PUBLIC INTEREST COMMENT ON FEDERAL TRADE COMMISSION REPORT, *PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE*[1]

FEBRUARY 18, 2011

Adam Thierer
Senior Research Fellow

CONTENTS

[1] Prepared by Adam Thierer, senior research fellow, Mercatus Center at George Mason University. This comment is one in a series of Public Interest Comments from Mercatus Center's Technology Policy Program and does not represent an official position of George Mason University.

INTRODUCTION

The Technology Policy Program at the Mercatus Center at George Mason University is dedicated to advancing knowledge of the impact of regulation on society. As part of its mission, the Mercatus Center conducts careful and independent analyses employing contemporary economic scholarship to assess rulemaking proposals from the perspective of the public interest. Thus, this comment on the Federal Trade Commission ("the Commission") December 2010 report, *Protecting Consumer Privacy in an Era of Rapid Change*,[2] does not represent the views of any particular affected party or special interest group, but is designed to assist the commission as it weighs the costs and benefits of expanded online privacy regulation.

NO SHOWING OF HARM OR MARKET FAILURE HAS BEEN MADE

How Do We Conduct Cost-Benefit Analysis When "Creepiness" Is the Alleged Harm?

It goes without saying that privacy is a highly subjective[3] and ever-changing condition.[4] Unsurprisingly, therefore, attitudes about targeted online advertising are evolving and in various filings to the Commission as well as countless news stories, we hear both regulatory advocates and average consumers alike stress the "creepiness" factor associated with online data collection and targeted advertising.

---

2 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (December 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

3 "Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves." Jim Harper, "Understanding Privacy—and the Real Threats to It," *Policy Analysis* 520 (Washington, DC: Cato Institute, August 4, 2004), www.cato.org/pub_display.php?pub_id=1652. "When it comes to privacy, there are many inductive rules, but very few universally accepted axioms." David Brin, *The Transparent Society* (New York: Basic Books, 1998), 77. "On the social Web, privacy is a global and entirely subjective quality—we each perceive different threats to it." Betsy Masiello, "Deconstructing the Privacy Experience," *IEEE Security & Privacy*, July/August 2009, 70. "Privacy is a matter of taste and individual choice." Michael Fertik, *Comments of Reputation.com, Inc. to the U.S. Department of Commerce*, January 28, 2011, 13, http://www.reputation.com/blog/2011/01/31/reputation-com-comments-commerce-department-privacy-green-paper. "In most conversations, no one knows what anyone else means by 'privacy,' or what information is included in the terms 'personally-identifiable information…" Larry Downes, "A Market Approach to Privacy Policy," in Berin Szoka and Adam Marcus, eds., *The Next Digital Decade: Essays on the Future of the Internet* (Washington, DC: TechFreedom, 2011), 514, http://nextdigitaldecade.com/ndd_book.pdf#page=510.

4 "The meaning of privacy has changed, and we do not have a good way of describing it. It is not the right to be left alone, because not even the most extreme measures will disconnect our digital selves from the rest of the world. It is not the right to keep our private information to ourselves, because the billions of atomic factoids don't any more lend themselves into binary classification, private or public." Abelson, Ledeen, and Lewis, *Blown to Bits*, 68.

"But creating new privacy rights cannot be justified simply because people feel vague unease," notes Solveig Singleton, formerly of the Cato Institute.[5] If harm is reduced to "creepiness" or even "annoyance" and "unwanted solicitations" as some advocate, it raises the question whether the commercial Internet as we know it can continue to exist. Such an amorphous standard leaves much to the imagination and opens the door to creative theories of harm that are sure to be exploited. In such a regime, harm becomes highly conjectural instead of concrete. This makes credible cost-benefit analysis virtually impossible since the debate becomes purely about emotion instead of anything empirical. It does not help that most modern theories of privacy are not grounded in any substantive theory of rights.

Importantly, nothing in the Commission's proceeding has thus far demonstrated that online data collection and "tracking" represent a clear harm to consumers *per se*, or that any "market failure" exists here. Such a showing would be difficult since using data to deliver more tailored advertising to consumers can provide important *benefits* to the public, as will be noted below.

In sum, the Commission should avoid calls to untether privacy regulation from a harms-based analysis, which tests whether concrete, tangible harms exist and then weighs the benefits of regulation against its costs. It is unlikely the vast majority of online advertising and data collection activity would meet this test.

Privacy Regulation & The Precautionary Principle

Some privacy advocates seemingly desire that policy makers enshrine the equivalent of a "privacy precautionary principle" into law that would disallow online developments and innovations that fail to first pass some amorphous balancing test.[6] The "precautionary principle" basically holds that since every technological advance poses some theoretical danger or risk, public policy should be crafted in a way that guarantees no possible harm will come from that innovation before further progress is allowed. In other words, law should mandate "just play it safe" as the default policy.[7]

The Commission seems to be flirting with such a notion for privacy in this proceeding. This would be a grave mistake since it would have a profoundly deleterious impact on the future of online innovation and free speech. As Kevin Kelly, author of *What Technology Wants*, eloquently argues, the problem with that logic is that because "every good produces harm somewhere . . . by the strict logic of an absolute precautionary principle no technologies would be permitted."[8] Thus, under a regulatory regime guided at every turn by the equivalent of a privacy precautionary principle, digital innovation and technological progress becomes impossible because trade-offs are considered unacceptable.

On "Informed Consent" & Information as Currency

The Commission devotes a section of its report to the fear that "a lack of understanding undermines informed consent" online.[9] Perfectly "informed consent" for each and every online informational transaction or data transfer is likely impossible, however. Any attempt to demand perfection in this regard would likely require the creation of a mandatory online identification/user-authentication regime. Ironically, that would create new—and far more serious—privacy tensions.

---

5 Solveig Singleton, "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector," *Policy Analysis* 295 (Washington, DC: Cato Institute, January 22, 1998), 8, http://www.cato.org/pubs/pas/pa-295.html.

6 See, e.g., Daniel Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008), which attempts to untether privacy law from harms-based tests and advance a so-called "pragmatic" framework. Unfortunately, although he does not acknowledge it, his pragmatic framework *is* value-laden; privacy seemingly always trumps ever other potential value or consideration.

7 The most obvious manifestation of this approach comes from proposals to apply the Privacy Act of 1974, which tightly limits governmental information collection or reuse, to private organizations. See Marc Rotenberg and Sharon Goott Nissim, *Comments of the Electronic Privacy Information Center to the U.S. Department of Commerce*, January 25, 2011, 8, http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=E7E84473-D7BA-4D21-9675-7DC97F68110D.

8 Kevin Kelly, *What Technology Wants* (New York: Viking, 2010) 247-8.

9 Federal Trade Commission, *Protecting Consumer Privacy*, 25-28.

We need to move toward a different norm whereby there exists a tacit understanding of the *quid pro quo* at work when Netizens use many online sites and services. Namely, consumers need to be made better aware that when they visit a site or use online services, information is often required as a condition of service. That information may be collected to facilitate a better browsing experience or, more importantly, to help the site or service remain viable. In essence, information will be used in lieu of currency, and it will improve consumer welfare by lowering the cost of online content and services, or even making them free.

More could be done ensure consumers understand the nature of this value exchange, and this would go a long way toward alleviating many of the concerns about online data collection and *perceived* harms. Commenting on the potential pitfalls of a move toward mandatory opt-ins for online advertising/data collection, Corey Kronengold of *Digiday* argues:

> The value chain of online publishing is increasingly complex. And most consumers don't have any interest in understanding the mechanics of targeting, data collection and re-selling, and ad revenue sharing. If continued access to free web content is what consumers are after, this has to change. Not participating in the value exchange is not an option. Yet we continue to struggle to explain. We need to do a better job of explaining the options and the consequences of those choices. When we can more clearly explain the benefits of allowing third party data to be bought and sold, users, and our government, are much more likely to allow us to continue to do so.[10]

Some suggest that this value exchange *is* understood by most consumers. "We accept our loss of privacy in exchange for efficiency, convenience, and small price discounts," argue Hal Abelson, Ken Ledeen, and Harry Lewis, authors of *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*.[11] "We give away information about ourselves—voluntarily leave visible footprints of our daily lives—because we judge, perhaps without thinking about it very much, that the benefits outweigh the costs. To be sure, the benefits are many."[12]

But Kronengold is probably more correct in noting that this trade-off should be relatively apparent to most of us and yet it isn't. He is probably on to something when he suggests that online developers "need to do a better job of explaining the options and the consequences of those choices." In a sense, web publishers have let users enjoy an ad-supported free ride for a long time now and failed to "more clearly explain the benefits of allowing third party data to be bought and sold," as Kronengold suggests.

This must change. "During the next round of transparency innovation, we should focus on how to make apparent the value and risk of sharing data," says Betsy Masiello.[13] Greater transparency is an essential first step by web publishers and service developers to better inform their users of how the value proposition works, while also informing users about how they might better shield their data or privacy. As Jules Polonetsky and Christopher Wolf, co-chairs of the Future of Privacy Forum, have noted:

> Solving the privacy dilemma online may be as simple as companies simply fessing up the truth to consumers. We are here to help connect you to other people and to help sell you things you may like. Whether online or in the mall, a little honesty and transparency can go a long way.[14]

Online advertisers and service providers could make this value proposition/trade-off more explicit by putting a theoretical price tag on their content or services if they were forced to curtail data collection/advertising, and then let consumers

---

[10] Corey Kronengold, "Taking Issue: The Value of Privacy," *Digiday*, December 16, 2010, http://www.digidaydaily.com/stories/taking-issue-the-value-of-privacy.

[11] Hal Abelson, Ken Ledeen, and Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (Upper Saddle River, NJ: Addison-Wesley, 2008), 20.

[12] Abelson, Ledeen, and Lewis, *Blown to Bits*, 36.

[13] Betsy Masiello, "Deconstructing the Privacy Experience," *IEEE Security & Privacy*, July/August 2009, 70.

[14] Jules Polonetsky and Christopher Wolf, "Solving the Privacy Dilemma," *Huffington Post*, July 27, 2010, http://www.huffingtonpost.com/jules-polonetsky/solving-the-privacy-dilem_b_660689.html.

weigh privacy trade-offs against increased costs. Only then will we know the true value of privacy to consumers and their willingness to pay for it relative to the plethora of content and services they currently receive largely gratis.

In this regard, and as noted below, the Commission's long-standing efforts to push for better notice and transparency are admirable and should not be casually abandoned.[15] Nonetheless, strict contracting and consent models are not always possible in sectors that rely heavily upon advertising support, even if such norms are the ideal. Even in the analog era, much of the history of advertising and marketing was built on unwritten quid pro quos. For example, no contractual model or even "notice-and-choice" system has ever existed for most traditional forms of advertising (radio or television broadcasting, print, direct mail, billboards, etc.) There are steps consumers can take to avoid advertising and marketing in those contexts, but few of us would expect any sort of formal contact and consent form to be delivered to our attention beforehand. And opting out of those forms of advertising entirely is very difficult. One can avert their eyes (or ears) to some extent, but much of that advertising will still be "consumed" even though no one got their permission beforehand. Thus, while in an ideal world, consumers would understand perfectly the nature of such advertising quid pro quos and formally agree to them in advance, such textbook models of perfect information and informed consent are not always possible.[16]

Importantly, as Masiello has noted in an important recent essay with co-author Nicklas Lundblad, more formal opt-in consent models may have many trade-offs and downsides that need to be considered relative to opt-out models, which are more prevalent online currently.[17] "The decisions a user makes under an opt-in model are less informed" they argue, because "the initial decision to opt-in to a service is made without any knowledge of what value that service provides," and, therefore, "under an opt-in regime a decision can probably never be wholly informed."[18] "If instead of thinking about privacy decisions as requiring ex-ante consent, we thought about systems that structured an ongoing contractual negotiation between the user and service provider, we might mitigate some of these harmful effects," they argue.[19]

Bargaining with information as part of "an ongoing contractual negotiation" about online privacy and services is more sensible than a top-down regulatory regime that seeks to micromanage the consent process. A more open and experimental model of "information as currency" and "privacy bargaining" will ultimately better serve consumers and online content/service providers since it treats consent as context-sensitive matter and encourages beneficial experimentation and an ongoing learning process instead of rigid, overly legalistic, one-size-fits-all regulatory requirements.

Markets may already be organically moving in that direction through "social sign-on" and "permission-based marketing" systems, in which websites use "technologies, brands, retailers, publishers and other sites . . . to actively establish a permission-based relationship with their users and customers on their own websites."[20] This experimentation and the organic movement toward a "privacy marketplace" should be encouraged, not preempted, by the Commission.[21]

---

[15] Google has argued that, "effective notice is the key to any well-functioning privacy regime because it allows users to understand, and hopefully become comfortable with, the kind of information being collected and how it is used. Effective notice can actually alleviate consumer harms related to concern or anxiety about an organization's data practices." Pablo Chavez, *Comments of Google, Inc. to the U.S. Department of Commerce*, January 28, 2010, 7, http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=10FE3003-691B-4E2E-9685-87D7DB413C1D.

[16] "Unfortunately, there is no horn that sounds when consumers are sufficiently aware, or when their preferences are being honored." Jim Harper, "Understanding Privacy," 4.

[17] Nicklas Lundblad & Betsy Masiello, "Opt-In Dystopias," 7 *Scripted* 1*,* April 2010, http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

[18] Ibid., 161.

[19] Ibid., 162. Kent Walker has also argued that, "opt-in approaches burden everyone who wants the advantage of shared information and imperil the viability of the businesses that provide those advantages." Kent Walker, "The Costs of Privacy," 25 *Harvard Journal of Law & Public Policy*, no 87, (Fall 2001) 116.

[20] David A. Yovanno, "Why Permission Marketing Is the Future of Online Advertising," *Mashable*, February 3, 2011, http://mashable.com/2011/02/03/permission-marketing-social-data.

[21] "The privacy marketplace is already here, and there is every indication that as technology continues to evolve, an increasingly robust and valuable set of institutions will develop alongside it." Downes, "A Market Approach to Privacy Policy," 527.

On "Commonly Accepted Practices"

The Commission spends much time grappling with this question of how far law should go to delineate "commonly accepted practices" online. But instead of attempting to preordain practices that represent supposed privacy harms, ongoing experimentation should be allowed to determine what consumers may actually desire. "After all," noted the Department of Commerce in its recent *Commercial Data Privacy and Innovation in the Internet Economy* green paper, "the rate at which new services develop, and the pace at which consumers form expectations about acceptable and unacceptable uses of personal information, is measured in weeks or months."[22] In light of that truism, what counts as "commonly accepted practices" should be the byproduct of the spontaneous evolution of marketplace choices and interactions instead of top-down, one-size-fits-all mandates.[23] As the National Cable and Telecommunications Association (NCTA) has argued, "attempting to create a static list of such practices poses the risk of freezing pre-approved 'accepted' practices in place, potentially stifling the evolution of more effective or efficient practices or technologies."[24]

For example, the much-discussed practice of deep packet inspection (DPI) to create marketing profiles is viewed by many with suspicion, and the Commission says it should be preemptively disqualified from any list of "commonly accepted practices."[25] The Commission reaches this judgment without having conducted any serious cost-benefit analysis of the impact of the technology on privacy or marketplace competition/innovation.

But might consumers (and the Commission) look at DPI in a different light if an enterprising Internet service provider (ISP) offered massive discounts off monthly broadband bills—potentially even free monthly service—in exchange for DPI-enabled "tracking" and more targeted advertising? It will be easy for some regulatory advocates to dismiss such a scenario as too outrageous to even ponder, but would there not be some value to allowing consumers to make that choice over time for themselves?

The Commission seems unwilling to allow such experimentation to continue. Instead, it seems eager to get into the ugly business of delineating verboten technologies and information practices. In other words, the Commission is preemptively picking winners and losers instead of letting marketplace experimentation and consumer choices guide that process. As will be noted below, this could have a deleterious impact on technological evolution, innovation, marketplace competition, and overall consumer welfare.

The Mythical Harm of Consumer "Walk Aways"

The Commission also worries that "new types of harm may also emerge as technology develops" and specifically mentions "a consumer who 'walks away' from a social networking site because of privacy concerns loses the time and effort invested in building a profile and connecting with friends."[26] A similar claim was found in the Department of Commerce's (DoC) recent privacy report, which was also released in December.[27] The DoC report argued that "maintaining consumer trust is vital to the success of the digital economy" and that "an erosion of trust will inhibit the adoption of new technologies."[28]

---

22 U.S. Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, U.S. Department of Commerce Internet Policy Task Force (December 2010).

23 Lundblad and Masiello argue: "When information services are open and based on opt-out, there are incentives to provide users the best experience possible or they will take their information elsewhere. When these services are closed and based on opt-in, there are incentives to induce lock-in to prevent users from switching services." Ibid, 164.

24 National Cable and Telecommunications Association, *Reply Comments to the U.S. Department of Commerce*, January 28, 2011, 10-11. http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=17AF54FD-5201-474A-8EB8-E8B6071AEDEC

25 Federal Trade Commission, *Protecting Consumer Privacy*, 58.

26 Federal Trade Commission, *Protecting Consumer Privacy*, 32.

27 Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy*.

28 Ibid., 15.

The problem with the theory that online commerce or consumer interactions online are somehow being thwarted by a lack of more privacy regulation is that it is plainly contradicted by the facts. Interestingly, one need only scan back just a couple of paragraphs from where that claim is made in the DoC report to find some of those facts. The DoC report notes, for example: "The Internet is also increasingly important to the personal and working lives of individual Americans. Ninety-six percent of working Americans use the Internet as part of their daily life, while sixty-two percent of working Americans use the Internet as an integral part of their jobs."[29] Does the DoC not see the contradiction here or is it the case that the agency will not rest until the needle is moved from 96 percent to 100 percent?

But what of the DoC's claim that "an erosion of trust will inhibit the adoption of new technologies." If that is true, what are we to make of the 500 million people who have flocked to Facebook despite repeated claims by some that it is a privacy pariah?[30] And there are plenty of other examples of the explosion of online activity over the past decade. The fact is, online participation and technology adoption is growing like wildfire. Data sets from the Pew Internet & American Life Project about Internet usage over time illustrate the steady rise of online activity and participation of all sorts.[31] If there was anything to the theory that more regulation was needed to encourage consumers to get online, one of the first ways it would likely manifest itself would be in the field of online commerce or in online marketplaces, where the potential for fraud always exists. Yet, online commerce continues to grow exponentially. For example, eBay is now the world's largest online marketplace with more than 90 million active users globally and $60 billion in transactions annually, or $2,000 *every second*.[32]

There will always likely be a handful of individuals who fear online interactions because of a theoretical loss of privacy or security, but neither the FTC nor the DoC has produced any evidence that large numbers of citizens are waiting to get online until new privacy regulations are put on the books.

PRIVACY REGULATION IS AN INFORMATION-CONTROL REGIME THAT FACES FORMIDABLE ENFORCEMENT CHALLENGES

Before considering the potential shortcomings of the Commission's proffered regulatory solution, it is worth considering the formidable challenges that await any effort to clamp down on the flow of information on digital networks—even if that regime is pursued in the name of protecting consumer privacy. The administrative or enforcement burdens associated with modern information-control efforts are as important as the normative considerations at play here. Some of those practical considerations are itemized below.

Begin with a simple truism: Information control can be complex and costly. This 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 paled 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. 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 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.

---

29 Ibid., pg. 14.

30 Mark Zuckerberg, "500 Million Stories," *The Facebook Blog*, July 21, 2010, http://blog.facebook.com/blog.php?post=409753352130.

31 "Trend Data," Pew Internet & American Life Project, http://www.pewinternet.org/Trend-Data/Usage-Over-Time.aspx.

32 eBay, "Who We Are," http://www.ebayinc.com/who.

Each of these phenomena is facilitated by the underlying drivers of the information revolution: digitization, dramatic expansions in computing/processing power ("Moore's Law"), a steady drop of digital storage costs, and the rise of widespread Internet access and ubiquitous mobile devices and access.

Media & Technological Convergence

First, content platforms and information distribution outlets are blurring together today thanks to the rise of myriad new technologies and innovations. New digital communication tools and entities generally ignore or reject the distribution-based distinctions and limitations of the past. In other words, convergence means that information is increasingly being "unbundled" from its traditional distribution platform and can find many paths to consumers.[33]

For example, a piece of personal information voluntarily uploaded to a blog can be reproduced instantaneously on other blogs or on a social networking site (such as Facebook, LinkedIn, or MySpace), sent to Twitter (where it could be re-Tweeted countless times), or sent directly via email or text messages. Again, this can, and often does, happen within minutes, even seconds. If the information in question contains a picture or video, it can also be reproduced across countless sites virtually instantaneously.

As a result of media and technological convergence, 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.

In this way, technological convergence complicates efforts to create effective information-control regimes. This is will be just as true for privacy regimes as it is for other regulatory efforts.

Decentralized, Distributed Networking

Second, information creation, curation, storage, and dissemination are all increasingly highly decentralized and distributed in nature. Milton Mueller, author of *Networks and States: The Global Politics of Internet Governance*, notes that:

> Combined with liberalization of the telecommunications sector, the 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.[34]

For example, shutting down a website, blog, social networking site, *etc.*, to control information flows is often 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.[35] The current debate over Wikileaks and control of state secrets demonstrates how challenging it can be to put information back into the bottle once it is released.[36]

---

[33] Henry Jenkins, founder and director of the MIT Comparative Media Studies Program and author of *Convergence Culture: Where Old and New Media Collide*, defines 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." Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York: New York University Press, 2006), 2.

[34] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: The MIT Press, 2010), 4.

[35] "[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." Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2009), 113.

[36] "WikiLeaks copycats are quickly proliferating around the globe, beyond the U.S. government's effective reach." Jack Goldsmith, "Why the U.S. shouldn't try Julian Assange," *Washington Post*, February 11, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/10/AR2011021006324.html. Similarly, *Wall Street Journal* columnist Daniel Henninger has argued

By contrast, controlling information in the past could have been accomplished by smashing 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 controlling information flows. But this was facilitated by the highly centralized nature of those older systems or networks. Because modern digital technologies are far more decentralized and distributed, it complicates efforts to centralize information control. Hierarchical or top-down regulatory schemes must contend with the atomization of information and its mercurial nature within these modern digital systems.

Unprecedented Scale of Networked Communications

Third, in the past, the reach of speech and information was limited by geographic, technological, and cultural/language considerations. Today, by contrast, media can now flow across the globe at the click of a button because of the dramatic expansion of Internet access and broadband connectivity. Commentary and personal information that appears on a blog or a Twitter account in Tunisia is just as visible in Toledo or Tokyo. Offshore hosting of content also makes it harder to know where content originates or is stored.[37]

While restrictions by government are certainly still possible, the scale of modern speech and content dissemination greatly complicates government efforts to control information flows.

Explosion of the Overall Volume of Information

Fourth, the volume of media and communications activity taking place today also complicates regulatory efforts. In simple terms, there is just too much stuff for regulators to police today relative to 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 Downes, author of *The Laws of Disruption*.[38] Mueller concurs, noting: "The sheer volume of transactions and content on the Internet often overwhelms the capacity of traditional government processes to respond" to developments in this space.[39] Almost a decade ago, a blue ribbon panel assembled by the National Research Council to examine the regulation objectionable content had already concluded that, "The volume of information on the Internet is so large—and changes so rapidly—that it is simply impractical for human beings to evaluate every discrete piece of information for inappropriateness."[40]

The problem has only grown larger since then. IDC's 2009 report, *The Digital Universe Ahead—Are You Ready*?[41] offers the following snapshot of the digital "data deluge" that is upon us:

- Last year, despite the global recession, the Digital Universe set a record. It grew by 62 percent to nearly 800,000 petabytes. A petabyte is a million gigabytes. Picture a stack of DVDs reaching from the earth to the moon and back.

- This year, the Digital Universe will grow almost as fast to 1.2 million petabytes, or 1.2 zettabytes.

---

that, "There is one certain fix for the WikiLeaks problem: Blow up the Internet. Short of that, there is no obvious answer." Daniel Henninger, "WikiLeaks R Us," *The Wall Street Journal,* December 2, 2010, http://online.wsj.com/article/SB10001424052748704594804575648983975942008.html. For a more technical explanation of why it is probably impossible to shut down Wikileaks, see Danny Sullivan, "Why Wikileaks Will Never Be Closed or Blocked," *Search Engine Land*, December 8, 2010, http://searchengineland.com/why-wikileaks-will-never-be-closed-58226. Also see, Joby Warrick and Rob Pegoraro, "WikiLeaks avoids shutdown as supporters worldwide go on the offensive," *Washington Post*, December 8, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/08/AR2010120804038.html.

37 "The bits are everywhere; there is simply no locking them down, and no one really wants to do that anymore." Abelson, Ledeen, and Lewis, *Blown to Bits*, 68.

38 Larry Downes, *The Laws of Disruption* (New York: Basic Books, 2009), 69.

39 Mueller, *Networks and States*, 4.

40 Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, DC: National Academy Press, 2002), 187.

41 John Gantz and David Reinsel, "The Digital Universe Ahead—Are You Ready?" IDC, May 2010, http://idcdocserv.com/925.

- This explosive growth means that by 2020, our Digital Universe will be 44 times as big as it was in 2009. Our stack of DVDs would now reach halfway to Mars.

The Global Information Industry Center's report on *How Much Information*? also reports:

> 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.[42]

Also, a February 2011 study by Martin Hilbert and Priscila Lopez 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. That's equivalent to every person in the world receiving 174 newspapers every day."[43]

This "volume problem" for information control efforts will only grow more acute in coming years, especially when the next consideration is taken into account.

Unprecedented Individual Information-Sharing Through User-Generation of Content and Self-Revelation of Data

Finally, in this new world in which every man, woman, and child can be a one-person publishing house or self-broadcaster, restrictions on information uploading, downloading, or subsequent aggregation/use will be become increasingly difficult to devise and enforce.[44] This is particularly relevant to any discussion of privacy regulation since millions of individuals are currently placing massive volumes of personal information online—both about themselves and others.

The rapid rise of data self-revelation leads many scholars to puzzle about the existence of a so-called "privacy paradox." "People value their privacy, but then go out of their way to give it up," notes Downes.[45] "It is time to admit that we don't even really know what we want," say Abelson, Ledeen, and Lewis. "And we often want information to be made public to serve our own, or society's purposes."[46]

Regardless, slowing such information flows through public-policy steps will be remarkably challenging since 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, Facebook says users submit around 650,000 comments on the 100 million pieces of content served up *every minute* on its site.[47] And Hilbert and Lopez found that "Humankind shared

---

[42] *How Much Information? 2009 Report on American Consumers*, Global Information Industry Center, January 2010, http://hmi.ucsd.edu/howmuchinfo_research_report_consum.php.

[43] Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information," *Science*, February 10, 2011, http://annenberg.usc.edu/News%20and%20Events/News/110210Hilbert.aspx.

[44] "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," notes Yochai Benkler. "Individuals can reach and inform or edify millions around the world. Such a reach was simply unavailable to diversely motivated individuals before," he says. Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, CT: Yale University Press, 2006), 4

[45] Downes, *The Laws of Disruption,* 79.

[46] Abelson, Ledeen, and Lewis, *Blown to Bits*, 68, 70.

[47] Ken Deeter, "Live Commenting: Behind the Scenes," Facebook.com, February 7, 2011, http://www.facebook.com/note.php?note_id=496077348919.

65 exabytes of information in 2007, the equivalent of every person in the world sending out the contents of six newspapers every day."[48] 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 devices that capture and reproduce information instantaneously. For example, practically every teenager today carries a powerful digital "sensor" or surveillance technology in their pocket today: their mobile phones.[49] They use them to record audio and video of themselves and the world around them and instantaneously share it will the planet. They also use geolocation technologies to pinpoint the movement of themselves and others in real time. Meanwhile, new 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 information almost instantly provided to the user.[50] Eventually, these technologies will merge with "wearable computing" technologies in which biometric buttons on our shirts or coats will feed live streams of our daily movements and interactions into social networking sites and databases. We'll use them to record our days and play them back later, or perhaps to just instantly scan and recognize faces and places in case we cannot remember them.

Such technologies and ubiquitous information-sharing activities are not going away; they are growing rapidly and will be commonplace in short order. As a result, mountains of intimate data will be created, collected, collated, and cataloged about us *and by us* on a daily basis.

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."[51]

Taken together, the end result of these five phenomena, as David Friedman of Santa Clara Law School has noted, is that "Once information is out there, it is very hard to keep track of who has it and what he has done with it."[52]

THE COMMISSION'S PROPOSED "DO NOT TRACK" REGIME CREATES POTENTIAL RISKS TO CONSUMERS, CULTURE, COMPETITION, AND GLOBAL COMPETITIVENES

More tailored forms of online advertising and the "tracking" technologies which make them possible are coming under increasing scrutiny today. Some of this can be attributed to a general unfamiliarity with how online advertising works and the role personal information and data collection play in the process.[53] Although, as noted above, no clear case of harm has been established, some privacy fundamentalists who oppose virtually *any* form data collection have elevated this concern to near "techno-panic" levels and are now demanding regulation.[54]

---

48 Hilbert and Lopez, "The World's Technological Capacity to Store."

49 "Young people are turning to mobile devices in droves. They use them to post more information about themselves and their friends into the ether." John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books, 2008), 62.

50 http://www.google.com/mobile/goggles/#text.

51 Bhavishya Kanjhan, "Online Privacy is Dead and It Is a Good Thing," *Social Media Today*, June 14, 2010, http://socialmediatoday.com/index.php?q=SMC/206725.

52 David Friedman, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge, MA: Cambridge University Press, 2008), 62.

53 "Exaggerated fears are particular common regarding new technologies." Kent Walker, "The Costs of Privacy," 126. A recent report by the U.K. government noted that "New media are often met by public concern about their impact on society and anxiety and polarisation of the debate can lead to emotive calls for action." *Safer Children in a Digital World*, Byron Review on Children and New Technology, Department for Children, Schools and Families, [U.K.] task force report, March 2008, 3, http://www.dfes.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf.

54 "The privacy problem has morphed . . . into the latest terror of the digital ago, surpassing earlier shibboleths," argues Larry Downes. Downes, "A Market Approach to Privacy Policy," 510. Also see generally Adam Thierer, "Parents, Kids & Policymakers

As noted below, a variety of tools—such as browser-cookie controls or third-party plugins—already exist that can help consumers block targeted ads or limit data collection. But the Commission, likely inspired by regulatory advocates' claims of the complexity of those voluntary systems, is now pushing for additional steps to simplify or speed up the process. Hence, a "Do Not Track" mechanism has become the preferred universal fix, and one that the Commission is now pushing upon the marketplace. Do Not Track would demand that websites honor a machine-readable header indicating that the user did not want to be "tracked." In theory, this will allow privacy-sensitive web surfers to signal to websites that they would like to opt-out of any targeted advertising or not have any information about them collected when visiting sites.

The potential costs of such a regime will be explored in this section.

Potential Direct Cost to Consumers

The Commission poses a variety of questions regarding how a Do Not Track regime may be implemented and what its potential impact might be.[55] How many consumers would opt-out? How many would be willing to pay site subscriptions? How would it impact online publishers and advertisers? And so on. The truth is, nobody knows the answers to these questions, and the Commission has made no attempt to conduct a serious cost-benefit analysis of such a regime. Importantly, opinion polls cannot predict with accuracy how things will turn out once such a regime takes effect because consumer and marketplace reactions to real-world developments are more complex and nuanced than artificial surveys or experiments.[56]

What we do know is that online advertising today allows consumers to enjoy a veritable cornucopia of innovative, and mostly free, sites and services. Government regulation could "break" the implicit online quid pro quo currently governing online sites and services—that consumers enjoy a bevy of free content and services in exchange for tolerating ads and data collection—by creating what appears to be a cost-free choice option for consumers. That choice, however, will be anything but costless.

Lauren Weinstein, co-founder of People For Internet Responsibility (PFIR), worries that the "ability [of Do Not Track concepts] to cause major collateral damage to the Internet ecosystem of free Web services is being unwisely ignored or minimized by many Do Not Track proponents."[57] Weinstein is correct. There is no free lunch. While well-intentioned, government regulation that attempts to create a cost-free opt-out for data collection and targeted online advertising will likely have damaging unintended consequences. In terms of direct costs to consumers, Do Not Track could result in higher prices for service as paywalls go up or, at a minimum, advertising will become less relevant to consumers and, therefore, more "intrusive" in other ways.

Why might less relevant advertising represent a cost to consumers? It comes down to the value of their time and the benefits of relevant advertising to them. Ben Kunz, director of strategic planning at Mediassociates, a media planning and Internet strategy firm, argues that Do Not Track "won't stop online ads" but will instead simply lead to "tons of banners and videos everywhere online. They'll simply be less relevant."[58] *The Wall Street Journal* agrees, noting: "While many supporters of Do Not Track imagine that the opt-out would reduce the ads they see, the opposite would more likely occur, causing advertisers to blanket more media and use more intrusive techniques to reach the same number of potential

---

in the Digital Age: Safeguarding Against 'Techno-Panics,'" *Inside ALEC*, July 2009, 16-17, http://www.alec.org/am/pdf/Inside_July09.pdf.

55 Federal Trade Commission, *Protecting Consumer Privacy*, A-4.

56 See, e.g., Berin Szoka, "Privacy Polls v. Real-World Trade-Offs," 5 *Progress Snapshot* 10 (Washington, DC: The Progress & Freedom Foundation, October 8, 2009), http://www.pff.org/issues-pubs/ps/2009/ps5.10-privacy-polls-tradeoffs.html; Downes, "A Market Approach to Privacy Policy," 514.

57 Lauren Weinstein, "Risks in Mozilla's Proposed Firefox 'Do Not Track' Header Thingy," Lauren Weinstein blog, January 24, 2010, http://lauren.vortex.com/archive/000803.html.

58 Ben Kunz, "The $8 Billion Do Not Track Prize," *Bloomberg Businessweek*, December 22, 2010, http://www.businessweek.com/technology/content/dec2010/tc20101222_392883.htm.

customers."[59] When Google recently announced it would be offering a "Keep My Opt-Outs" extension to its Chrome web browser to come into line with the FTC's desire for more Do Not Track mechanisms, the company also noted that "once you install the Keep My Opt-Outs extension, your experience of online ads may change: You may see the same ads repeatedly on particular websites, or see ads that are less relevant to you."[60] Thus, Do Not Track "will stop marketers from serving up ads for products you may actually want," Kunz notes.[61] This represents a direct cost to consumers in terms of the hassle of unwanted, intrusive (or "spammy") advertising.

But it is the potential for prices to rise for online content and services that is the most important direct cost to consumers. If paywalls go up and subscriptions are required as a result of the new Do Not Track regime, Corey Kronegold of *Digiday* suggests the response of users could take one of two forms:[62]

1. Users (especially those who are highly privacy sensitive) might gladly accept the trade-off and pay something more for those sites and services instead of having data collected or ads served; or

2. Users might revolt against the resulting paywalls, subscriptions, micropayment schemes, tiered services, etc, and demand government intervention in the name of "fairness." We might even hear talk of "gouging" and calls for price regulation, even though developers would have no choice but to raise prices to cover costs in the absence of advertising support.

Some mix of the two could be the end result, but the latter scenario seems far more likely. "If we move too far one way, the people supplying the free content will get together and say we aren't going to supply the content for free," says Dilip DaSilva, chief executive of Exponential Interactive, owner of the Tribal Fusion online advertising network. "It's not like the publishers will offer free content to people who visit their site but don't want ads tracking them."[63]

Of course, there is nothing wrong with online sites and service providers charging for what they offer consumers, but, as Kronegold suggests, if regulation moves the marketplace in that direction unnaturally, many consumers *will* likely have a problem with it since they have grown accustomed to an abundance of "free" online services. It is impossible to determine what prices online providers might seek to charge for their services, but anything more than the $0.00 they currently charge will likely come as a shock to many consumers. As discussed in the following section, it will also have profound repercussions on the broader availability of much content and many of the services consumers take for granted. In this sense, Do Not Track becomes a "privacy tax" on consumers, requiring them to pay for things they previous received inexpensively, or for free.[64]

There are other costs associated with the process of creating paywalls and setting prices that will be borne by online content providers and consumers, as Commissioner William Kovacic noted in his statement on the Commission's privacy report:

> Setting prices is costly; if willingness to pay to avoid tracking varies substantially, the informational requirements to set access prices will be large. For a number of content providers, a price-for-content model is likely to provide less revenue than monetization via advertising; that most websites choose an ad-driven model rather than a direct fee model suggests that the former is a more efficient means than

---

[59] "The Internet Browsing Cops," January 21, 2011, http://online.wsj.com/article/SB10001424052748704723104576061900000013690.html

[60] Sean Harvey and Rajas Moonka, "Keeping Your Opt-Outs," *Google Public Policy Blog*, January 24, 2010, http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

[61] Kunz, "The $8 Billion Do Not Track Prize."

[62] Corey Kronengold, "Taking Issue: The Value of Privacy," *Digiday*, December 16, 2010, http://www.digidaydaily.com/stories/taking-issue-the-value-of-privacy.

[63] Quoted in Tanzina Vega and Verne Kopytoff, "In Online Privacy Plan."

[64] "We might better think of a privacy tax—we pay the regular price *unless* we want to keep information about our food, alcohol, and pharmaceutical purchases from the market; to keep our habits to ourselves, we pay extra." Abelson, Ledeen, and Lewis, *Blown to Bits*, 11.

> the latter to monetize content in most circumstances. At the margin—which may be large—forcing firms away from their revealed-preferred method of monetization may reduce revenue and hence degrade quality. In discussing whether website content might be degraded by consumers choosing not to be tracked, how, if at all, should such risks impact the Commission's analysis?[65]

How much content will go behind paywalls? Dan Castro of the Information Technology & Innovation Foundation fears much will:

> If a Do Not Track list ever became widely implemented companies could respond by simply blocking access to those sites for users who opt out, just as some sites today block users who use ad-blocking software or do not register on a site. Users who currently opt out of targeted advertising but continue to use the content or service which the advertising pays for are essentially free riders. They are the minority of users who are benefitting from the willingness of the majority to divulge some personal information in exchange for free or reduced-price content. It is this exchange that enables the U.S. Internet ecosystem to be so robust and largely free of charge to the average user. Privacy advocates rarely acknowledge the harm to advertising revenues that would result from a large number of consumers signing up for Do Not Track.[66]

Another alternative short of paywalls would be interstitial pop-ups warning consumers they must first disable Do Not Track before they are allowed to use portions of the site, or perhaps any of it.[67] In other words, sites may seek to formalize the previously unwritten quid pro quo of information as currency. Some Do Not Track regulatory advocates try to assuage such concerns by pointing to the existence of widespread online website registration or site "login" procedures today, which do not generally require user to disable settings (such as cookie-blocking or ad-blocking) or pay anything before using site content/services. For example, Arvind Narayanan of Stanford University argues:

> I do not believe that disabling DNT as a requirement for service will become anywhere near as prevalent as logging in as a requirement for service. I bring up login only to make the comforting observation there seems to be a healthy equilibrium between sites that require login always, some of the time, or never.[68]

Ultimately, however, this observation provides little comfort since it ignores the fact that Do Not Track could be preemptively breaking business models on an unprecedented scale, thus forcing vast numbers of online publishers to make uncomfortable trade-offs going forward if they wish to provide the current level of service or expanded options. Narayanan may end up being correct and a highly tiered, permission-based Internet may not be erected. But, as the next section notes, that is a risky bet and one that could have profound consequences for the future online content and the richness of its culture.

Potential Indirect Costs/Impact on Content & Culture

Direct monetary cost to consumers is not the only issue here. The indirect impact of regulation on content and culture must also be considered.

---

65 Concurring Statement of Commissioner Kovacic, in Federal Trade Commission, *Protecting Consumer Privacy*, D-4.

66 Daniel Castro, "Policymakers Should Opt Out of 'Do Not Track'," Information Technology & Innovation Foundation, November 2010, 3, www.itif.org/files/2010-do-not-track.pdf.

67 Ironically, depending on how such permission systems are structured, this may actually end up forcing consumers to reveal *more* information about themselves to many sites as a condition of access content or services on those sites.

68 Arvind Narayanan, "'Do Not Track' Explained," *33 Bits of Entropy*, September 30, 2010, http://33bits.org/2010/09/20/do-not-track-explained.

While targeted online advertising only accounted for $1.1 billion in 2010, it has been growing at healthy 20 percent clip, estimates eMarketer.[69] "Factor in the use of data to determine marketing efficiencies and that figure could be as high as $7 billion to $8 billion of the $25 billion online ad spend," says Katy Bachman of *AdWeek*.[70] Larry Ponemon, chairman of the Ponemon Institute, which studies privacy and security issues, told the *New York Times* that "Privacy fears are definitely having an economic impact" on the market, especially the uncertain legal and regulatory environment and the threat of regulation.[71] A May 2010 Ponemon Institute survey of senior marketing executives with 90 diverse organizations that were actively engaged in online marketing found that:

> 63 percent of those we surveyed said behavioral advertising generated their *greatest return on investment*. Yet 98 percent told us that, because of consumers' privacy fears, their companies are curtailing investments in online behavioral targeting. These companies are willing to sacrifice the revenue they believe they can generate through an online campaign rather than risk the potential hit to brand reputation for being as aggressive as they would like to be. Overall that curtailment has kept more than $600 million out of the behavioral targeting industry.[72]

This matters because it represents foregone investment in new forms of content, culture, and services. Media economists and industry experts have long realized that advertising is the great sustainer of media.[73] Advertising benefits society by subsidizing the creation of news, information, and entertainment. "Advertisers are critical to the success of commercial media because they provide the primary revenue stream that keeps most of them viable," argues Robert G. Picard, author of *The Economics and Financing of Media Companies.*[74] Mary Alice Shaver of the University of Central Florida puts this support in context: "Advertising revenues pay for virtually all broadcast media, 70% to 80% of support for newspapers and an equally high percentage for magazines."[75]

Importantly, advertising is proving increasingly to be the only business model with any real staying power for many media and information-producing sectors. Pay-per-view mechanisms, micropayments, and even subscription-based business models are all languishing.[76] Consequently, the overall health of modern media marketplace and the digital economy—and the aggregate amount of information and speech that can be produced or supported by those sectors—is fundamentally tied up with the question of whether policy makers allow the advertising marketplace to evolve in an efficient, dynamic fashion.[77] In this sense, it is not hyperbole to say that an attack on advertising is tantamount to an attack on media itself.[78]

---

69 David Hallerman, "Audience Ad Targeting: Data and Privacy Issues," eMarketer, February 2010, http://www.emarketer.com/Reports/All/Emarketer_2000636.aspx.

70 Bachman, "(Ad) Apocalypse Soon."

71 Quoted in Steve Lohr, "Privacy Concerns Limit Online Ads, Study Says," *New York Times,* April 30, 2010, http://bits.blogs.nytimes.com/2010/04/30/privacy-concerns-limit-online-ads-study-says.

72 Larry Ponemon, "Fear and Loathing in Online Advertising," Ponemon Institute blog, May 3, 2010, http://www.ponemon.org/blog/post/fear-and-loathing-in-online-advertising.

73 For a summary, see Adam Thierer, "Unappreciated Benefits of Advertising and Commercial Speech," *Mercatus on Policy* 86 (Arlington, VA: Mercatus Center at George Mason University), January 2011, http://mercatus.org/publication/unappreciated-benefits-advertising-and-commercial-speech.

74 Robert G. Picard, *The Economics and Financing of Media Companies* (Bronx, NY: Fordham University Press, 2002), 122.

75 Mary Alice Shaver, "The Economics of the Advertising Industry," in Alison Alexander, *et. al., Media Economics: Theory and Practice* (Mahwah, NJ: Lawrence Erlbaum Associates, Third Edition, 2004), 250.

76 To some extent, these are all just variations of a fee-for-service business model. "Micropayments," for example, would require a small payment for each media unit accessed or downloaded, such as $1 per news article or song.

77 Much of the valuable information content available on the Internet, and so many of the useful services we use every day, is free," explains Larry Downes, "not because of some utopian dream of inventors or even because of the remarkably low transactions costs of the digital economy. The content is free because the costs of the services—blogs, stock quotes, even home movies posted on YouTube—are underwritten by advertisers. If we don't read and respond to ads, we'll have to pay for these services some other way," he notes. Downes, *The Laws of Disruption,* 83-4.

78 See Adam Thierer, Berin Szoka, and W. Kenneth Ferree, *Comments of the Progress & Freedom Foundation in the Matter of the Federal Communications Commission's Examination of the Future of Media and Information Needs of Communities In a Digital Age*, The Progress & Freedom Foundation, May 5, 2010, 28-38, http://www.pff.org/issues-pubs/testimony/2010/2010-05-05-Comments_in_FCC_Future_of_Media_proceeding.pdf.

A March 2010 study on "The Value of Behavioral Targeting," conducted by Howard Beales on behalf of the Network Advertising Initiative, demonstrates how this could be the case.[79] Beales, the former Director of the Bureau of Consumer Protection at the FTC, found that advertising rates are significantly higher for behaviorally targeted ads, with the average return on behaviorally targeted advertising being just over twice that of other advertising. The reason that greater return on investment is important, Beales notes, is because:

> Advertising using behavioral targeting is more successful than standard run of network advertising, creating greater utility for consumers from more relevant advertisements and clear appeal for advertisers from increased ad conversion. Finally, a majority of network advertising revenue is spent acquiring inventory from publishers, making behavioral targeting an important source of revenue for online content and services providers as well as third party ad networks.[80]

This illustrates how more effective advertising can cross-subsidize and sustain online content and culture. More and better advertising means more and better content and services will be made available to consumers. Beales concluded his study by noting: "Increasingly, advertising is the financing mechanism that makes online content and services possible as well. As content traditionally provided offline (such as newspapers) continues to move to the Internet, the link between online advertising and content is likely to become increasingly vital to the provision of information and services that we have long taken for granted."[81]

With these insights in mind, it is peculiar that the Commission ignores the connection between this proceeding and another FTC proceeding which poses the question, "How Will Journalism Survive the Internet Age?"[82] That is a fair question for the FTC to ask, and one that the Federal Communications Commission has also been pondering in a series of workshops on "The Future of Media."[83] What the Commission proposes in this proceeding certainly will not help matters any and it begs the question: If not advertising, then what will sustain online media, digital age culture, and social networking services going forward?[84]

John Battelle is blunter in his assessment of how damaging this move could be to online culture:

> [D]on't come crying to me when you realize that in opting out of our marketing-driven world, you've also opted out of, well, a pretty important part of our ongoing cultural conversation, one that, to my mind, is getting more authentic and transparent thanks to digital platforms. And, to my mind, you've also opted out of being a thinking person capable of filtering this stuff on your own, using that big ol' bean which God, or whoever you believe in, gave you in the first place. Life is a conversation, and part of it is commercial. We need to buy stuff, folks. And we need to sell stuff too.[85]

This is a simplified explanation of the value exchange that drives the Internet, but Battelle is correct that if heavy-handed regulation replaces common sense or the current online quid pro quo of information-for-services, then something must give. While the idea of a cost-free opt-out model for the all online data collection/advertising may sound seductive to

---

79 Howard Beales, "The Value of Behavioral Targeting," Network Advertising Initiative, March 2010, www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

80 Ibid., 1.

81 Ibid., 18.

82 Federal Trade Commission, "How Will Journalism Survive the Internet Age?" *Workshop Series*, 2010, http://www.ftc.gov/opp/workshops/news/index.shtml. All filing made to the Commission in the proceeding are located here: http://www.ftc.gov/os/comments/newsmediaworkshop/index.shtm.

83 Federal Communications Commission, "Future of Media," http://reboot.fcc.gov/futureofmedia.

84 Castro goes even further, arguing that "If the goal of the initiative is to restrict targeted advertising, it would be better for Congress to just ban Internet advertising outright and develop a 'Corporation for Public Internet' to fund Internet content and applications." Castro, "Policymakers Should Opt Out of 'Do Not Track'," 4.

85 John Battelle, "Thurs. Signal: Go On, Opt Out. Just Don't Come Cryin' To Me . . ." *Federated Media Publishing*, December 1, 2010, http://www.federatedmedia.net/blog/2010/12/thurs-signal-go-on-opt-out-just-dont-come-cryin-to-me.

some, it is vital to take into account the opportunity costs of such regulation. The real world is full of trade-offs and there is no such thing as a free lunch.

Competition & Market Structure

The Commission does not need to be reminded that it was created in large part to safeguard competition. This proceeding, however, threatens to tip the balance in favor of existing technologies or market players over future ones.[86] *AdWeek*'s Katy Bachman argues that:

> Heavy-handed privacy legislation could actually curb competition by crippling ad networks that serve ads to niche Web sites dependent on advertising to fund content. Web sites would have to resort to pay models in a medium where free content is the norm. No doubt the big brands would still draw contextual advertising, but that would come at the expense of new, emerging brands, thus squelching competition in a space that has thrived on it.[87]

Similarly, Tanzina Vega and Verne Kopytoff of *The New York Times* have noted that:

> The Federal Trade Commission's proposed privacy mechanism could cause a major shift in the online advertising industry, as companies that have relied on consumers' browsing history try to make up for what could be billions in lost revenue.
>
> If the vast majority of online users chose not to have their Internet activity tracked, the proposed "do not track" system could have a severe effect on the industry, some experts say. It would cause major harm to the companies like online advertising networks, small and midsize publishers and technology companies like Yahoo that earn a large percentage of their revenue from advertising that is tailored to users based on the sites they have visited.
>
> Under a situation where many users opt out of being tracked, other companies, like Google, may take a much smaller hit because the vast majority of its revenue comes through search ads that would not be affected by a do-not-track mechanism. Microsoft, which also sells display advertising through its ad network, could also survive a hit to user data collection since it earns revenue from sources other than advertising, including software and gaming, experts say.[88]

"In a setting where first-party advertising is allowable but third-party marketing is not, substantial advantages may be created for large incumbent firms," argue Avi Goldfarb and Catherine Tucker.[89] "For example, if a large website or online service were able to use its data to market and target advertising, it will be able to continue to improve and hone its advertising, while new entrants will find it difficult to challenge the incumbent's predominance by compiling other data or collecting their own data," they conclude.[90]

---

[86] "Regulation that disfavors one technology or business model would also deter entry, thwart innovation, and limit competition and choice in the sale of online advertising." Joan Gillman, *Testimony before the House Energy & Commerce Committee, Hearing on Do Not Track Legislation: Is Now the Right Time?* December 2, 2010, 5, http://energycommerce.house.gov/hearings/Testimony.aspx?TID=4184.

[87] Katy Bachman, "(Ad) Apocalypse Soon," *AdWeek*, December 19, 2010, http://www.adweek.com/aw/content_display/esearch/e3i9f75082f2f627711694ca34d9b326105.

[88] Tanzina Vega and Verne Kopytoff, "In Online Privacy Plan, the Opt-Out Question Looms," *New York Times,* December 5, 2010, http://www.nytimes.com/2010/12/06/business/media/06privacy.html.

[89] Avi Goldfarb and Catherine Tucker, "Comments on 'Information Privacy and Innovation in the Internet Economy,'" *Comments to the U.S. Department of Commerce*, January 24, 2011, 4, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NTIA_comments_2011_01_24.pdf.

[90] Ibid.

And Kunz fears that "the 'Long Tail' of niche content is going to get crushed" since "thousands of small websites may disappear as dollars flow to consolidated publishing centers." "Do Not Track will send billions of dollars to the big online publishers, hurting the little sites you might find most interesting. The second point is painful. It could really harm you, too, dear consumer, if you read things online other than *The New York Times*, Bloomberg, or iVillage.com."[91] This should hardly be surprising since economists have long recognized that "advertising typically benefits new entrants and small firms more than it does large, established firms,"[92] and that is likely to be the case for targeted online advertising since it would be the easiest way for niche sites to find interested consumers and advertisers.

Thus, the risk exists that a Do Not Track mandate could steer markets in unnatural, inefficient directions by erecting new barriers to entry or directly picking technological winners and losers.[93] If so, the Commission will have failed in its mission to safeguard competition and improve consumer welfare.

International Competitiveness

Some advocates of intervention on this front do not hide their desire to move the United States in a direction the European Union has followed with "data directives" and more stringent forms of privacy regulation. But America's refusal thus far to walk down that more regulatory path offers scholars the chance to evaluate Europe's more-restrictive approach and study whether America's lead in the global digital marketplace might be tied to its more "hands-off" approach to online regulation. A recent study by Goldfarb and Tucker found that "after the [European Union's] Privacy Directive was passed [in 2002], advertising effectiveness decreased on average by around 65 percent in Europe relative to the rest of the world."[94] They argue that because regulation decreases ad effectiveness, "this may change the number and types of businesses sustained by the advertising-supporting Internet." Regulation of advertising and data collection for privacy purposes, it seems, can affect the global competitiveness of online firms.

This is what makes talk of "harmonization" among privacy regimes so dangerous. It threatens to undermine America's competitive advantage in the global digital arena. It is hard to find many European counterparts that rival Google, Amazon, Apple, Facebook, eBay, Microsoft, or other market leaders. Why is it that the information technology sector has thrived in America and that U.S. companies are leaders in many of their respective sectors across the globe? Might it be precisely because the U.S. did *not* follow others down the path of "data directives" and heavy handed, top-down regulation of the Internet more generally? "If applied to American companies, these European laws would restrict the breakneck innovation of the commercial web," argues the NetChoice Coalition.[95] And Yahoo! correctly summarizes:

> It is no coincidence that the U.S. is the birthplace of most of the widely used global websites and online services. Our legal frameworks encourage innovation through reasonable liability regimes, controls on harmful uses of information, promotion of a diversity of online voices, security requirements based on

---

91 Kunz, "The $8 Billion Do Not Track Prize."

92 Thomas M. Lenard and Paul H. Rubin, *Privacy and the Commercial Use of Personal Information* (Washington, DC: The Progress & Freedom Foundation, 2002), xxii.

93 As the National Cable and Telecommunications Association (NCTA) noted in comments to the Department of Commerce: "In a nascent and highly dynamic market characterized by rapid technological change such as online advertising, any regulation that favors or disfavors one technology or business model over another could seriously thwart innovation and the development of new business models that could benefit consumers, content providers, and advertisers, by prematurely locking market participants into one sanctioned approach. Moreover, limiting online advertising to specified designated permissible techniques would deter new entry, and limit competition." National Cable and Telecommunications Association, *Reply Comments to the U.S. Department of Commerce*, January 28, 2011, 10-11. http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=17AF54FD-5201-474A-8EB8-E8B6071AEDEC.

94 Avi Goldfarb and Catherine Tucker, "Privacy Regulation and Online Advertising," 57 *Management Science* 1, (January 2011), 57-71, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.

95 Steve DelBianco and Braden Cox, *NetChoice Reply Comments on Department of Commerce Green Paper*, January 28, 2011, 7, http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=1EA98542-23A4-4822-BECD-143CD23BB5E9.

> the sensitivity of the data, and a light regulatory hand that favors and recognizes complementary roles for industry self-regulation.[96]

The Department of Commerce's recent privacy green paper says America should look to "prevent conflicting policy regimes from serving as a trade barrier."[97] But should the U.S. impose burdensome new regulations on American companies to achieve that goal? Would we really be better off if all U.S. firms and policy more closely resembled the E.U. in this regard?

Some privacy advocates posit the need for greater "interoperability" or harmonization of privacy policies internationally to facilitate smoother online commercial interactions or data flows. Yet, the Commerce Department's recent privacy green paper notes that "a considerable amount of global commerce takes place on the Internet [and] global online transactions currently total an estimated $10 trillion annually" and is growing. Still, it continues on to claim that "the lack of cross-border interoperability in privacy principles and regulations creates barriers to cross-border data flow and significant compliance costs for companies,"[98] and repeats the argument for harmonization.

There are three problems with that theory. First, it assumes that the benefits of regulatory harmonization—*which, to be perfectly clear, would arrive in the form increased regulation on U.S. operators*—would outweigh the cost of complying with those new rules.

Second, there is no reason that harmonization could not work in the *opposite* direction. If the Commerce Department, the FTC, and other U.S. lawmakers want to promote U.S. trade, exports, commerce, and global competitiveness, the proper way to "leveling the playing field" in this context should be the same as it is in relation to speech policy or trade law: the rest of the world should follow America's lead; the U.S. should absolutely not regulate up to achieve parity with theirs.

Which raises a final problem with the argument for harmonization of privacy regimes through increased regulation on U.S. businesses: it sets a horrible precedent. At least thus far this has not been the approach the U.S. government has taken in most other Internet policy contexts, and with good reason. Consider this in the context of speech controls. When policy makers in Europe and other regions or countries stifle free speech and expression online, America's response has not been to mimic them but, rather, to lead by example. That is, when confronted with conflicting regulatory regimes abroad, our response has usually been to proudly boast to the world that we have the more sensible approach to Internet regulation, which is to say, it should be tightly limited so as not to stifle speech or commerce. Some critics might label this "American exceptionalism," but it is really just common sense if we hope to promote the international competitiveness of U.S. online businesses and remain a global leader in this arena.

"Silver-Bullet" Solutions Rarely Adapt or Scale Well

Finally, there is the more general normative problem of the Commission seeking a simple solution to a complex "problem" such as online privacy protection. Do Not Track fits into a long line of proposed silver-bullet solutions that would mandate a "universal" solution to a complicated economic or social issue.

When it comes to such information-control efforts, there aren't many good examples of simple fixes or silver-bullet solutions that have worked, at least not very long. Consider the illusive search for a solution to online pornography. The PICS/ICRA experience is instructive in this regard. PICS and ICRA refer to the W3C's Platform for Internet Content Selection[99] and Internet Content Rating Association.[100] For a time, there was hope that voluntary metadata tagging and content labeling could be used to screen objectionable content on the Internet. But the sheer volume of material to be dealt

---

96 Anne Toth, *Comment of Yahoo! on "Commercial Sata Privacy and Innovation in the Internet Economy,* January 28, 2011, 2, http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=F6A50C0B-00CC-44A6-B475-FE218170CA02.

97 Department of Commerce, *Commercial Data Privacy and Innovation,* 20.

98 Ibid.

99 http://www.w3.org/PICS.

100 http://www.fosi.org/icra.

with made that task almost impossible. The effort has been abandoned now.[101] Of course, it is true that effort did not have a government mandate behind it to encourage more widespread adoption, but even if it would have, it is hard to believe that all pornography or other objectionable content would have been labeled and screened properly.

In a similar way, The CAN-SPAM Act aimed to curtail the flow of unsolicited email across digital systems and, 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 percent of all emails were spam.[102] "Spam pages," are also a growing concern. In January 2011, Blekko, a new search engine provider, created a "Spam Clock" to track new spam pages and found 1 million new spam pages were being created *every hour*.[103]

Similar problems await information control efforts in the privacy realm, even if a mandated Do Not Track mechanism required the re-engineering of web browser architecture and/or standards. "It's a single response to an overly-simplified set of choices we encounter on the web," notes the NetChoice Coalition, which represents e-commerce companies.[104] 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.[105] "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. "There is no reliable way of ensuring this technology is being used, however," says Sidney Hill of *Tech News World.* "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."[106]

Importantly, Do Not Track would not slow the "arms race" in this arena as some seem to hope or suggest.[107] If anything, as noted in more detail below, a Do Not Track mandate will speed up that arms race and have many other unintended consequences.[108] Complex definitional questions also remain unanswered, such as how define and then limit "tracking" in various contexts, as well as how to enforce such a regime. Lauren Weinstein summarizes some of the most obvious issues:

> Sending out a new "Do Not Track" header—even beyond basic associated technical requirements at the client and server ends—and even if there's agreement on how that header is defined—tells you nothing about what actually happens to that header after being sent by the client browser. How does the user who sends such a header actually confirm that they're "not being tracked" as a result? And how do they know that continued tracking isn't caused by a technical issue that prevented the header from ever being received and processed by the destination server?

---

[101] http://www.icra.org.

[102] Royal Pingdom, "Internet 2010 in Numbers," January 12, 2011, http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers.

[103] http://www.spamclock.com. Also see, Danny Sullivan, "Blekko Launches Spam Clock To Keep Pressure On Google," *Search Engine Land*, January 7, 2011, http://searchengineland.com/blekko-launches-spam-clock-to-keep-pressure-on-google-60634.

[104] Steve DelBianco and Braden Cox, *NetChoice Reply Comments on Department of Commerce Green Paper*, January 28, 2011, 14, http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=1EA98542-23A4-4822-BECD-143CD23BB5E9.

[105] Michael Fertik, *Comments of Reputation.com, Inc. to the U.S. Department of Commerce*, January 28, 2011, 12, http://www.reputation.com/blog/2011/01/31/reputation-com-comments-commerce-department-privacy-green-paper.

[106] Sidney Hill, "Internet Tracking May Not Be Worth the Headaches," *Tech News World*, December 29, 2010, http://www.technewsworld.com/story/Internet-Tracking-May-Not-Be-Worth-the-Headaches-71543.html.

[107] Some examples: "The header-based Do Not Track system appeals because it calls for an armistice in the arms race of online tracking." Rainey Reitman, "Mozilla Leads the Way on Do Not Track," *Deeplinks*, Electronic Frontier Foundation, January 24, 2011, https://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track. Similarly, Chris Soghoian argues that "opt out mechanisms . . . [could] finally free us from this cycle of arms races, in which advertising networks innovate around the latest browser privacy control." Christopher Soghoian, "What the U.S. Government Can Do To Encourage Do Not Track," *Slight Paranoia*, January 27, 2011, http://paranoia.dubfire.net/2011/01/what-us-government-can-do-to-encourage.html. Finally, Arvind Narayanan of Stanford University argues that Do Not Track, "is a way to move past the arms race between tracking technologies and defense mechanisms, focusing on the actions of the trackers rather than their tools." Arvind Narayanan, "'Do Not Track' Explained," *33 Bits of Entropy*, September 30, 2010, http://33bits.org/2010/09/20/do-not-track-explained.

[108] "Too often, well-intentioned efforts to regulate technology are far worse than the imagined evils they were intended to prevent." Abelson, Ledeen, and Lewis, *Blown to Bits*, 159.

> Perhaps the header line was "eaten" by an intermediate proxy server (it's quite common for proxies not to pass along all headers). Or maybe the header reached a server that simply hadn't been modified to recognize it yet. Or did the header reach a server in some jurisdiction (say, outside of the U.S.) that wouldn't even be "required" to know about that new header? And so on.
>
> You can't just send a Do Not Track header and expect meaningful results. In practice, you end up having to build an entire confirmation apparatus of some sort—and even then it's likely to be a mess. Without confirmation, you can send out whatever headers you wish, but when you don't get the results you expect, what does that mean? Who knows? This all gets very complicated, very quickly.[109]

Moreover, in light of the global nature of online commerce and speech, Do Not Track will not scale as well as advocates hope.[110] Castro says:

> Another problem with Do Not Track is that it does not scale well on the global Internet. As described above, to 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.[111]

Again, as noted previously, the regulatory experience with spam, objectionable content, and copyrighted content suggest serious challenges lie ahead because of the borderless nature of online activity / commerce.

Implications of This New Regime in Other Contexts

A final danger with the FTC's proposed Do Not Track information-control regime is that it could also establish a precedent for other forms of Internet regulation. If, in the context of privacy policy, "opt-in" becomes the new default norm or mechanisms such as Do Not Track become the preferred top-down mandate, similar regulatory norms might be expected in other contexts. Why not mandatory "opt-in" for other types of speech or content? For example, should the presence of potentially objectionable content across digital networks be used as an excuse for greater regulation of the Internet?

That is not the way things currently work, of course. At least in the United States, we demand that personal and parental responsibility be the first and primary line of defense against unwanted communications or content. Why should it be any different when it comes to "privacy" concerns?[112]

Consider how things work in the context of speech and content regulation, American jurisprudence has become a fairly settled matter: people (or parents) are expected to take responsibility for unwanted information flows in their lives (or the lives of their children). Under current law, it is assumed that the many user-empowerment tools on the market (filters, monitoring software, other parental-control technologies) constitute a so-called "less-restrictive means" of controlling content when compared to government regulation.

---

[109] Lauren Weinstein, "Risks in Mozilla's Proposed Firefox "Do Not Track" Header Thingy," Lauren Weinstein blog, January 24, 2010, http://lauren.vortex.com/archive/000803.html.

[110] "Many behavioral targeting companies are based outside the US—making legislation ineffective," says Doug Wolfgram, CEO of IntelliProtect, an online privacy management company. Quoted in Tony Bradley, "Why Browser 'Do Not Track' Features Will Not Work," *Computerworld*, February 10, 2011, http://news.idg.no/cw/art.cfm?id=ACE91A0E-1A64-6A71-CE2572C981C0204A.

[111] Castro, "Policymakers Should Opt Out of 'Do Not Track'," 3.

[112] The Cato Institute's Jim Harper argues: "Privacy is not a gift from politicians or an entitlement that can be demanded from government. Privacy is a product of personal responsibility. Like moral living, privacy is the product of careful consideration and concerted effort by individuals. To be sure, protecting privacy can be hard. It involves knowledge, vigilance, and constant trade-offs." Harper, "Understanding Privacy," 5.

Many privacy advocates—such as the ACLU, the Center for Democracy & Technology, and the Electronic Frontier Foundation—vociferously endorse this "less-restrictive means" test or "educate and empower" paradigm in the free-speech context. Generally speaking, when it comes to speech regulation, they rightly argue "household standards" (user-level controls) should trump "community standards" (government regulation). And in court they repeatedly employ the "less-restrictive means" test to counter government efforts to regulate information flows.

When it comes to privacy, however, many of them abandon this vision. For some reason, when the topic of debate shifts from concerns about potentially objectionable content to the free movement of personal information, personal responsibility and self-regulation become the *last* option, not the first. What is most troubling about this is that those advocates could be unwittingly undermining the power of the "less-restrictive means" test more generally, which is a vitally important barrier to greatly enhanced government control of cyberspace. That is, when privacy advocates ignore, downplay, or denigrate user-empowerment tools, they are essentially saying self-help is the right answer in one context, but not the other.

That is a shame because, as discussed below, self-help tool work well in both contexts. And the same arguments used against private parental-empowerment technologies are often trotted out in opposition to privacy controls. Can privacy tools be confusing at times or difficult to set up? Yes, they can, but no more so that parental-control tools. Are privacy tools as effective as parental-control tools? In some ways privacy tools are actually *more* effective because in the case of parental controls, the person you are attempting to "protect" (namely, kids) often have a stronger incentive to evade/defeat those tools. Moreover, privacy-enhancing controls can be very effective—perhaps even *too effective*—at shutting down unwanted information flows. Whether it is ad-blocking tools, cookie controls, or encryption techniques, these tools can actually be far more effective blocks on information flows than, say, Internet filters meant to block porn or hate speech, which is also more subjective by nature.

Of course, no technological empowerment tool or solution is perfect. But as the Supreme Court held in *United States v. Playboy*, empowerment tools need not be perfect to be preferable to government regulation. "Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests," the court held.[113] Moreover, "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."[114]

Again, the exact same principle should hold for privacy regulation[115] Why not expect those especially privacy-sensitive users who object to targeted online advertising to do something about it? To the extent effective self-help privacy tools exist, they provide a means of solving policy problems that is not only "less restrictive" than government regulation but generally more *effective* and customizable as well. Why settle for one-size-fits-all solutions of incomplete effectiveness when users can quite easily and effectively manage their own privacy? Indeed, those who advocate personal responsibility and industry self-regulatory approaches to free-speech and child-protection issues should be advancing the same position with regards to privacy.

PRIVACY REGULATION RAISES SERIOUS FREE SPEECH AND PRESS FREEDOM ISSUES

As the Commission continues its push for a new regulatory regime for online privacy, it is important to acknowledge that important free-speech values are at stake here and to understand how increased privacy controls could conflict with them. "Recognizing that we are legislating in the shadow of the First Amendment suggests a powerful guiding principle for

---

113 *United States v. Playboy Entertainment Group*, 529 U.S. 803, 815 (2000).

114 Ibid., 824.

115 Chapman University Law Professor Tom Bell has argued the same principle should hold in both contexts. Tom W. Bell, "Internet Privacy and Self-Regulation: Lessons from the Porn Wars," *Briefing Paper* 65 (Washington, DC: Cato Institute, August 9, 2001), http://www.cato.org/pub_display.php?pub_id=1504.

framing privacy regulations," argues Kent Walker. "Like any laws encroaching on the freedom of information, privacy regulations must be narrowly tailored and powerfully justified."[116]

Ironically, many privacy advocates are strongly critical of copyright law and claim that, as currently structured, it represents an unjust or excessive information control regime. Yet, privacy regulation would constitute a stronger information control regime by creating the equivalent of copyright law for personal information, which would, in turn, conflict mightily with the First Amendment.

In his recent book *Skating on Stilts*, Stewart Baker reminds us that the famous 1890 Samuel Warren and Louis Brandeis *Harvard Law Review* essay on "The Right to Privacy"[117]—which is tantamount to a sacred text for many modern privacy advocates—was heavily influenced by copyright law. As Baker explains:

> 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: "the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds." . . . Brandeis thought that the way to ensure the strength of his new right to privacy was to enforce it just like state copyright law. If you don't like the way "your" private information is distributed, you can sue everyone who publishes it.[118]

Incidentally, it is important to recall that their call for such a regime was essentially driven by a desire to censor the press. In their article, Warren and Brandeis argued that:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.[119]

So angered were Warren and Brandeis by reports in daily papers of specifics from their own lives that they were led to conclude that:

> [M]an, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[120]

It is unclear how one could have greater "pain and distress" inflicted by words than "by mere bodily injury," and yet the law review article that essentially gave birth to American privacy law articulated such a theory of harm. And it only follows, then, that they would advocate fairly draconian controls on speech and press rights if they felt this strongly.[121]

---

[116] Kent Walker, "The Costs of Privacy," 123.

[117] Samuel Warren and Louis Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193 (1890)

[118] Stewart Baker, *Skating on Stilts* (Hoover Institution Press, 2010) 319, http://www.skatingonstilts.com/files/chapter-13---skating-on-stilts-by-stewart-baker-3.pdf.

[119] Ibid.

[120] Ibid.

[121] In this sense, Warren and Brandeis were attempting to enshrine into American law what the norm across the Atlantic in many European states: The elevation of privacy, or "dignity" rights, over speech or liberty rights. *See* James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," 113 *Yale Law Journal* (2004), 1151-1221.

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 freedom of speech. As Eugene Volokh argued in a 2000 law review article entitled, "Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking about You":

> The difficulty is that the right to information privacy—the right to control other people's communication of personally identifiable information about you—is a right to have the government stop people from speaking about you. And the First Amendment (which is already our basic code of "fair information practices") generally bars the government from "control[ling the communication] of information," either by direct regulation or through the authorization of private lawsuits.[122]

This is what makes the Commission's effort to untether privacy regulation from a harms-based model or mode of analysis so troubling. For example, the Commission says that "the FTC's harm-based approach also has limitations [because] it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives."[123] The Commission then suggests that "for some consumers, the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there,'" and suggests "consumers may feel harmed when their personal information . . . is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations."[124]

Not only does the Commission fail to offer any data on how this supposed harm manifests itself, how severe it is, or what trade-offs it presents to society, but it utterly fails to account for the dangerous slippery slope of speech control it puts us on.[125] If appeals for regulation are based on emotion instead of concrete evidence of consumer harm, where will this take us next? If, for example, the Commission is to regulate based upon the fact that "consumers may feel harmed . . . when their personal information . . . in a manner that is contrary to their expectations," how long will it be before some suggest this standard should trump First Amendment rights in other contexts?[126]

For example, this more emotional approach to privacy regulation brings us one step closer to a "right not to be offended" or a "right to be forgotten," as some in Europe favor.[127] How could a journalist even conduct their business in such a world? By their very nature, good reporters are nosy and, to some extent, disregard the privacy of the people and institutions they report on.[128]

This is why privacy regulation must not be reduced to amorphous claims of "dignity" rights, where an assertion by a small handful that they "feel harmed" comes to replace a strict showing of actual harm to persons or property. To go down that path would have grave consequences for the future of freedom of speech, transparency, openness, and accountability.

BETTER, LESS-RESTRICTIVE SOLUTIONS TO PRIVACY-RELATED CONCERNS

---

122 Eugene Volokh, "Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You," 52 *Stanford Law Review*, 1049 (2000).

123 Federal Trade Commission, *Protecting Consumer Privacy,* 20.

124 Ibid.

125 For further discussion of the trade-offs at work between speech and privacy, see: Adam Thierer, "Book Review: Solove's *Understanding Privacy*," *Technology Liberation Front*, November 8, 2008, http://techliberation.com/2008/11/08/book-review-soloves-understanding-privacy.

126 "A continuing border war is likely to be waged, however, along an existing free speech front: the line separating my right to tell the truth about you from your right not to have that information used against you. In the realm of privacy, the digital explosion has left matters deeply unsettled." Abelson, Ledeen, and Lewis, *Blown to Bits*, 70.

127 Adam Thierer, "The Conflict Between a 'Right to Be Forgotten' & Speech / Press Freedoms," *Technology Liberation Front*, November 5, 2010, http://techliberation.com/2010/11/05/the-conflict-between-a-right-to-be-forgotten-speech-press-freedoms.

128 As Singleton has noted, "Journalists have no general obligation to get anyone's permission before writing a story about her activities, even though that story and the details of the person's life that they report may be very personal and are sold for commercial value. Journalists have often used information available over computer networks to develop and track important news stories. . . . No general 'consent' requirement applies. Singleton, *Privacy as Censorship*, 7.

As noted previously, it is not unreasonable to expect privacy-sensitive consumers to exercise some degree of personal responsibility to avoid unwanted content or communications in this context, just as they must in the context of objectionably content or online child safety.[129] Luckily, a variety of less-restrictive alternatives exist that are superior to the regulatory approach the Commission is considering.

Education, Empowerment, & Self-Regulation

The Commission rightly notes that education must still be the first line of defense. The Commission's outstanding "OnGuard Online" 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.[130] Many companies and trade associations are also taking steps to raise awareness among their users about they can better protect their privacy and security. Other nonprofits—including many privacy advocates—offer instructional websites and video explain how privacy-sensitive consumers can take steps to protect their personal information online.

More importantly, the market for digital "self-help" tools continues to expand quite rapidly. Commenting on the *EDiscovery Map* blog, Monique Altheim notes how strange it is that, compared to recent E.U. privacy white papers, "None of the U.S. proposals mention the use of PET (Privacy Enhancing Technologies) as an alternative and additional tool to ensure consumer privacy."[131] This oversight is unfortunate since "consumers today can technically prevent tracking by using cookie settings or browser based options or third party browser plug-ins which limit the data that is shared by their browsing activity," notes the Future of Privacy Forum.[132]

Indeed, 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. Consider some of the amazing privacy-enhancing tools and information already available on the market today:

- "Ad preference managers" have caught on with major search companies. Google,[133] Microsoft,[134] and Yahoo![135] all offer easy to use opt-out tools and educational webpages that clearly explain to consumers how digital advertising works.[136] Meanwhile, DuckDuckGo offers as alternative search experience that blocks data collection altogether.[137]

- Major browser providers also offer "private browsing" mode, which allows users to turn on a "stealth browsing mode" to avoid data collection/tracking. This functionality is available as a menu option in Microsoft's Internet Explorer ("InPrivate Browsing"[138]) and Google's Chrome ("Incognito")[139] and Mozilla's Firefox ("Private Browsing"[140]). Firefox also has many add-ons available that provide the functional equivalent to stealth mode or

---

129 "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." Palfrey and Gasser, *Born Digital*, 70.

130 http://www.onguardonline.gov.

131 Monique Altheim, "The Recent Privacy Framework Proposals, The Internet of Things and PET," *EDiscovery Map*, January 12, 2011, http://ediscoverymap.com/2011/01/the-recent-privacy-framework-proposalsthe-internet-of-things-and-pet.

132 http://www.futureofprivacy.org/2011/01/24/breaking-news-firefox-do-not-track-advances.

133 http://www.google.com/ads/preferences.

134 http://choice.live.com/Default.aspx and https://choice.live.com/AdvertisementChoice/Default.aspx.

135 http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html.

136 Microsoft Advertising AdCenter: http://advertising.microsoft.com/home?s_cid=us_msn_footer; Yahoo! Privacy Center: http://info.yahoo.com/privacy/us/yahoo; Google Privacy Center: http://www.google.com/privacy/ads.

137 http://duckduckgo.com/privacy.html. Also see, Jennifer Valentino-DeVries, "Can Search Engines Compete on Privacy?" *Wall Street Journal*, January 25, 2011, http://blogs.wsj.com/digits/2011/01/25/can-search-engines-compete-on-privacy.

138 http://www.microsoft.com/windows/internet-explorer/features/safer.aspx?tab=6.

139 http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95464.

140 http://support.mozilla.com/en-US/kb/Private%20Browsing.

offers additional functionality.[141] "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."[142]

- 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 ones include: Ghostery,[143] NoScript,[144] Cookie Monster,[145] Better Privacy[146], Track Me Not,[147] and the Targeted Advertising Cookie Opt-Out or "TACO"[148] (all for Firefox); No More Cookies[149] (for Internet Explorer); Disconnect (for Chrome);[150] AdSweep (for Chrome and Opera);[151] CCleaner[152] (for PCs); and Flush[153] (for Mac). New empowerment solutions are constantly turning up.[154] 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.[155]

- The success of one particular program, AdBlockPlus, deserves special mention. AdBlockPlus, which lets users blocks advertising on most websites, the most-downloaded add-on for both the Firefox and Chrome web browsers.[156] As of February 2011, roughly 110 million people (roughly 900,000 per week) had downloaded the Adblock Plus add-on for the Firefox web browser.[157] Incidentally, both Adblock Plus and NoScript, which is the third-most popular download on Firefox, support the Do Not Track protocol.[158]

- Finally, pressured by the Commission and privacy advocates, all three of those browser-makers (Microsoft,[159] Google,[160] and Mozilla[161]) 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. These developments build

---

141 https://addons.mozilla.org/en-US/firefox/tag/incognito.

142 Dennis O'Reilly, "Add 'Do Not Track' to Firefox, IE, Google Chrome," *CNetNews.com*, December 7, 2010, http://news.cnet.com/8301-13880_3-20024815-68.html.

143 https://addons.mozilla.org/en-US/firefox/addon/ghostery.

144 https://addons.mozilla.org/en-US/firefox/addon/noscript.

145 https://addons.mozilla.org/en-US/firefox/addon/cookie-monster.

146 https://addons.mozilla.org/en-US/firefox/addon/betterprivacy.

147 https://addons.mozilla.org/en-US/firefox/addon/trackmenot.

148 There are multiple versions of the TACO add-on available for Firefox web browser.

149 http://download.cnet.com/No-More-Cookies/3000-2144_4-10449885.html.

150 http://www.disconnectere.com.

151 https://addons.opera.com/addons/extensions/details/adsweep/2.0.3-3/?display=en.

152 http://www.piriform.com/ccleaner.

153 http://www.macupdate.com/app/mac/32994/flush.

154 David Gorodyansky, "Web Privacy: Consumers Have More Control Than They Think," *The Huffington Post*, December 30, 2010, http://www.huffingtonpost.com/david-gorodyansky/web-privacy-consumers-hav_b_799881.html.

155 http://www.reputation.com/myprivacy.

156 https://adblockplus.org/en.

157 https://addons.mozilla.org/en-US/firefox/addon/adblock-plus.

158 http://hackademix.net/2010/12/28/x-do-not-track-support-in-noscript.

159 Dean Hachamovitch, "IE9 and Privacy: Introducing Tracking Protection," Microsoft *IE Blog*, December 7, 2010, 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*, January 25, 2010, http://blogs.msdn.com/b/ie/archive/2011/01/25/update-effectively-protecting-consumers-from-online-tracking.aspx.

160 Sean Harvey and Rajas Moonka, "Keeping Your Opt-Outs," *Google Public Policy Blog*, January 24, 2010, http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

161 Stephen Shankland, "Mozilla Offers Do-Not-Track Tool to Thwart Ads," *CNet News Deep Tech*, January 24, 2011, http://news.cnet.com/8301-30685_3-20029284-264.html; Julia Angwin, "Web Tool On Firefox To Deter Tracking," *Wall Street Journal*, January 24, 2011, http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html.

on industry-wide efforts by the Network Advertising Initiative and the "Self-Regulatory Program for Online Behavioral Advertising"[162] to make opting-out on targeted advertising simpler. This latter effort, which was announced last fall, 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.[163] Their program uses an "Advertising Option Icon" to highlight a company's use of targeting advertising and gives consumers an easy-to-use opt-out option. It was accompanied by an educational initiative, www.AboutAds.info, which offers consumers information about online advertising.[164] The independent Council of Better Business Bureaus will enforce compliance with the system. 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.

What these developments illustrate is a well-functioning marketplace at work that is evolving to offer consumers greater control over their privacy without upending online markets or destroying the quality of the browsing experience. Thus, the Commission 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.

Importantly, it is vital to realize that most consumers will never take advantage of these empowerment tools, much as the vast majority of parental control technologies go untapped by most families.[165] This cannot possible be used as determination of "market failure" or the need for government regulation, however. What matters is that the tools exist for those who wish to use them, not the actual uptake/usage of those tools.

"Simplified" Privacy Policies, Enhanced Notice, & "Privacy by Design"

In various portions of the Commission's report, the agency stresses the benefits of "simplified" privacy policies.[166] The Commission complains that "the notice-and-choice model, as implemented, as led to long, incomprehensible privacy policy that consumers typically do not read, let alone understand."[167]

No doubt, more clearly worded privacy policies would be a welcome development. As Google has noted in a filing to the Department of Commerce, "Consumers 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."[168] Nonetheless, there are other considerations that must be taken into account.

First, in noting that consumers do not necessarily read or understand every word of a company's privacy policy, the Commission seemingly implies a state of market failure exists. But that should not be the standard upon which a determination of "market failure" exists. Consider how other transparency or disclosure policies or regulatory mandates have worked out. Do consumers really fully understand each and every proviso contained in the stacks of paper placed in front of them when they sign a home mortgage (even with the Truth in Lending Act disclosure requirements in place)? The same is true for life insurance policies, which are full of incomprehensible provisions and stipulations, even though

---

[162] http://www.aboutads.info.

[163] *Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data For Online Behavioral Advertising*, October 4, 2010, www.networkadvertising.org/pdfs/Associations104release.pdf.

[164] http://www.aboutads.info/principles.

[165] Adam Thierer, "Who Needs Parental Controls? Assessing the Relevant Market for Parental Control Technologies," *Progress on Point* 16.5, The Progress & Freedom Foundation, February 27, 2009, http://www.pff.org/issues-pubs/pops/2009/pop16.5parentalcontrolsmarket.pdf.

[166] Federal Trade Commission, *Protecting Consumer Privacy*, 19, 26, 70.

[167] Federal Trade Commission, *Protecting Consumer Privacy*, iii.

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

regulations govern those policies as well. The same is also true of mandatory FDA disclosures on pharmaceuticals. Finally, do consumers read and understand every provision of their car loan or warranty? In each case, far more is at stake for consumers than whatever "risk" they face by not fully comprehending online privacy policies. We must learn to tolerate a certain amount of "rational ignorance" as it pertains to privacy policies. In other words, while increased transparency should always be welcomed, people value their time and often ignore those disclosure policies for a variety of reasons. Increased "simplification" of privacy policies is not going to magically make them start reading them.

Second, will the highly litigious nature of America's legal system allow for simplification of privacy policies? By its very nature, simplification likely entails less specificity about what the legal obligations of either party are. Thus, some companies will rightly fear that a move toward more "simplified" privacy policies opens them up to potentially greatly legal liability.

If the agency persists in its effort to force the "simplification" of privacy policies, therefore, it may need to craft and extend to site operators some sort of safe-harbor provision 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 don't" position. Satisfying regulators' desire for simplicity will simply open them to attacks by trial lawyers 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 design." There's already been amazing strides made in this regard, and progress—while slow—will continue. "The signs are already beginning to appear," says Ann Cavoukian, who is widely credited with coining the term. "[M]arket leaders are embracing *Privacy by Design*, and are, in turn, reaping the benefits,"[169] she notes.

Increased Sec. 5 Enforcement, Targeted Statutes & The Common Law

Perhaps, then, the best of all worlds would be to work to continuously improve existing privacy policies, ensuring that they are accompanied by clearer notice about specific data collection practices, and then to hold companies to the promises they make to their customers.[170] As Commissioner Rosch argues, "if there is anything wrong with the 'notice' model, it is that we do not enforce it stringently enough."[171] The Commission report notes that it has already brought and settled many cases involving its Section 5 authority to police unfair and deceptive practices.[172] This should continue to be the baseline legal norm.[173] Again, as Commissioner Rosch notes, "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."[174]

Commissioner Kovacic also mentions that the Commission's report fails to provide much context regarding the role of tort, property, and contract law as they pertain to privacy enforcement and data security.[175] We have only just begun to

---

169 Ann Cavoukian, "2011: The Decade of Privacy by Design Starts Now," *ITBusiness.CA*, January 15, 2011, http://blogs.itbusiness.ca/2011/01/2011-the-decade-of-privacy-by-design-starts-now.

170 "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." Palfrey and Gasser, *Born Digital*, 73-74.

171 Concurring Statement of Commissioner J. Thomas Rosch, in Federal Trade Commission, *Protecting Consumer Privacy*, at E-6-7.

172 Federal Trade Commission, *Protecting Consumer Privacy*, 45.

173 "[S]ince 1996 the 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 for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury." Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Ground and On the Books," 63 *Stanford Law Review* (January 2011), 127, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385.

174 Concurring Statement of Commissioner J. Thomas Rosch, in Federal Trade Commission, *Protecting Consumer Privacy*, E-2.

175 "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. Companies that store information about users should be held to a

explore the interaction of these systems as they pertain to online privacy. That evolutionary learning process should not be preempted by a top-down regulatory regime that suffocates further marketplace *or legal* experimentation and innovation.

Other targeted statutes and regulations are also already on the books to address specific concerns. On its website, the Commission itemizes those rules it already enforces[176] and they include: the Truth in Lending Act, the Fair Credit Billing Act, the Fair Credit Reporting Act, the Electronic Fund Transfer Act, the Consumer Leasing Act, the Children's Online Privacy Protection Act (COPPA), the Health Breach Notification Rule (2009), among others. Other laws exist and are enforced by other agencies, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

In sum, a plethora of privacy-related laws and anti-fraud/disclosure statutes and regulations already exist. Before adding more to the books, perhaps more focused enforcement efforts should be pursued using existing authority.

CONCLUSION

In closing, while it remains impossible to predict with precision the impact a new privacy regulatory regime will have the Internet economy and digital consumers, regulation *will* have consequences; of that much we can be certain.

As the Commission and other policy makers move forward with proposals to expand regulation in this regard, it is vital that the surreal "something-for-nothing" quality of current privacy debate cease. Those who criticize data collection or online advertising and call for expanded regulation should be required to provide a strict cost-benefit analysis of the restrictions they would impose upon America's vibrant digital marketplace.

In particular, it should be clear that the debate over Do Not Track and online advertising regulation is fundamentally tied up with the future of online content, culture, and services. Thus, regulatory advocates must explain how the content and services supported currently by advertising and marketing will be sustained if current online data collection and ad targeting techniques are restricted.

The possibility of regulation also retarding vigorous marketplace competition—especially new innovations and entry—is also very real. Consequently, the Commission bears the heavy burden of explaining how such results would be consistent with its long-standing mission to protect consumer welfare and promote competition. Importantly, the "harm" that critics claim online advertising or data collection efforts gives rise to must be shown to be concrete, not merely conjectural. Too much is at stake to allow otherwise.

Finally, as it pertains to solutions for those who remain sensitive about their privacy online, education and empowerment should trump regulation. Regulation would potentially destroy innovation in this space by substituting a government-approved, "one-size-fits-all" standard for the "let-a-thousand-flowers-bloom" approach, which offers diverse tools for a diverse citizenry.[177] Consumers can and will adapt to changing privacy norms and expectations, but the Commission should not seek to plan that evolutionary process from above.[178]

---

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." Palfrey and Gasser, *Born Digital*, 79. Also see Concurring Statement of Commissioner Kovacic, in Federal Trade Commission, *Protecting Consumer Privacy*, D-1.

[176] Federal Trade Commission, "Advertising and Marketing on the Internet: Rules of the Road," http://business.ftc.gov/documents/bus28-advertising-and-marketing-internet-rules-road.

[177] "Even if we sympathize with the general idea that we should use the law to protect our privacy, we have to acknowledge that well-intentioned but overly broad or badly drafted laws can do more harm than good in a quicksilver technological environment." Palfrey and Gasser, *Born Digital*, 78.

[178] "But society is an adaptive organism; it adjusts to new values, rebalances the old ones, and usually bends without breaking." Computer Science and Telecommunications Board, *Global Networks and Local Values: A Comparative Look at Germany and the United States* (Washington, DC: National Academy Press, 2001), 56.