, social adaptation, and long-run prosperity.[20] If public policy is guided at every turn by the precautionary principle, technological innovation is impossible because of fear of the unknown; hypothetical worst-case scenarios trump most other considerations.[21] Social learning and economic opportunities become far less likely, perhaps even impossible, under such a regime. Precautionary principle-based reasoning also cuts against the grain of the "permissionless innovation" ethos that has thus far powered the Internet and digital innovation.[22] "In practical terms, therefore, precautionary principle-based regulation means fewer services, lower quality goods, higher prices, diminished economic growth, and a decline in the overall standard of living."[23] Moreover, as will be discussed further below, precautionary principle-based regulation also can take on a paternalistic cast when it denies individuals the right to freely exercise their preferred choices in either economic or social circumstances.

---

http://www.washingtonpost.com/national/on-leadership/googles-eric-schmidt-expounds-on-his-senate-testimony/2011/09/30/gIQAPyVgCL_story.html.

17. Section III is adapted from: ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM, (Arlington, VA: Mercatus Center at George Mason University, 2014); Adam Thierer, *Edith Ramirez's 'Big Data' Speech: Privacy Concerns Prompt Precautionary Principle Thinking,* TECH. LIBERATION FRONT (Aug. 29, 2013), http://techliberation.com/2013/08/29/edith-ramirezs-big-data-speech-privacy-concerns-prompt-precautionary-principle-thinking. *See also* Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON L. REV. 1055, 1066-69 (2013).

18. Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, N.Y. TIMES, Mar. 31, 2013, at BU1, *available at* http://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html (quoting Leslie Harris, President of the Center for Democracy and Technology, as stating: "We've been trying to get a comprehensive privacy law for over a decade, a law that would work for today and for technologies that we have not yet envisioned.").

19. Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309, 353 (2013).

20. Jonathan H. Adler, *The Problems with Precaution: A Principle without Principle*, THE AMERICAN (May 25, 2011), http://www.american.com/archive/2011/may/the-problems-with-precaution-a-principle-without-principle.

21. *See* CASS R. SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE 24-34 (2005).

22. Eli Dourado, *'Permissionless Innovation' Offline as Well as On*, THE UMLAUT (Feb. 6, 2013), http://theumlaut.com/2013/02/06/permissionless-innovation-offline-as-well-as-on.

23. Adam Thierer, *Who Really Believes in "Permissionless Innovation"?* TECH. LIBERATION FRONT, Mar. 4, 2013, http://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation.

Yet, precautionary logic regularly guides privacy-related proposals. For example, Federal Trade Commission (FTC) Chairwoman Edith Ramirez has recently focused her attention on privacy and security fears about the growth of "big data."[24] Ramirez claimed that "[o]ne risk is that the lure of 'big data' leads to the indiscriminate collection of personal information," and she continued on to argue:

> The indiscriminate collection of data violates the First Commandment of data hygiene: Thou shall not collect and hold onto personal information unnecessary to an identified purpose. Keeping data on the off-chance that it might prove useful is not consistent with privacy best practices. And remember, not all data is created equally. Just as there is low quality iron ore and coal, there is low quality, unreliable data. And old data is of little value.[25]

"Information that is not collected in the first place can't be misused," she claimed, and she also outlined hypothetical worst-case scenarios that might come about if such data collection was allowed at all.[26] She is particularly concerned that all this data might somehow be used by companies to discriminate against certain classes of customers.

Ramirez's complaint is closely related to a concern voiced by some legal scholars today regarding what Ryan Calo calls "digital market manipulation," or the belief that, "[f]irms will increasingly be able to trigger irrationality or vulnerability in consumers—leading to actual and perceived harms that challenge the limits of consumer protection law, but which regulators can scarcely ignore."[27] Other scholars fear "power asymmetries" between companies and consumers and even suggest that consumers' apparent lack of concern about sharing information means that people may not be acting in their own best self-interest when it comes to online safety and digital privacy choices.[28]

Similarly, Siva Vaidhyanathan claims that consumers are being tricked by the

---

24. Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard's Chair 1 (Aug. 19, 2013), *available at* http://www.ftc.gov/speeches/ramirez/130819bigdataaspen.pdf.

25. *Id.* at 4.

26. *Id.* at 6.

27. Ryan Calo, *Digital Market Manipulation*, 42 GEO. WASH. L. REV. (forthcoming 2014) (manuscript at 5), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703; *see also*, David Talbot, *Data Discrimination Means the Poor May Experience a Different Internet*, MIT TECH. REV. (Oct. 9, 2013), http://www.technologyreview.com/news/520131/data-discrimination-means-the-poor-may-experience-a-different-internet.

28. *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J. L. & POL'Y INFO. SOC'Y 425, 443 (2011) ("The idea is that individual choice in this area would lead, in a piecemeal fashion, to the erosion of privacy protections that are the foundation of the democratic regime, which is the heart of our political system. Individuals are making an assessment—at least implicitly—of the advantages and disadvantages to them of sharing information. They are determining that information sharing is, on balance, a net gain for them. But the aggregate effect of these decisions is to erode the expectation of privacy and also the role of privacy in fostering self-development, personhood, and other values that underlie the liberal way of life. In this way, individual choices are not sufficient to justify information practices that collectively undermine widely shared public values." (footnote omitted)).

"smokescreen" of "free" online services and "freedom of choice."[29] Although he admits that no one is forced to use online services and that consumers are also able to opt-out of most of its services or data collection practices, Vaidhyanathan argues that "such choices mean very little" because "the design of the system rigs it in favor of the interests of the company and against the interests of users."[30] "Celebrating freedom and user autonomy is one of the great rhetorical ploys of the global information economy," he says.[31] "We are conditioned to believe that having more choices—empty though they may be—is the very essence of human freedom. But meaningful freedom implies real control over the conditions of one's life."[32]

If imposed in the form of legal sanctions, such reasoning would open the door to almost boundless controls on the activities of both producers and consumers of digital services, potentially limiting future innovations in this space. Moreover, it would lead to what Daniel J. Solove has referred to as privacy law's "paternalism" problem.[33] "Privacy regulation," he notes, "risks becoming too paternalistic. Regulation that sidesteps consent denies people the freedom to make choices. The end result is that either people have choices that are not meaningful or people are denied choices altogether."[34] To the extent preemptive regulations restrict user choices in this way, it seems to confirm Thomas Lenard and Paul Rubin's claim that "many of the privacy advocates and writers on the subject do not trust the consumers for whom they purport to advocate."[35]

Consumer protection standards have traditionally depended on a clear showing of *actual*, not prospective or hypothetical, harm.[36] In some cases, when the potential harm associated with a particular practice or technology is extreme and poses a direct threat to physical well-being, law has displaced the general presumption that ongoing experimentation and innovation should be allowed by default.[37] However, these are extremely rare scenarios, at least as it pertains to privacy concerns under American law, and they mostly involved health and safety measures aimed at preemptively avoiding catastrophic harm to individual or environmental well-being. In the vast majority of other cases, our culture has not accepted the paternalistic idea that law must "save us from ourselves" (i.e., our own

29. SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 83 (2011).

30. *Id.* at 84.

31. *Id.* at 89.

32. *Id.*

33. Solove, *supra* note 12, at 1882.

34. *Id.* at 1894.

35. THOMAS M. LENARD & PAUL H. RUBIN, TECH. POLICY INST., THE BIG DATA REVOLUTION: PRIVACY CONSIDERATIONS 24 (Dec. 2013), http://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconsiderations.pdf.

36. *See* Solove, *supra* note 12, at 1897. ("The law generally does not override consent, even with potentially dangerous activities. . . . As a general matter, the law refrains from restricting transactions that appear on the surface to be consensual, and the law will tolerate a substantial amount of manipulation and even coercion before it deems a transaction to be nonconsensual.").

37. *See* Zachary Lees, *Anticipated Harm, Precautionary Regulation, and Hydraulic Fracturing*, 13 VT. J. ENVTL. L. 575, 584-89 (2012) (summarizing how the precautionary principle has been applied in various environmental contexts where potential harm was presumed to be significant).

irrationality or mistakes).[38]

But it is not just that precautionary principle-based logic rejects personal responsibility, it is that it ignores the costs of preemptive policy action.[39] This is particularly true for highly subjective values like digital privacy. As Solove notes, "the correct choices regarding privacy and data use are not always clear. For example, although extensive self-exposure can have disastrous consequences, many people use social media successfully and productively."[40]

Unfortunately, as noted in the next section, many privacy scholars do not bother conducting a serious review of the potential costs of their regulatory proposals. As a result, preemptive policy action is almost always the preferred remedy to any alleged harm. "By limiting or conditioning the collection of information, regulators can limit market manipulation at the activity level," Calo says.[41] "We could imagine the government fashioning a rule—perhaps inadvisable for other reasons—that limits the collection of information about consumers in order to reduce asymmetries of information."[42] Ultimately, Professor Calo does not endorse such a rule, but the corresponding cost of such regulatory proposals must be taken into account. If preemptive regulation slowed or ended certain information flows, it could, as noted below, stifle the provision of new and better services that consumers demand.[43]

The views set forth by some of these scholars as well as Chairwoman Ramirez represent a rather succinct articulation of precautionary principle thinking as applied to modern data collection practices. They are essentially claiming that—because there are various privacy risks associated with data collection and aggregation—policymakers should consider preemptive and potentially restrictive approaches to the initial collection and aggregation of data.

The problem with that logic should be fairly obvious, however, and as identified by the late political scientist and risk analysis expert Aaron Wildavsky, "if you can do nothing without knowing first how it will turn out, you cannot do anything at all."[44] *Best* case scenarios will never develop if we are gripped with fear by the *worst* cases scenarios and try to preemptively plan for them with policy interventions. "'Worst case' assumptions can convert otherwise quite ordinary conditions . . . into disasters, provided only that the right juxtaposition of unlikely

38. *See id.* ("People make decisions all the time that are not in their best interests. People relinquish rights and take bad risks, and the law often does not stop them."); Tom W. Bell, *Free Speech, Strict Scrutiny, and Self-Help: How Technology Upgrades Constitutional Jurisprudence*, 87 MINN. L. REV. 743, 743 (2003) ("The state ought not to help those who can better help themselves."); *see also* Thierer, *A Framework for Benefit-Cost Analysis, supra* note 17, at 1066-69.

39. J.R. SMITH & SIOBHAN MACDERMOTT, WIDE OPEN PRIVACY: STRATEGIES FOR THE DIGITAL LIFE 165-66 (2012) ("[A]t this point, the attempt to impose one-size-fits-all regulation on an as-yet-to-be-fully-known Internet strikes us as impractical, ineffective, and quite possibly counterproductive to continued innovation.").

40. Solove, *supra* note 12, at 1895.

41. Calo, *supra* note 27, at 38.

42. *Id.*

43. *A Status Update on the Development of Voluntary Do-Not-Track Standards: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 113th Cong. (2013) (testimony of Adam Thierer; transcript made available by the Mercatus Center, George Mason University, at http://mercatus.org/sites/default/files/Thierer_testimony_DNT_042313.pdf) [hereinafter Thierer Testimony].

44. AARON WILDAVSKY, SEARCHING FOR SAFETY 38 (1988).

factors occur."[45] In other words, it will always be easy to string together some random anecdotes or stories and concoct horrific-sounding scenarios about the future that leave us searching for preemptive solutions to problems that have not even developed yet.

For example, when Chairwoman Ramirez argues that "[i]nformation that is not collected in the first place can't be misused," that is undoubtedly true.[46] However, it is equally true that information that is not collected at all is information that might have been used to provide us with the next "killer app" or the great gadget or digital service that we cannot currently contemplate but that some innovative entrepreneur might be looking to develop. Likewise, claiming that "old data is of little value" and issuing the commandment that "[t]hou shall not collect and hold onto personal information unnecessary to an identified purpose" implies that she believes little good will come from serendipitous data discovery.[47] Yet, the reality is that the cornucopia of innovative information options and opportunities users have at their disposal today was driven in large part by data collection, including personal data collection.[48] Those innovations were not necessarily part of a firm's initial design; many came about after the fact with the discovery of new and interesting things that could be done with data.

Examples of after-the-fact data-driven innovations include many of the information services and digital technologies that consumers take for granted today, such as mobile traffic services, digital mapping technologies, spam and fraud detection tools, instant spell-checkers, and language translation tools. As Viktor Mayer-Schonberger and Kenneth Cukier point out, "data's value needs to be considered in terms of all the possible ways it can be employed in the future, not simply how it is used in the present."[49] "In the big-data age," they note, "data is like a magical diamond mine that keeps on giving long after its principal value has been tapped."[50] If privacy law had been premised on Chairwoman Ramirez's pronouncement that "keeping data on the off-chance that it might prove useful is not consistent with privacy best practices," then many of these innovations might never have come about, and future data-driven innovations would need to be curtailed significantly.[51]

It is useful to contrast Chairwoman Ramirez's approach to these concerns with her fellow FTC Commissioner Maureen K. Ohlhausen. Commissioner Ohlhausen has noted that, "[t]he success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the

45. *Id.* at 92.

46. Ramirez, *supra* note 24, at 6.

47. *Id.* at 4.

48. Farhad Manjoo, *Do We Want an Erasable Internet*?, WALL ST. J., Dec. 22, 2013, 4:46 AM, http://online.wsj.com/news/articles/SB10001424052702304773104579272723222788620 ("There is a good chance you love some of the many tech products that could only have come about because tech companies saved and analyzed your data.").

49. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 103 (2013).

50. *Id.* at 104.

51. Ramirez, *supra* note 24, at 4.

impact on consumers and competitors."[52] Commissioner Ohlhausen also makes another crucial point about why the precautionary mindset is problematic: *regulator irrationality* or *regulatory ignorance*.[53] Myopically focusing on the supposed irrationality of consumers and their openness to persuasion or "manipulation" ignores the potential irrationality or ignorance of regulators who simply do not possess the requisite knowledge to perfectly plan for every conceivable outcome.[54] This is particularly true for information technology markets, which generally evolve much more rapidly than other sectors, and especially more rapidly that law itself.[55] That insight leads Commissioner Ohlhausen to issue a word of caution to her fellow regulators:

> It is thus vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.[56]

This again suggests that Commissioner Ohlhausen's approach to technological innovation is consistent with the permissionless innovation approach that powered the first wave of Internet innovation, whereas Chairwoman Ramirez's approach is based on precautionary principle reasoning. This tension dominates almost all privacy debates today, even if it is not always on such vivid display as it is here.

IV. TOWARD SERIOUS BENEFIT-COST ANALYSIS

At some point the full range of costs associated with precautionary principle-based regulatory proposals must be taken into account. If policymakers conduct a careful benefit-cost analysis of various regulatory proposals—something that has been woefully lacking on the privacy front in recent years—they would find that many complex economic and social trade-offs are at work.[57] Regulation is not a costless exercise and, as noted, there are reasons to doubt it will even be effective if pursued.

Despite this, Obama administration officials and other congressional lawmakers who have proposed expanded privacy regulation have failed to fully grapple with the costs associated with such rules in recent reports and statements.[58] This is unfortunate since a blueprint already exists for how to do so. In its 1980

---

52. Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, The Internet of Things and The FTC: Does Innovation Require Intervention?, Remarks Before the U.S. Dept. of Commerce, at 3-4 (Oct. 18, 2013), *available at* http://www.ftc.gov/public-statements/2013/10/internet-things-ftc-does-innovation-require-intervention-0.

53. *See id.*

54. *See* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE 138, 140 (2d ed. 2010) (describing the problem of "epistemic arrogance" or hubris concerning the limits of our knowledge. "We are demonstrably arrogant about what we think we know. . . . We overestimate what we know, and underestimate uncertainty.").

55. *See* Olhausen, *supra* note 52, at 3-4.

56. *Id.*

57. Thierer Testimony, *supra* note 43, at 3.

58. Thierer, *A Framework for Benefit-Cost Analysis*, *supra* note 17, at 1057.

Policy Statement on Unfairness,[59] the FTC clarified for members of Congress how the agency interpreted and enforced its statutorily granted authority under Section 5 of the Federal Trade Commission Act.[60] Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[61] In its *Policy Statement*, the agency noted that, "[t]o justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[62] This "is essentially a cost-benefit test," note two former FTC officials.[63]

The *Policy Statement* also specified that "the injury must be substantial" and that "[t]he Commission is not concerned with trivial or merely speculative harms. . . . Emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair."[64] Of course, measuring such harms is a highly subjective and controversial undertaking,[65] which may explain why the FTC has not made a serious effort to weigh the relative costs and benefits of various regulatory proposals.[66]

Regardless, the benefits associated with commercial data collection and data-driven marketing and innovation are clear.[67] In a study commissioned by the Direct Marketing Association, John Deighton and Peter Johnson found that data-driven marketing added $156 billion in revenue to the U.S. economy and fueled

---

59. Letter from the Fed. Trade Comm'n to Wendell H. Ford, Chairman, Consumer Subcomm., U.S. S. Comm. on Commerce, Sci., & Transp., & John C. Danforth, Ranking Minority Member, Consumer Subcomm., U.S. S. Comm. on Commerce, Sci., & Transp. (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter FTC Policy Statement on Unfairness].

60. *See, e.g.*, Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 828-32 (2011); J. Howard Beales, Former Dir., Fed. Trade Comm'n, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, Speech at The Marketing and Public Policy Conference (May 30, 2003), *available at* http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection; J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Deceptive and Unfair Acts and Practices Principles: Evolution and Convergence, Speech at the Cal. State Bar (May 18, 2007), *available at* http://www.ftc.gov/speeches/rosch/070518evolutionandconvergence.pdf.

61. 15 U.S.C. § 45(a) (2012).

62. FTC Policy Statement on Unfairness, *supra* note 59.

63. J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 132 (2008).

64. FTC Policy Statement on Unfairness, *supra* note 59 (footnotes omitted).

65. *See* Thierer, *supra* note 6, at 414-21.

66. Commenting on the FTC's two recent privacy reports, economists Paul Rubin and Thomas Lenard observe that "[n]either 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." Thomas M. Lenard & Paul H. Rubin, *The FTC and Privacy: We Don't Need No Stinking Data*, ANTITRUST SOURCE, Oct. 2012, at 4, http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/oct12_lenard_10_22f.authcheckdam.pdf.

67. *See* SOFTWARE & INFO. INDUS. ASS'N, DATA-DRIVEN INNOVATION, A GUIDE FOR POLICYMAKERS: UNDERSTANDING AND ENABLING THE ECONOMIC AND SOCIAL VALUE OF DATA 12-15 (May 2013), *available at* http://siia.net (follow "Public Policy" hyperlink; then follow "Data-Driven Innovation" hyperlink).

more than 675,000 jobs in 2012.[68] Major reports from consultancies Gartner[69] and McKinsey Global Institute[70] have also documented significant consumer benefits from "big data" across multiple sectors.

Meanwhile, commercial data collection allows better targeting of advertising and marketing that produces significant benefits for consumers.[71] Howard Beales, former director of the Bureau of Consumer Protection at the FTC, found that "the price of [behaviorally targeted] advertising in 2009 was 2.68 times the price of run of network advertising," and this increased return on investment is important because it creates "greater utility for consumers [from more relevant advertisements] and clear appeal for advertisers" because of the increased conversion of ads into sales.[72] This helps the creators of digital content and services continue to make cheap or even free goods available to consumers.[73] If privacy regulation made such services more expensive or led them to disappear entirely, a consumer backlash would likely ensue.[74] Importantly, firms would likely be able to use incentives to opt back in to various types of tracking and data

---

68. JOHN DEIGHTON & PETER A. JOHNSON, THE VALUE OF DATA: CONSEQUENCES FOR INSIGHT, INNOVATION & EFFICIENCY IN THE U.S. ECONOMY 5 (2013), http://ddminstitute.thedma.org/#valueofdata (follow "Get the Study" hyperlink).

69. Press Release, Gartner, Gartner Says Big Data Will Drive $28 Billion of IT Spending in 2012 (Oct. 17, 2012), *available at* http://www.gartner.com/newsroom/id/2200815.

70. JAMES MANYIKA ET AL., MCKINSEY & CO., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 97-106 (May 2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation (follow "Full Report" hyperlink).

71. *See* Adam Thierer, *Relax and Learn to Love Big Data*, U.S. NEWS & WORLD REP. (Sept. 16, 2013), http://www.usnews.com/opinion/blogs/economic-intelligence/2013/09/16/big-data-collection-has-many-benefits-for-internet-users.

72. HOWARD BEALES, THE VALUE OF BEHAVIORAL TARGETING 3 (Network Adver. Initiative, Mar. 2010), *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. A more recent study from Beales and economist Jeffrey Eisenach, which was sponsored by the Digital Advertising Alliance, revealed that

> advertisers place significantly greater value on users for whom more information is available, and . . . the availability of cookies to capture user-specific information is found to increase the observed exchange transaction price by at least 60 percent relative to the average price (for users with "new" cookies), and by as much as 200 percent (for users with longer-lived cookies).

J. HOWARD BEALES & JEFFREY A. EISENACH, AN EMPIRICAL ANALYSIS OF THE VALUE OF INFORMATION SHARING IN THE MARKET FOR ONLINE CONTENT 1 (2014), *available at* http://images.politico.com/global/2014/02/09/beales_eisenach_daa_study.html.

73. *See* Berin Szoka & Adam Thierer, *Targeted Online Advertising: What's the Harm & Where Are We Heading?*, 16 PROGRESS & FREEDOM FOUND.: PROGRESS ON POINT, issue 2, June 2009, at 6, *available at* http://www.pff.org/issues-pubs/pops/2009/pop16.2targetonlinead.pdf; BEALES & EISENACH, *supra* note 72, at 16 ("At a time when 'traditional media' face considerable challenges to their underlying business models, online advertising constitutes a dynamic and rapidly expanding component of the digital economy. The advent of information sharing in the market for online content has created unprecedented opportunities for the exchange of information to more efficiently connect consumers with the ultimate suppliers of the products they value the most." The authors continue on to note that "the largest publishers rely on third-party technology models for approximately half of their advertising needs, while 'long-tail' publishers rely even more heavily on these models.").

74. *See* Szoka & Thierer, *supra* note 73, at 6.

collection schemes even if privacy law was adjusted to make that more difficult.[75]

Finally, privacy regulation could have a profound impact on market dynamics and the competitiveness of U.S. firms both domestically and internationally.[76] These impacts must also be taken into account when conducting benefit-cost analysis of new legislative or regulatory enactments since they could limit consumer choices or raise costs.

V. NEW APPROACHES

In light of the myriad new challenges associated with information control efforts as well as the costs associated with precautionary principle-based regulatory efforts, new approaches to privacy protection will need to be considered. We can find some of those alternative approaches by examining the debate that has taken place about online child protection over the past fifteen years.[77]

Since the dawn of the commercial Internet in the early 1990s, online safety and access to objectionable content—especially underage access to pornography—has been a major public policy concern. As a result, a wide variety of regulatory schemes and technical solutions were proposed. Yet, those efforts were largely abandoned over time as policymakers and online safety advocates came to realize that legal hurdles and practical realities meant a new approach to dealing with access to objectionable online content was needed.

Between 2000 and 2010, six major online safety task forces were formed to study online concerns and to consider possible solutions.[78] The United States government convened three of these task forces, and they issued reports in 2000,[79] 2002,[80] and 2010 respectively.[81] The British government formed another task force in 2007, which issued a report in March 2008.[82] Finally, two additional task forces were formed in the U.S. in 2008 and concluded their work, respectively, in

---

75. Solove, *supra* note 12, at 1898 ("[M]any organizations will have the sophistication and motivation to find ways to generate high opt-in rates. They can do so simply by conditioning products, services, or access on opting in.").

76. *See* Thierer Testimony, *supra* note 43, at 2-3.

77. *See generally* ADAM THIERER, PARENTAL CONTROLS & ONLINE CHILD PROTECTION: A SURVEY OF TOOLS AND METHODS (version 4.0, 2009), *available at* http://www.pff.org/parentalcontrols (describing the various methods available to parents to control child access to media and arguing against regulation as a solution).

78. *See* Adam Thierer, *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer*, 16 PROGRESS & FREEDOM FOUND.: PROGRESS ON POINT, issue 2, July 2009, at 1, *available at* http://www.pff.org/issues-pubs/pops/2009/pop16.13-five-online-safety-task-forces-agree.pdf; ONLINE SAFETY & TECH. WORKING GRP., NAT'L TELECOMM. & INFO. ADMIN., YOUTH SAFETY ON A LIVING INTERNET: REPORT OF THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP (June 4, 2010), *available at* http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf.

79. *See Report to Congress*, COPA COMM'N (Oct. 20, 2000), www.copacommission.org.

80. *See* COMPUTER SCI. & TELECOMM. BD., NAT'L RESEARCH COUNCIL, YOUTH, PORNOGRAPHY AND THE INTERNET (Dick Thornburgh & Herbert S. Lin eds., 2002), *available at* http://www.nap.edu/openbook.php?isbn=0309082749.

81. *See* ONLINE SAFETY & TECH. WORKING GRP., *supra* note 78.

82. *See* BYRON REV., SAFER CHILDREN IN A DIGITAL WORLD (Mar. 2008), *available at* http://dera.ioe.ac.uk/7332/1/Final%20Report%20Bookmarked.pdf.

December of 2008[83] and July of 2009.[84]

Hundreds of experts submitted material to these task forces or testified before them.[85] There was a great deal of unanimity among these task forces in terms of their conclusions and recommendations. Most notably, the commissions all generally agreed that there is no single "silver-bullet" technological solution or legal quick-fix to concerns about online safety or access to objectionable content.[86] The rapid pace of technological change was a primary factor that these task forces cited when drawing this conclusion.[87]

Each of the task forces concluded that education should be the primary solution to most online child safety concerns.[88] Specifically, these task forces consistently stressed the importance of media literacy, awareness-building efforts, public service announcements, targeted intervention techniques, and better mentoring and parenting strategies.[89]

As part of these efforts to strive for "digital citizenship," online safety experts stressed the vital importance of teaching both children and adults smarter online hygiene (sensible personal data use) and "netiquette" (proper behavior toward others), which can further both online safety and digital privacy goals.[90] More generally, as part of these digital literacy and citizenship efforts, more should be done to explain the potential perils of over-sharing information about ourselves and others while simultaneously encouraging consumers to delete unnecessary online information occasionally and cover their digital footprints in other ways.

These education and literacy efforts are also important because they help us adapt to new technological changes by employing a variety of coping mechanisms or new social norms. These efforts and lessons should start at a young age and continue on well into adulthood through other means, such as awareness campaigns and public service announcements.

The importance of empowerment and user "self-help" is another lesson that flows from recent online safety discussions. All the major online safety task forces that met over the past fifteen years recommended the use of technological self-help tools that could help users tailor online experiences to their own preferences and values.[91] A wide variety of online safety- and privacy-enhancing tools already

---

83. *See* BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV., ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES: FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE TO THE MULTI-STATE WORKING GROUP ON SOCIAL NETWORKING OF STATE ATTORNEYS GENERAL OF THE UNITED STATES (Dec. 31, 2008), *available at* http://cyber.law.harvard.edu/pubrelease/isttf.

84. *See* POINTSMART.CLICKSAFE, TASK FORCE RECOMMENDATIONS FOR BEST PRACTICES FOR CHILD ONLINE SAFETY (July 2009), *available at* http://www.pointsmartreport.org/PointSmartReport.pdf.

85. *See* Thierer, *supra* note 78.

86. *Id.*

87. *See id.*

88. *See id.*; ONLINE SAFETY & TECH. WORKING GRP., *supra* note 78, at 18-19.

89. *See* Thierer, *supra* note 78; ONLINE SAFETY & TECH. WORKING GRP., *supra* note 78, at 6-9.

90. *See, e.g.*, Anne Collier, *From Users to Citizens: How to Make Digital Citizenship Relevant*, NETFAMILYNEWS.ORG (Nov. 16, 2009, 2:23 PM), www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html; *Digital Literacy and Citizenship in the 21st Century: Educating, Empowering, and Protecting America's Kids*, COMMON SENSE MEDIA (June 2009), www.commonsensemedia.org/sites/default/files/CSM_digital_policy.pdf.

91. *See* Thierer, *supra* note 78; ONLINE SAFETY & TECH. WORKING GRP., *supra* note 78, at 6-7.

exist for those looking to safeguard their child's online experiences or their own online privacy.[92] A host of tools are available to block or limit various types of data collection, and every major web browser has cookie-control tools to help users manage data collection.[93] Many nonprofits—including many privacy advocates—offer instructional websites and videos explaining how privacy-sensitive consumers can take steps to protect their personal information online.[94]

Taken together, these lessons suggest a "layered approach" for enhancing both online safety and privacy protection. This layered approach relies on using many tools, methods, and strategies; it implicitly assumes that law will always be one step behind in attempting to remedy these concerns, and hence, these alternative methods will need to fill the gap.

Governments can play a major role in this process by facilitating educational and empowerment-based solutions.[95] Governments are uniquely positioned to get the word out about new technologies—both the benefits and dangers—and can develop privacy and safety messaging—especially to youngsters—about appropriate use of new technologies. The FTC already does so. Along with over a dozen other federal agencies, it runs a website called "OnGuard Online," which addresses various online threats and offers the public helpful advice to combat them.[96] In theory, government agencies could even go further and create privacy and safety-related apps that help users better protect themselves or their families online. Of course, an extensive array of privacy and safety-enhancing empowerment tools already exists.[97]

Beyond classroom media literacy and digital citizenship efforts, government can undertake broad-based public awareness campaigns.[98] Government officials at the federal, state, and local levels should work together to devise media literacy campaigns focused on online safety, understanding the existing rating systems, and how to use parental controls. These campaigns should include broadcast (radio and TV) ads, Internet websites and advertising, and promotional posters and brochures that could be distributed at schools and government institutions. Government has undertaken (or lent its support to) such public awareness campaigns to address other concerns in the past and had a great deal of success, including forest fire prevention ("Smokey the Bear");[99] anti-littering ("Give a Hoot, Don't Pollute");[100]

---

92. *See* Thierer, *supra* note 6, at 440-46.

93. *See id.*

94. *See id.* at 439.

95. *See* ONLINE SAFETY & TECH. WORKING GRP., *supra* note 78, at 31 ("There needs to be ongoing communications and interaction among all departments involved in Internet safety and education including Education, Justice, Homeland Security, Substance Abuse and Mental Health Services Administration (SAMHSA), Centers for Disease Control, Commerce, the FCC, the FTC and the White House with liaisons to Congress and state and local agencies.").

96. *See About Us*, ONGUARD ONLINE, http://www.onguardonline.gov/about-us (last visited Jan. 27, 2014).

97. *See* THIERER, *supra* note 77, at 103-43.

98. *See* ONLINE SAFETY & TECH. WORKING GRP., *supra* note 78, at 32 ("The government can't legislate civility, but it can encourage it. This will not be an easy fix but, like cutting down on smoking, racism, sexism and other social ills, it can be accomplished through awareness-raising over time.").

99. *See Campaign History*, SMOKEY BEAR, http://www.smokeybear.com/vault/history_main.asp (last visited Jan. 31, 2014).

crime prevention ("McGruff the Crime Dog");[101] and seat-belt safety.[102] These and similar initiatives have helped change public attitudes toward important social matters without heavy-handed and expensive top-down controls being imposed on business models or innovations.

VI. THE ROLE OF PRIVACY PROFESSIONALS AND THE DIGITAL DESIGNERS OF THE FUTURE

Education and digital citizenship efforts are essential not only because they teach consumers how to navigate new information environments and challenges but also because they can guide the actions of current or future *producers* of new digital technologies.

Much effort has been spent in recent years encouraging digital innovators to institute "privacy by design" when contemplating their new products.[103] But *real* privacy by design should be a state of mind and a continuous habit of action that influences how designers think about the impact of their products and services before and after creation. We should continue to consider how we might achieve "privacy by design" before new services are rolled out, but the reality is that "privacy on the fly" may become even more essential.

This is where the role of privacy professionals—Chief Privacy Officers, Chief Information Officers, Chief Data Officers, "Data Architects," etc.—becomes vital.[104] Solove notes that Chief Privacy Officers and other privacy professionals "educate personnel to be mindful of privacy and influence software, product, and service design to be more privacy friendly. Privacy self-management thus has the salutary effect of creating beneficial structural privacy protections and accountability inside institutions."[105] The steadily growing ranks of the International Association of Privacy Professionals (IAPP), which trains and certifies privacy professionals, reflects the expanded focus on privacy and security by design efforts. Membership in the IAPP has grown to more than 15,000, up from 10,000 in March 2012.[106]

The rise of the privacy professional could have a profound impact on privacy protection in the future. As Deirdre Mulligan and Kenneth Bamberger have noted, it is increasingly what happens "on the ground"—the day-to-day management of privacy decisions through the interaction of privacy professionals, engineers, outside experts, and regular users—that is really important for protecting

100. *See A Short History*, U.S. DEP'T AGRIC. FOREST SERV., http://www.fs.usda.gov/main/conservationeducation/smokey-woodsy/woodsy-owl (follow "A Short History" hyperlink) (last visited Jan. 31, 2014).

101. *See About McGruff*, NAT'T CRIME PREVENTION COUNCIL, http://www.ncpc.org/about/about-mcgruff (last visited Jan. 31, 2014).

102. *See Safety Belt Education*, AD COUNCIL, http://www.adcouncil.org/Our-Work/The-Classics/Safety-Belt-Education (last visited Jan. 31, 2014).

103. Ann Cavoukian, *2011: The Decade of Privacy by Design Starts Now*, ITBUSINESS.CA (Jan. 15, 2011), http://blogs.itbusiness.ca/2011/01/2011-the-decade-of-privacy-by-design-starts-now.

104. *See* Brad Peters, *Meet the CDO*, FORBES (Dec. 20, 2013, 2:00 PM), http://www.forbes.com/sites/bradpeters/2013/12/20/meet-the-cdo.

105. Solove, *supra* note 12, at 1900.

106. Omer Tene, *2013: The Year of Privacy*, IAPP: PRIVACY PERSPS. (Dec. 19, 2013), https://www.privacyassociation.org/privacy_perspectives/post/20.13_the_year_of_privacy.

consumers' privacy. They suggest that "governing privacy through flexible principles" may be the best regulatory approach.[107] In this way, privacy policy can again draw lessons from the online safety field where "bottom-up" safety-by-design and safety-on-the-fly efforts have been underway for many years.

VII. RELIANCE ON NORMS AND SOCIAL PRESSURE WILL EXPAND

Another lesson that flows from the field of online child safety is that norms will play a greater role over time. Social pressure and private norms of acceptable use often act as "regulators" of the uses (and misuses) of new technologies. This has been true long before the Internet and digital technologies began raising privacy concerns.

The rise of the camera and public photography, for example, led to an initial backlash among some critics on privacy grounds. Notably, in response to the privacy-related concerns about photography, Samuel D. Warren and Louis D. Brandeis penned the most important essay ever written on privacy law, their 1890 *Harvard Law Review* essay on "The Right to Privacy" claiming that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life."[108] However, public attitudes toward cameras and public photography evolved quite rapidly, and they became an ingrained part of the human experience. At the same time, social norms and etiquette evolved to address those who would use cameras in inappropriate or intrusive ways. This holds true for modern technology. Using smartphone cameras in gym locker rooms, for example, is frowned upon not just by gym management (which often posts notices restricting use) but also by patrons.[109] Social constraints on mobile phones also constrain their uses in other public establishments and settings, such as in movie theaters, fancy restaurants, and "quiet cars" on trains. These norms or social constraints are purely bottom-up and group-driven.

Norms are also influenced by the social pressure exerted by advocacy organizations. Media watchdogs and online safety groups have been quite successful in shaping media norms over the past two decades. Groups like Common Sense Media have influenced content decisions through the pressure they have brought to bear on media providers in the marketplace. Common Sense Media not only encouraged and influenced the development of private content rating systems for video games, but the group also developed its own content rating system for games, TV, and movies to provide parents and others with useful

107. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 253 (2011).

108. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

109. *See* Farhad Manjoo & Emily Yoffe, *Cellphones in Locker Rooms (Transcript)*, SLATE (May 15, 2012, 12:30 PM), http://www.slate.com/articles/podcasts/manners_for_the_digital_age/2012/05/digital_manners_gym_is_too_lax_in_enforcing_its_cellphone_free_locker_room_policy_transcript_.html; Catherine Saint Louis, *Cellphones Test Strength of Gym Rules*, N.Y. TIMES (Dec. 8, 2011), at E1, *available at* http://www.nytimes.com/2011/12/08/fashion/struggle-to-ban-smartphone-usage-in-gyms.html.

information.[110] Similarly, the Parents Television Council (PTC) awards a "seal of approval" to advertisers and programmers that only support programs that the PTC classifies as family-friendly.[111] The organization also encourages parents to send letters and e-mails to advertisers who support programming they find objectionable and encourage those advertisers to end their support of those shows.[112]

In recent years, privacy advocates have also become more visible and gained influence that closely mirrors what occurred with online child safety organizations in the previous two decades. While both sets of advocates were slow to gain influence at first, as their respective issues gained more prominence, their power steadily grew. Many other non-profit and advocacy organizations—including the Electronic Privacy Information Center,[113] the Future of Privacy Forum,[114] Privacy Rights Clearinghouse,[115] ACLU,[116] and others—have developed websites and materials to better inform consumers about how they can protect their data. Going forward, we can expect privacy policies—both legal enactments and informal corporate standards—to be significantly influenced by the pressure that these advocates exert on the process.

Finally, the media offers a powerful check on mistakes and misbehavior. Technology developers today face near constant scrutiny, not just from large media outlets, but also from what Dan Gillmor refers to as the rise of the "we-dia" (user-generated content and citizen journalism) that is an increasingly important part of the modern media landscape.[117] Gillmor, a former *San Jose Mercury News* columnist, asserts that we are in the middle of "a modern revolution . . . because technology has given us a communications toolkit that allows anyone [to] become a journalist at little cost and, in theory, with global reach. Nothing like this has ever been remotely possible before."[118] "We are seeing the emergence of new, decentralized approaches to fulfilling the watchdog function and to engaging in political debate and organization," notes Yochai Benkler.[119]

Consider how public and media pressure forced both Instagram and Twitter to make almost immediate about-faces after changing privacy settings. On December 17, 2012, Instagram, an online photo sharing service owned by Facebook,

---

110. *See Behind the Common Sense Media Ratings System*, COMMON SENSE MEDIA, http://www.commonsensemedia.org/about-us/our-mission/about-our-ratings (last visited Feb. 5, 2014).

111. *The PTC Seal of Approval*, PARENTS TELEVISION COUNCIL, http://www.parentstv.org/PTC/awards/main.asp (last visited Feb. 1, 2014).

112. *See Advertiser Accountability*, PARENTS TELEVISION COUNCIL, http://w2.parentstv.org/main/Campaigns/Accountability.aspx (last visited Feb. 5, 2014).

113. *See About EPIC*, ELEC. PRIVACY INFO. CTR., http://epic.org/epic/about.html (last visited Feb. 1, 2014).

114. *See Our Mission*, FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/about/our-mission (last visited March 14, 2014).

115. *See Fact Sheets,* PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/privacy-rights-fact-sheets (last visited Feb. 1, 2014).

116. *See* Nicole A. Ozer, *It's Time to Demand Our dotRights!*, ACLU OF N. CAL. (Nov. 18, 2009), https://www.aclunc.org/blog/its-time-demand-our-dotrights.

117. *See* GLENN REYNOLDS, AN ARMY OF DAVIDS: HOW MARKETS AND TECHNOLOGY EMPOWER ORDINARY PEOPLE TO BEAT BIG MEDIA, BIG GOVERNMENT, AND OTHER GOLIATHS 89-114 (2006).

118. DAN GILLMOR, WE THE MEDIA xxiii (paperback ed. 2006).

119. YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 11 (2006).

announced it would be changing its policies and making it easier for the company to share user information and photographs with Facebook and advertisers.[120] The change prompted an intense user backlash and widespread media coverage.[121] Other photo-sharing applications saw a boost in traffic following Instagram's debacle.[122] Three days later, Instagram reversed its decision and reverted to its previous privacy policy.[123] The company's co-founder also issued a public apology on Instagram's corporate blog.[124]

A year later, on December 12, 2013, the microblogging service Twitter was forced to immediately reverse its decision to change the way users could block others on the site.[125] "The brief change set off an uproar among users who said it opened the door for abusive behavior," since it meant that blocked users "could view and send tweets to the person who blocked them, but those tweets would have been invisible to that person."[126] Following the backlash, Twitter reversed its decision and reinstated its former blocking policy just a few hours later.[127]

These examples show how the combination of social norms, media attention, and public pressure provides a powerful check on abuses of new technologies and proves that new technologies can be regulated by more than law.

VIII. CONCLUSION

Although policymakers will likely continue to pursue law and regulation and, at the margin, may be able to help with egregious privacy and security harms, the reality is that, outside narrow exceptions such as health and financial privacy regulation, the case for regulatory controls becomes harder to justify since the costs will typically exceed the benefits. To the extent greater information controls are pursued, the burden of proof lies with advocates of precautionary principle-based regulation to demonstrate unambiguous harms are omnipresent and unavoidable absent prophylactic constraints. Even then, benefit-cost analysis is essential.

Regardless, it is essential to have a good backup plan when privacy controls are impossible or too costly. Education is the strategy with the most lasting impact.

---

120. *See* Jenna Wortham & Nick Bilton, *What Instagram's New Terms of Service Mean for You*, N.Y. TIMES BITS BLOG (Dec. 17, 2012, 5:02 PM), http://bits.blogs.nytimes.com/2012/12/17/what-instagrams-new-terms-of-service-mean-for-you.

121. *See* Joshua Brustein, *Anger at Changes on Instagram*, N.Y. TIMES BITS BLOG (Dec. 18, 2012, 4:05 PM), http://bits.blogs.nytimes.com/2012/12/18/anger-at-changes-on-instagram.

122. *See* Nicole Perlroth & Jenna Wortham, *Instagram's Loss Is a Gain for Its Rivals*, N.Y. TIMES BITS BLOG (Dec. 20, 2012, 10:00 PM), http://bits.blogs.nytimes.com/2012/12/20/instagrams-loss-is-other-apps-gain.

123. *See* Declan McCullagh & Donna Tam, *Instagram Apologizes to Users: We Won't Sell Your Photos*, CNET (Dec. 18, 2012, 2:13 PM), http://news.cnet.com/8301-1023_3-57559890-93/instagram-apologizes-to-users-we-wont-sell-your-photos.

124. *See* Kevin Systrom, *Thank You, and We're Listening*, INSTAGRAM BLOG, http://blog.instagram.com/post/38252135408/thank-you-and-were-listening (last visited Feb. 1, 2014).

125. Claire Cain Miller, *Twitter Reverses Privacy Change in Response to User Complaints*, N.Y. TIMES BITS BLOG (Dec. 13, 2013, 4:35 PM), http://bits.blogs.nytimes.com/2013/12/13/twitter-reverses-privacy-change-in-response-to-user-complaints.

126. *Id.*

127. *See* Michelle Quinn, *Users Everywhere Rise Up and Fight Tweaks to Their Internet Services,* SILICONBEAT (Dec. 13, 2013), http://www.siliconbeat.com/2013/12/13/users-everywhere-rise-up-and-fight-tweaks-to-their-internet-services.

Media literacy and digital literacy provide skills and wisdom that can last a lifetime, enhancing individual resiliency. Specifically, education can help teach both children and adults how to behave in, or respond to, a wide variety of situations. Rethinking privacy from the bottom-up and engaging citizens in this way will ultimately serve us better than most of the top-down legalistic approaches being pursued today.