MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

TESTIMONY

A STATUS UPDATE ON THE DEVELOPMENT OF VOLUNTARY DO-NOT-TRACK STANDARDS

BY ADAM D. THIERER
Senior Research Fellow

Testimony before the Senate Committee on Commerce, Science & Transportation

April 24, 2013

Mr. Chairman and members of the Committee, thank you for inviting me here today to comment on the important issues of online privacy policy and commercial data collection. My name is Adam Thierer and I am a senior research fellow at the Mercatus Center at George Mason University, where I study Internet policy issues in the Mercatus Center's Technology Policy Program.

My message here today, condensed from two recent law review articles,[1] boils down to three points:

1. First, no matter how well-intentioned, *restrictions on data collection could negatively impact the competitiveness of America's digital economy, as well as consumer choice*.

2. Second, *it is unwise to place too much faith in any single, silver-bullet solution to privacy*, including "Do Not Track," because such schemes are easily evaded or defeated and often fail to live up to their billing.

3. Finally, with those two points in mind, *we should look to alternative and less costly approaches to protecting privacy* that rely on education, empowerment, and targeted enforcement of existing laws. Serious and lasting long-term privacy protection requires a layered, multifaceted approach incorporating many solutions.

1. Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J. L. & PUB. POL. 409 (2013), papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680; Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON UNIV. L. REV., (forthcoming, Summer 2013).

For more information or to meet with the scholar, contact
Taylor Barkley, (703) 993-8205, tbarkley@mercatus.gmu.edu
Mercatus Center at George Mason University, 3351 Fairfax Drive, 4th Floor, Arlington, VA 22201

TRADE-OFFS ASSOCIATED WITH RESTRICTIONS ON DATA COLLECTION

Let's be more specific about the potential costs of restrictions on data collection. Online advertising and data collection are the fuel that powers our information economy. Privacy-related mandates that curtail the use of data to better target ads or services could have several deleterious effects.[2]

First, **data restrictions could raise *direct* costs for consumers** if walled gardens and paywalls are erected in response. Something has to pay for all the wonderful free sites and services we enjoy today.

Second, **data restrictions could *indirectly* cost consumers by diminishing the abundance of content and culture now supported by data collection and advertising**. In other words, even if prices and paywalls don't go up, overall quantity or quality could suffer if data collection is restricted.[3]

Third, **data restrictions could hurt the competitiveness of domestic markets**. While regulation raises the costs of doing business for all online operators, those costs will fall hardest on smaller operators and new start-ups.[4] For example, today's "app economy" has given countless small innovators a chance to compete on even footing with the biggest players.[5] Burdensome data collection restrictions could short-circuit the engine that drives entrepreneurial innovation among mom-and-pop companies if ad dollars get consolidated in the hands of only the larger companies that can afford to comply with new rules.[6]

Fourth, **data restrictions could undermine America's global competitive advantage in this space**. We should ask ourselves how it is that America's Internet sector came to be the envy of the world and why it is so hard to

2. See generally Adam Thierer & Berin Szoka, *The Hidden Benefactor: How Advertising Informs, Educates & Benefits Consumers, Progress & Freedom Foundation*, PROGRESS SNAPSHOT, Feb. 2010; Berin Szoka & Adam Thierer, *Online Advertising & User Privacy: Principles to Guide the Debate, Progress & Freedom Foundation*, PROGRESS SNAPSHOT, Sept. 2008.

3. A 2010 study by Howard Beales, the former Director of the Bureau of Consumer Protection at the FTC, found that "the price of behaviorally targeted advertising in 2009 was 2.68 times the price of run of network advertising." That increased return on investment is important, Beales notes, because it creates "greater utility for consumers from more relevant advertisements and clear appeal for advertisers from increased ad conversion." Beales also noted that, "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." Howard Beales, Network Advertising Initiative, *The Value of Behavioral Targeting*, at 1 (March 2010), www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

4. "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 Professors Avi Goldfarb and Catherine Tucker. "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." Avi Goldfarb & Catherine Tucker, *Comments on 'Information Privacy and Innovation in the Internet Economy*,' Comments to the US Department of Commerce, Jan. 24, 2011, at 4, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NTIA_comments_2011_01_24.pdf.

5. "The App Economy now is responsible for roughly 466,000 jobs in the United States, up from zero in 2007 when the iPhone was introduced." Michael Mandel, *Where the Jobs Are: The App Economy*, (TechNet, Feb. 7, 2012) http://www.technet.org/wp-content/uploads/2012/02/TechNet-App-Economy-Jobs-Study.pdf.

6. Apple's Safari browser already blocks third-party cookies and now Mozilla's Firefox browser will as well. This has led to concerns about how market structure and competition will be impacted. See: Tim Peterson, *The Demise of Third-Party Cookies Could Help Premium Publishers*, ADWEEK, Apr. 15, 2013, http://www.adweek.com/news/technology/demise-third-party-cookies-could-help-premium-publishers-148573: "First Safari and now Firefox are blocking third-party companies from dropping cookies on publishers' sites to protect users' privacy. Those moves hurt revenues of the smaller publishers that depend on third parties to sell ads. But, paradoxically, the winners could be premium publishers and large media companies, especially Facebook and Google, who will be able to prop up their proprietary audience data as the ideal alternative. Big traditional publishers whose ad revenue has shrunk as readers and advertisers shift online could recoup their losses by parlaying their first-party audience data into even higher ad rates"; Adam Lehman, *Don't Fear the Cookie Backlash*, DIGIDAY, Apr. 17, 2013, http://www.digiday.com/platforms/dont-fear-the-cookie-backlash: "Several people have already pointed out that the Mozilla [third-party cookie restriction] change will create even greater advantages for the largest players in digital media."

name any major Internet company from Europe.[7] Our more flexible, light-touch regulatory regime leaves more room for competition and innovation compared to Europe's top-down regime.[8]

UNINTENDED CONSEQUENCES OF DO NOT TRACK

Generally speaking, when it comes to privacy protection, **we should avoid placing excessive faith in schemes like Do Not Track** because they could fail, just as previous techno-fixes failed to keep pace with fast-moving developments in this space.

[*See* Appendix I: "Techno-'Silver-Bullet' Solutions Don't Work—Some Case Studies."]

Even if Do Not Track takes root and some consumers turn it on, many will be incentivized by ad networks or publishers to opt right back in to "tracking" to retain access to sites and services they desire.[9] In doing so, they may end up sharing even more information than they do today.[10] Moreover, this may drive still greater consolidation since larger players will be in a position to grant Internet-wide opt-in exceptions, while smaller providers cannot.[11]

CONSTRUCTIVE ALTERNATIVES TO REGULATION

In light of these trade-offs, **we should subject new data restrictions to strict benefit-cost analysis** to ensure that we are not imposing unnecessary burdens on our data-driven economy.[12]

We should simultaneously consider how **we might better spend our time and resources developing a richer mosaic of privacy-enhancing tools and educational strategies**. Luckily, an extensive array of such tools and strategies already exists.[13]

[*See* Appendix II: "Digital Self-Help Tools."]

7. Goldfarb and Tucker have also 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." They argue that because regulation decreases ad effectiveness, "this may change the number and types of businesses sustained by the advertising-supporting Internet." The European Union's experience makes it clear that regulation of online advertising and data collection can affect market structure, competitive rivalry, and the global competitiveness of online firms. This could also have antitrust implications that the FTC or other agencies would need to take into account when considering new privacy rules. Goldfarb & Tucker, *Comments on 'Information Privacy*,' 4.
8. Adam Thierer, *A Better, Simpler Narrative for U.S. Privacy Policy*, TECHNOLOGY LIBERATION FRONT, Mar. 19, 2013, http://techliberation.com/2013/03/19/a-better-simpler-narrative-for-u-s-privacy-policy.
9. Berin Szoka, *The Paradox of Privacy Empowerment: The Unintended Consequences of "Do Not Track*," Position paper for W3C Workshop: Do Not Track and Beyond Berkeley, California, (Nov. 26-27, 2012), http://www.w3.org/2012/dnt-ws/position-papers/5.pdf.
10. See Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7:1 SCRIPTed 155, (2010), http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp, noting that as a result of a push for stronger-opt-in regimes, "service providers may attempt to maximise data collection in every instance that they are forced to use an opt-in framework; once a user consents to data collection, why not collect as much as possible? And the increased transaction costs associated with opt-in will lead service providers to minimise the number of times they request opt-in consent. In combination these two behaviours are likely to lead to an excessive scope for opt-in agreements. In turn, users will face more complex decisions as they decide whether or not to participate."
11. Szoka, The Paradox of Privacy Empowerment, 3.
12. I have explained how to conduct such an analysis in my forthcoming article, Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON UNIV. L. REV., (forthcoming, Summer 2013).
13. They include: ad preference managers, "private browsing" tools, ad-blocking technologies, cookie-blockers, web script blockers, encryption and web proxy tools, and reputation protection services.

Web browser providers continue to experiment with different privacy defaults,[14] and while the World Wide Web Consortium (W3C) continues to pursue a single Do Not Track standard, innovators in the marketplace have already made private Do Not Track tools a reality.[15]

It is worth noting that **almost all of these tools are available free of charge**, and no barrier to widespread adoption exists.[16] As is the case with online safety concerns,[17] **citizens have access to many tools and methods that let them protect their privacy as they see fit**, and evidence suggests they already actively do so.[18]

ALTERNATIVE ENFORCEMENT APPROACHES

Finally, where serious privacy harms are documented, **the Federal Trade Commission already possesses broad enforcement authority** to police unfair and deceptive practices and has recently been using it more aggressively.[19] Targeted federal statutes already exist to address sensitive issues related to health,[20] financial,[21] and children's privacy.[22] Enforcement alternatives are also available through state courts, including torts,[23] contract law,[24] and

14. Megan Geuss, *Firefox 22 Will Block Third-Party Cookies*, Ars Technica, Feb. 23, 2013, http://arstechnica.com/business/2013/02/firefox-22-will-block-third-party-cookies; Alexis Santos, Microsoft Sets 'Do Not Track' as Default on IE10, Ruffles Feathers, ENGADGET, June 1, 2012, http://www.engadget.com/2012/06/01/do-not-track-is-default-on-ie10.
15. Online privacy company Abine offers a "Do Not Track Plus," which it claims blocks more than 600 trackers. See http://www.abine.com/dntdetail.php.
16. The only serious objection to this bottom-up, user empowerment-based approach is that it could inconvenience users by making it more difficult to use some sites or slow down their browsing experience in some fashion. But it is no more an inconvenience than it is to use parental control tools so that your kids won't see or download objectionable content.
17. Adam Thierer, Progress & Freedom Foundation, *Parental Controls & Online Child Protection: A Survey of Tools*, Version 4.0, Summer 2009, http://www.pff.org/parentalcontrols.
18. The Pew Research Center's Internet & American Life Project has note that 88% of US adults now own cell phones, and 43% say they download cell phone applications or "apps" to their phones. When surveyed, 54% of those app users said they had decided to not install a cell phone app when they discovered how much personal information they would need to share in order to use it and 30% of them had uninstalled an app that was already on their cell phone because they learned it was collecting personal information that they didn't wish to share. "Taken together," Pew notes, "57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons." Jan Lauren Boyles, Aaron Smith, and Mary Madden, *Privacy and Data Management on Mobile Devices*, (Pew Research Center's Internet & American Life Project, Sept. 5, 2012), http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx.
19. In its March 2012 *Protecting Consumer Privacy in an Era of Rapid Change* report, the FTC noted that, using its Section 5 authority and other powers, the agency has carried out many privacy and data security-related actions just since December 2010. See Fed. Trade Comm'n , PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) at ii, http://ftc.gov/os/2012/03/120326privacyreport.pdf. The FTC brought several other privacy and data security-related cases using its Section 5 powers after the 2012 report was released. *See: FTC Finalizes Privacy Settlement with Myspace*, Fed. Trade Comm'n, (Sept. 11, 2012), http://www.ftc.gov/opa/2012/09/myspace.shtm; *FTC Halts Computer Spying*, Fed. Trade Comm'n, (Sept. 25, 2012), http://www.ftc.gov/opa/2012/09/designware.shtm; *Tracking Software Company Settles FTC Charges That it Deceived Consumers and Failed to Safeguard Sensitive Data it Collected*, Fed. Trade Comm'n, (Oct. 22, 2012), http://www.ftc.gov/opa/2012/10/compete.shtm.
20. See Health Breach Notification Rule (2009), 16 C.F.R. § 318.1 (2012).
21. See Truth in Lending Act, 15 U.S.C. §§ 1601–1667(f) (2006); Fair Credit Billing Act, 15 U.S.C. §§ 1666–1666(j) (2006); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681–1681(u) (2006).
22. See Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6501 (2006).
23. See Jim Harper, *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection* (2002), http://www.privacilla.org/releases/Torts_Report.html.
24. See Jim Harper, *Understanding Privacy—and the Real Threats to It*, Cato Policy Analysis, Aug. 4 2004, at 3, www.cato.org/pub_display.php?pub_id=1652: "Contract law, for example, allows consumers to enter into enforceable agreements that restrict the sharing of information involved in or derived from transactions. Thanks to contract, one person may buy foot powder from another and elicit as part of the deal an enforceable promise never to tell another soul about the purchase."

state statutes.[25] Class action lawsuit activity is also remarkably intense following any major privacy violation or data breach.[26]

CONCLUSION

In closing, if we want America's digital economy to remain open, innovative, and vibrantly competitive, then this flexible, bottom-up approach to privacy protection is the constructive path forward.

If our fear is that consumers lack enough information to make smart privacy choices, then let's work harder to educate them while pushing for greater transparency about online data collection practices.

Finally, we should remember that not everyone shares the same privacy sensitivities and that citizens also care about other values, such as cost, convenience, and choice.

Moreover, we must also take into account the strong likelihood that citizens will adjust their privacy expectations in response to ongoing technological change, just as they have many times before.[27]

[*See* Appendix III: "Societal Adaptation, Evolving Cultural Norms & Privacy."]

I thank you again for inviting me here today and I would be happy to take any questions.

25. State governments and state attorneys general also continue to advance their own privacy policies, and those enforcement efforts are often more stringent than federal law. Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority as Catalysts for Data Protection*, at 3 (2010), http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFData-ProtectionandPrivacyCommissioners.pdf: "At the state level, legislatures have become the proving grounds for new statutory approaches to privacy regulation. Some of these developments include the enactment of data security breach notification laws . . . as well as highly detailed data security laws, enacted largely in response to data breaches. This partnership has resulted in a set of robust standards for the protection of personal data."

26. Peter Fleischer, *Privacy-litigation: get ready for an avalanche in Europe*, PETER FLEISCHER: PRIVACY ? (Oct. 26, 2012), http://peter-fleischer.blogspot.com/2012/10/privacy-litigation-get-ready-for.html?m=1: "Within hours of any newspaper headline (accurate or not) alleging any sort of privacy mistake, a race begins among privacy class action lawyers to find a plaintiff and file a class action. Most of these class actions are soon dismissed, or settled as nuisance suits, because most of them fail to be able to demonstrate any 'harm' from the alleged privacy breach. But a small percentage of privacy class actions do result in large transfers of money, first and foremost to the class action lawyers themselves, which is enough to keep the wheels of the litigation-machine turning."

27. See Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309, 364-73, (2013).

APPENDIX I:

TECHNO-"SILVER-BULLET" SOLUTIONS DON'T WORK – SOME CASE STUDIES

Seeking a simple solution to a complex problem such as online privacy protection is quixotic. In this sense, the Do Not Track falls into a long line of proposed silver-bullet or "universal" solutions to complicated technological problems. When it comes to such information control efforts, there are not many good examples of simple fixes or silver-bullet solutions that have been effective, at least not for very long.

- **Online Pornography:** Consider the elusive search for a universal solution to controlling access to online pornography. The experience of the W3C's Platform for Internet Content Selection (PICS)[28] and the Internet Content Rating Association (ICRA)[29] is instructive in this regard. Around the turn of the century, there was hope that voluntary metadata tagging and content labeling could be used to screen objectionable content on the Internet,[30] but the sheer volume of material to be dealt with made that task almost impossible.[31] The effort was eventually abandoned.[32] Of course, the effort did not have a government mandate behind it to encourage more widespread adoption, but even if it had, it is hard to believe that all pornography or other objectionable content would have properly been labeled and screened.

- **Spam:** In a similar way, the CAN-SPAM Act[33] aimed to curtail the flow of unsolicited email across digital systems, yet failed to do so. Private filtering efforts have helped stem the flow to some extent, but have not eliminated the problem altogether. Royal Pingdom estimates that in 2010, 89.1% of all e-mails were spam.[34] "Spam pages" are also a growing concern.[35] In January 2011, Blekko, a new search engine provider, created a "Spam Clock" to track new spam pages and found one million new spam pages were being created *every hour*.[36]

- **Privacy:** Technical silver-bullet solutions have also been tried on the privacy front before Do Not Track. The Platform for Privacy Preferences (P3P) is an earlier W3C project that began in the 1990s and attempted to make the use of privacy policies easier for consumers to understand. It sought to do so by encoding those privacy policies in a standard machine-readable format. The hope was that this would allow sites "to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily" by users and then allow users "to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit."[37] In theory, "such a privacy disclosure format could also allow the FTC to automate enforcement of its existing authority to punish unfair or deceptive trade practices."[38] Unfortunately,

28. *PICS Frequently Asked Questions* (FAQ), WORLD WIDE WEB CONSORTIUM, http://www.w3.org/2000/03/PICS-FAQ, (last visited Jan. 30, 2013).
29. *About ICRA*, FAMILY ONLINE SAFETY INST., http://www.fosi.org/icra, (last visited Jan. 30, 2013).
30. *See, e.g., Joris Evers, Net labels mean choice, not censorship*, PC ADVISOR, Oct. 23, 2001, http://www.pcadvisor.co.uk/news/desktop-pc/1646/net-labels-mean-choice-not-censorship/.
31. See PHIL ARCHER, ICRAFAIL: A LESSON FOR THE FUTURE 9 (2009), philarcher.org/icra/ICRAfail.pdf: "The problem with a safety system that has a label at one end and a filter at the other is that unlabelled sites can only be treated as a single group, i.e. you either block them all or allow them all. Since the number of labelled sites was very small, blocking all unlabelled sites would effectively shut off most of the Web."
32. FAMILY ONLINE SAFETY INST., http://www.icra.org, (last visited Nov. 30, 2012).
33. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at various sections of 15 and 18 U.S.C.).
34. *Internet 2010 in Numbers*, ROYAL PINGDOM, Jan. 12, 2011, http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers.
35. Spam pages are "useless pages that contain only a nugget of relevancy to your query and are slathered in ads." Caleb Johnson, Spam Clock *Claims 1 Million Spam Pages are Created Every Hour,* Jan. 10, 2011, SWITCHED.COM, http://switched.com/2011/01/10/blekko-spam-clock-1-million-pages-an-hour.
36. SPAMCLOCK, http://www.spamclock.com, (last visited Jan. 30, 2013); see also Danny Sullivan, *Blekko Launches Spam Clock To Keep Pressure On Google*, SEARCH ENGINE LAND.COM, Jan. 7, 2011, http://searchengineland.com/blekko-launches-spam-clock-to-keep-pressure-on-google-60634.
37. W3C, Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P (last accessed Apr. 21, 2013).
38. Adam Thierer & Berin Szoka, The Progress & Freedom Foundation, *Chairman Leibowitz's Disconnect on Privacy Regulation & the Future of News at 7*, (Jan. 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1619470.

> the P3P project has not been successful. Even though the process got underway in the mid-1990s and the W3C had a formal process in place to guide its development by 1997, the project was suspended in 2007.[39] A 2009 survey of privacy technologies by analysts at the UC Berkeley School of Information found that "to date, the adoption rate of P3P has been fairly low. Our analysis of the top 100 websites for this project revealed that only 27 of them provided a P3P policy, and only a subset of those were valid according to the P3P standard."[40]

Similar problems likely await the Do Not Track mechanism.[41] 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.[42] "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.[43] "There is no reliable way of ensuring this technology is being used," adds Sidney Hill of *Tech News World*.[44] "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."[45]

Importantly, Do Not Track would not slow the "arms race" in this arena as some have suggested.[46] If anything, a Do Not Track mandate will speed up that arms race and have many other unintended consequences.[47] Complex definitional questions also remain unanswered, such as how to define and then limit "tracking" in various contexts.[48]

In sum, in light of the global, borderless nature of online rapid data flows, the Do Not Track scheme likely will not be effective.[49] The regulatory experience with spam, objectionable content, and copyrighted content suggests serious challenges lie ahead for top-down regulatory efforts.

39. Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 279-82 (2012).

40. Joshua Gomez, Travis Pinnick & Ashkan Soltani, UC Berkeley, School of Information, *Know Privacy*, at 12 (June 1, 2009).

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

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

43. *Id*.

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

45. *Id*.

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

47. "Too often, well-intentioned efforts to regulate technology are far worse than the imagined evils they were intended to prevent." HAL ABELSON ET AL., BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 159 (2008).

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

49. "Many behavioral targeting companies are based outside the US—making legislation ineffective," says Doug Wolfgram, CEO of IntelliProtect, an online privacy management company. Tony Bradley, *Why Browser 'Do Not Track' Features Will Not Work*, COMPUTERWORLD, Feb. 10, 2011, http://news.idg.no/cw/art.cfm?id=ACE91A0E-1A64-6A71-CE2572C981C0204A; DANIEL CASTRO, POLICYMAKERS SHOULD OPT OUT OF "DO NOT TRACK" 1, 3 (2010), www.itif.org/files/2010-do-not-track.pdf: "Another problem with Do Not Track is that it does not scale well on the global Internet. . . . 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."

APPENDIX II:

DIGITAL SELF-HELP TOOLS / PRIVACY-ENHANCING TECHNOLOGIES

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

- The major online search and advertising providers offer "ad preference managers" to help users manage their advertising preferences. Google,[50] Microsoft,[51] and Yahoo![52] all offer easy-to-use opt-out tools and educational webpages that clearly explain to consumers how digital advertising works.[53] Meanwhile, a relatively new search engine, DuckDuckGo, offers an alternative search experience that blocks data collection altogether.[54]

- Major browser providers also offer variations of a "private browsing" mode, which allows users to turn on a stealth browsing mode to avoid data collection and other forms of tracking. This functionality is available as a menu option in Microsoft's Internet Explorer ("InPrivate Browsing"),[55] Google's Chrome ("Incognito")[56] and Mozilla's Firefox ("Private Browsing").[57] Firefox also has many add-ons available that provide additional privacy-enhancing functionality.[58] "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."[59]

- There are also many supplemental tools and add-ons that users can take advantage of to better protect their privacy online by managing cookies, blocking web scripts, and so on. Like the marketplace for parental control technologies, a remarkable amount of innovation continues in the market for privacy empowerment tools, so much so that it is impossible to document all of them here. However, some of the more notable privacy-enhancing tools and services include: Ghostery,[60]

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

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

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

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

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

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

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

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

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

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

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

NoScript,[61] Cookie Monster,[62] Better Privacy,[63] Track Me Not,[64] Collusion,[65] and the Targeted Advertising Cookie Opt-Out or "TACO"[66] (all for Firefox); No More Cookies[67] (for Internet Explorer); Disconnect (for Chrome);[68] AdSweep (for Chrome and Opera);[69] CCleaner[70] (for PCs); and Flush[71] (for Mac). New empowerment solutions are constantly turning up.[72] Many of these tools build around the Do Not Track notion and functionality that the FTC has been encouraging. For example, Reputation.com's new "MyPrivacy" service lets users remove their information from various sites and helps them create the equivalent of a Do Not Track list for over 100 online networks.[73] New tools from Priveazy[74] and Privacyfix[75] offer similar functionality and allow users to adjust privacy settings for several sites and services at once. Finally, online privacy company Abine offers a "Do Not Track Plus," which it claims blocks more than 600 trackers.[76] Abine also sells a "PrivacyWatch" service, which alerts Facebook users to privacy policy changes on the site,[77] as well as a "DeleteMe" service that helps users erase personal information from various other online sites and services.[78]

- The success of one particular tool, AdBlockPlus, deserves special mention. AdBlockPlus, which lets users blocks advertising on most websites, is the most-downloaded add-on for both the Firefox and Chrome web browsers.[79] As of October 2012, roughly 175 million people had downloaded the Adblock Plus add-on for the Firefox web browser.[80] Incidentally, both Adblock Plus and NoScript, another of the most popular privacy-enhancing downloads for Firefox, support the Do Not Track protocol.[81]

61. *No Script Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/noscript (last visited Jan. 30, 2013).
62. *Cookie Monster Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/cookie-monster (last visited Jan. 30, 2013).
63. *BetterPrivacy Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/betterprivacy (last visited Jan. 30, 2013).
64. *TrackMeNot Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/trackmenot (last visited Jan. 30, 2013).
65. *Collusion Add-On*, MOZILLA, http://www.mozilla.org/en-US/collusion (last visited Jan. 30, 2013).
66. *Targeted Advertising Cookie Opt-Out (TACO) Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/targeted-advertising-cookie-op/ (last visited Jan. 30, 2013).
67. *No More Cookies*, CNET.COM, http://download.cnet.com/No-More-Cookies/3000-2144_4-10449885.html (last visited Jan. 30, 2013).
68. DISCONNECT, https://disconnect.me (last visited Jan. 30, 2013).
69. *AdSweep Add-On*, OPERA, https://addons.opera.com/addons/extensions/details/adsweep/2.0.3-3/?display=en (last visited Jan. 30, 2013).
70. *CCleaner*, PIRIFORM, http://www.piriform.com/ccleaner (last visited Jan. 30, 2013).
71. *Flush*, MACUPDATE, http://www.macupdate.com/app/mac/32994/flush (last visited Jan. 30, 2013).
72. David Gorodyansky, *Web Privacy: Consumers Have More Control Than They Think*, HUFFINGTON POST, Dec. 30, 2010, http://www.huffingtonpost.com/david-gorodyansky/web-privacy-consumers-hav_b_799881.html.
73. *My Privacy*, REPUTATION.COM, http://www.reputation.com/myprivacy (last visited Jan. 30, 2013).
74. PRIVEAZY, https://www.priveazy.com (last visited Jan. 30, 2013).
75. PRIVACYFIX, https://privacyfix.com (last visited Jan. 30, 2013).
76. *Do Not Track Plus*, ABINE, http://www.abine.com/dntdetail.php (last visited Jan. 30, 2013).
77. PrivacyWatch, ABINE, http://www.abine.com/privacywatchdetail.php (last visited Jan. 30, 2013).
78. DeleteMe, ABINE, http://www.abine.com/marketing/landing/index.php (last visited Jan. 30, 2013).
79. ADBLOCKPLUS, https://adblockplus.org/en (last visited Jan. 30, 2013).
80. *Statistics for Adblock Plus Add-On*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/adblock-plus./statistics/?last=30 (last visited Jan. 30, 2013).
81. *X-Do-Not-Track support in NoScript*, HACKADEMIX, http://hackademix.net/2010/12/28/x-do-not-track-support-in-noscript (Dec. 28, 2010, 5:31 PM).

- Finally, pressured by policymakers and privacy advocates, all three of those browser makers (Microsoft,[82] Google,[83] and Mozilla[84]) have now agreed to include some variant of a Do Not Track mechanism or an opt-out registry in their browsers to complement the cookie controls they had already offered. Microsoft has even decided to turn on Do Not Track by default, although it has been a controversial move.[85] These developments build on industry-wide efforts by the Network Advertising Initiative and the "Self-Regulatory Program for Online Behavioral Advertising"[86] to make opting out of targeted advertising simpler. The resulting Digital Advertising Alliance is a collaboration among the leading trade associations in the field, including: American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Better Business Bureau, Digital Marketing Association, Interactive Advertising Bureau, and Network Advertising Initiative.[87] Their program uses an "Advertising Option Icon" to highlight a company's use of targeted advertising and gives consumers an easy-to-use opt-out option.[88] It was accompanied by an educational initiative, www.AboutAds.info, which offers consumers information about online advertising.[89] The independent Council of Better Business Bureaus will enforce compliance with the system.[90] Self-regulatory efforts such as these have the added advantage of being more flexible than government regulation, which tends to lock in sub-optimal policies and stifle ongoing innovation.

Again, this survey only scratches the surface of what is available to privacy-sensitive web surfers today.[91] Importantly, this inventory does not include the many different types of digital security tools that exist today.[92]

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

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

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

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

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

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

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

88. *Id*.

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

90. Major Marketing, supra note 180, at 2.

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

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

Importantly, it is vital to realize that most consumers will never take advantage of these empowerment tools, just as the vast majority of parental control technologies go untapped by most families.[93] This is due to a number of factors, most notably that not every individual or household will have the same needs and values as they pertain to either online safety and digital privacy.

Therefore, the fact that not every individual or household uses empowerment tools should not be used as determination of "market failure" or the need for government regulation. Nor should the effort or inconvenience associated with using such tools be viewed as a market failure.[94] What matters is that these tools exist for those who wish to use them, not the actual uptake or usage of those tools or the inconvenience they might pose to daily online activities.

Government officials can take steps to encourage the use of PETs, but it is even more essential that they do not block or discourage their use.[95] For example, limitations on encryption technologies or mandates requiring that web surfers use online age verification or identify authentication technologies would undermine user efforts to shield their privacy.[96]

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

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

95. A. Michael Froomkin, *The Death of Privacy*, Stan. L. Rev. 1461, 1506, 1529 (2000): "Sometimes overlooked, however, are the ways in which existing law can impose obstacles to PETs. Laws and regulations designed to discourage the spread of cryptography are only the most obvious examples of impediments to privacy-enhancing technology."

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

APPENDIX III:
SOCIETAL ADAPTATION, EVOLVING CULTURAL NORMS & PRIVACY

Many technologies or types of media that are originally viewed as culturally offensive or privacy-invasive very quickly come to be assimilated into our lives, despite initial resistance.[97] A cycle of initial *resistance*, gradual *adaptation*, and then eventual *assimilation* is well-established in the context of popular entertainment.[98] For example, the emergence of dime novels, comic books, movies, rock-and-roll music, video games, and social networking services all lead to "moral panics"[99] or "technopanics."[100] Over time, however, society generally came to accept and then even embrace these new forms of media or communications technologies.[101]

The same cycle of resistance, adaptation, and assimilation has played out countless times on the privacy front as well and "after the initial panic, we almost always embrace the service that once violated our visceral sense of privacy."[102] The introduction and evolution of photography provides a good example of just how rapidly privacy norms adjust. The emergence of the camera as a socially disruptive force was central to the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis's famous 1890 *Harvard Law Review* essay on "The Right to Privacy."[103] Brandeis and Warren claimed "modern enterprise and invention have, through invasions upon his privacy, subjected [man] to mental pain and distress, far greater than could be inflicted by mere bodily injury."[104] In particular, "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life," they claimed, "and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[105]

The initial revulsion that many citizens felt toward this new technology was a logical reaction to the way it disrupted well-established social norms.[106] But personal norms and cultural attitudes toward cameras and public photography evolved quite rapidly. Eventually, cameras became a widely embraced part of the human experience and social norms evolved to both accommodate their place in society but also scold those who would use them in inappropriate, privacy-invasive ways.

That same sort of societal adaptation was on display more recently following the introduction of Google's "Gmail" e-mail service in 2004. Gmail was greeted initially with hostility by many privacy advocates and some policymakers, some of whom wanted the service prohibited or tightly regulated.[107] A bill was floated in California that would

97. Doug Aamoth, *A Bunch of Tech Things People Have Threatened to Quit Recently*, TIMETECH, Dec. 18, 2012, http://techland.time.com/2012/12/18/a-bunch-of-tech-things-people-have-threatened-to-quit-recently.

98. Adam Thierer, *Why Do We Always Sell the Next Generation Short?*, FORBES, Jan. 8, 2012, http://www.forbes.com/sites/adamthierer/2012/01/08/why-do-we-always-sell-the-next-generation-short. ("many historians, psychologists, sociologists, and other scholars have documented this seemingly never-ending cycle of generational clashes.")

99. Robert Corn-Revere, *Moral Panics, the First Amendment, and the Limits of Social Science*, 28 COMMUNICATIONS LAWYER (2011).

100. Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 Minn. J. L. Sci. & Tech. 309, 364-73, (2013).

101. *Id*. at 364-8.

102. Larry Downes, Cato Institute, *A Rational Response to the Privacy "Crisis*," Policy Analysis, 10, Jan. 7, 2013, http://www.cato.org/publications/policy-analysis/rational-response-privacy-crisis.

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

104. *Id*. at 196.

105. *Id*. at 195.

106. Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295 (2010): "the rapid adoption of the portable camera had begun to make people uneasy about its ability to record daily life away from the seclusion of the photo studio. Old norms of deference and respect seemed under assault, and there was great anxiety among elites keen on protecting their status, authority, and privacy."

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

have banned the service.[108] Some privacy advocates worried that Google's contextually targeted advertisements, which were based on keywords that appeared in their e-mail messages, were tantamount to reading users' e-mail and constituted a massive privacy violation.[109] Users quickly adapted their privacy expectations to accommodate this new service, however, and the service grew rapidly.[110] By the summer of 2012, Google announced that 425 million people were actively using Gmail.[111]

Sometimes companies push too aggressively against established privacy norms, however, and users push back. This was true for Instagram in late 2012. On December 17, 2012, the popular online photo sharing service, which is owned by Facebook, announced changes to its terms of service and privacy policy that would have allowed it to more easily share user information and even their photographs with Facebook and advertisers.[112] Within hours of announcing the changes, Instagram found itself embroiled in a consumer and media firestorm.[113] The uproar also "helped a number of [competing] photo-sharing applications garner unprecedented amounts of traffic and new users."[114] One rival called EyeEm reported that daily sign-ups had increased a thousand percent by the morning after the Instagram announcement.[115] According to some estimates, Instagram "may have shed nearly a quarter of its daily active users in the wake of the debacle."[116]

Instagram's experience serves as an example of how consumers often "vote with their feet" and respond to privacy violations by moving to other services, or at least threatening to do so unless changes are made by the offending company.[117] Just three days after announcing those changes, Instagram relented and revised its privacy policy.[118] In an apology posted on its corporate blog, Instagram co-founder Kevin Systrom noted that "we respect that your

108. See Eric Goldman, *A Coasean Analysis of Marketing*, Wisc. L. Rev 1151, 1212 (2006) ("California's reaction to Gmail provides a textbook example of regulator antitechnology opportunism.")

109. See Chris Jay Hoofnagle et al., *Letter to California Attorney General Lockyer, Electronic Privacy Information Center*, May 3, 2004, http://epic.org/privacy/gmail/agltr5.3.04.html.

110. Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 984-5 (2013), (noting that the Gmail case study, "serves as a reminder of the limits of privacy law, because sometimes the consuming public, faced with truthful full disclosure about a service's privacy choices, will nevertheless choose the bad option for privacy, at which point there is often little left for privacy advocates and regulators to do.")

111. Dante D'Orazio, *Gmail Now Has 425 Million Total Users*, THE VERGE, June 28, 2012, http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users.

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

113. Joshua Brustein, *Anger at Changes on Instagram*, N.Y. TIMES BITS, Dec. 17, 2012, http://bits.blogs.nytimes.com/2012/12/18/anger-at-changes-on-instagram.

114. Nicole Perlroth & Jenna Wortham, *Instagram's Loss Is a Gain for Its Rivals*, N.Y. TIMES BITS, Dec. 20, 2012, http://bits.blogs.nytimes.com/2012/12/20/instagrams-loss-is-other-apps-gain/?smid=tw-nytimesbits&seid=auto.

115. *Id*.

116. Garett Sloane, *Rage Against Rules*, N.Y. POST, Dec. 27, 2012, http://www.nypost.com/p/news/business/rage_against_Dh05rPifiXBIJRE1rCOyML.

117. Downes, *A Rational Response*, 11: "Often the more efficient solution is for consumers to vote with their feet, or these days with their Twitter protests. As social networking technology is coopted for use in such campaigns, consumers have proven increasingly able to leverage and enforce their preferences."

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

photos are your photos. Period."[119] Despite the rapid reversal, a class action lawsuit was filed less than a week later.[120] Although experts agreed the lawsuit was unlikely to succeed, such legal threats can have a profound impact on current and future corporate behavior.[121]

These episodes show how, time and time again, humans have proven to be resilient in the face of rapid technological change by using a variety of adaptation and coping mechanisms to gradually assimilate new technologies and business practices into their lives.[122] Other times they push back against firms that disrupt establish privacy norms and encourage companies to take a more gradual approach to technological change.

119. Instagram, *Thank You, and We're Listening*, INSTAGRAM BLOG, Dec. 18, 2012, http://blog.instagram.com/post/38252135408/thank-you-and-were-listening.

120. Zach Epstein, *Instagram Slapped with Class Action Lawsuit over Terms of Service Fiasco*, BGR.COM, Dec. 25, 2012, http://bgr.com/2012/12/25/instagram-slapped-with-class-action-lawsuit-over-terms-of-service-fiasco-267480/?utm_source=dlvr.it&utm_medium=twitter.

121. Jeff John Roberts, *Instagram Privacy Lawsuit is Nonsense Say Experts,* GIGAOM, Dec. 26, 2012, http://gigaom.com/2012/12/26/instagram-privacy-lawsuit-is-nonsense-say-experts.

122. Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 Minn. J. L. Sci. & Tech. 309, 364-73, (2013).

APPENDIX IV:
WHY AMERICA'S PRIVACY REGIME IS WORTH DEFENDING:
A Better, Simpler Narrative for US Privacy Policy

by Adam Thierer
[originally published on the *Technology Liberation Front* blog, March 19, 2013]

Last week on his personal blog, Peter Fleischer, Global Privacy Counsel for Google, posted an interesting essay titled, "We Need a Better, Simpler Narrative of US Privacy Laws."[123] Fleischer says that Europe has done a better job marketing its privacy regime to the world than the United States and argues that "the US has to figure out how to explain its privacy laws on the global stage" since "Europe is convincing many countries around the world to implement privacy laws that follow the European model." He notes that "in the last year alone, a dozen countries in Latin America and Asia have adopted euro-style privacy laws [while] not a single country, anywhere, has followed the US model." Fleischer argues that this has ramifications for long-term trade policy and global Internet regulation more generally.

I found this essay very interesting because I deal with some of these issues in my latest law review article, "The Pursuit of Privacy in a World Where Information Control is Failing."[124] In the article, I suggest that the United States *does* have a unique privacy regime and it is one that is very similar in character to the regime that governs online child safety issues. Whether we are talking about online safety or digital privacy, the defining characteristics of the US regime are that it is bottom-up, evolutionary, education-based, empowerment-focused, and resiliency-centered. It focuses on responding to safety and privacy harms after exhausting other alternatives, including market responses and the evolution of societal norms.

The EU regime, by contrast, is more top-down in character and takes a more static, inflexible view of privacy rights. It tries to impose a one-size-fits-all model on a diverse citizenry and it attempts to do so through heavy-handed data directives and ongoing "agency threats." It is a regime that makes more sweeping pronouncements about rights and harms and generally recommends a "precautionary principle"[125] approach to technological change in which digital innovation is more "permissioned."[126]

Put simply, the US regime is *reactive* in character while the EU regime is more *preemptive*. The US system focuses on responding to safety and privacy problems using a more diverse toolbox of solutions, some of which are governmental in character while others are based on evolving social and market norms and responses. To be clear, law *does* enter the picture here in the United States, but it does so in a very different way than it does in the European Union. Fleischer actually explains that point quite nicely in his essay:

> What is the US model? People in the privacy profession know that the US has a dense "patchwork" model of privacy laws: every individual US State has numerous privacy laws, the Federal government has numerous sectoral laws, and numerous other "non-privacy" laws, like consumer protec-

123. Peter Fleischer, *We Need a Better, Simpler Narrative of US Privacy Laws*, Mar. 12, 2013, http://peterfleischer.blogspot.com/2013/03/we-need-better-simpler-narrative-of-us.html.

124. Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 Harv. J. L. & Pub. Pol. 409 (2013), papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680.

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

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

> tion laws, are regularly invoked in privacy matters. Regulators in many corners of government, ranging from State attorneys general, to the Federal Trade Commission, and armies of class action lawyers inspect every privacy issue for possible actions.[127]

Indeed, in my new law review article, I summarize the litany of cases the FTC has brought recently on the data security and privacy front using its authority under Section 5 of the Federal Trade Commission Act to police "unfair and deceptive" practices. State AGs are active on this front as well, and there is plenty of class action activity every time there's a privacy or data security screw-up.

Meanwhile, public officials continue to work collaboratively with privacy advocates, corporations, and educators to develop better education and awareness-building efforts, including "best practices" on safety, security, and privacy issues.

For more details on this US model, please consult pages 436–454 of my article, in which I provide a comprehensive overview of what I refer to as America's "3-E Approach" to dealing with online safety and digital privacy concerns. The "3-Es" refer to *education*, *empowerment*, and targeted *enforcement* of existing legal standards. As I note in the article:

> [America's "3-E Approach"] does not imagine it is possible to craft a single, universal solution to online safety or privacy concerns. It aims instead to create a flexible framework that can help individuals cope with a world of rapidly evolving technological change and constantly shifting social and market norms as they pertain to information sharing.[128]

But what frustrates Fleischer is that the U.S model still doesn't translate into a simple narrative for international audiences:

> How on earth do you explain US privacy laws to an international audience? How do you explain the role of class action litigation to people in countries where it doesn't even exist? The US privacy law narrative is convoluted. That's a pity, since almost all of the global privacy professionals with whom I've discussed this issue agree with me that the sum of all the individual parts of US privacy laws amounts to a robust legal framework to protect privacy. (I didn't say "perfect", since laws never are, and I'm not grading them either.) By contrast, Europe's privacy narrative is simple and appealing. Its laws are very general, aspirational, horizontal and concise. Critics could say they're also inevitably vague, as any high-level law would have to be. But, like the US Bill of Rights, they have a sort of simple and profound universality that has inspired people around the world. And they are enforced (at least, on paper) by a single, identifiable, specialist regulator.[129]

I understand the frustration Fleischer is expressing here regarding how to frame the US model for broader audiences. But the crucial point here is that, as he correctly notes, "the sum of all the individual parts of US privacy laws amounts to a robust legal framework to protect privacy," even if it is the case that we will never achieve anything near perfection when it comes to online privacy (or online safety for that matter). But it is unfortunate that Fleischer ignores the many other moving pieces at work here that are important to the US system, especially the diverse array of educational and awareness-building efforts, as well as the astonishing array of empowerment tools that currently exist to help user protect their privacy to the degree they desire.

Of course, it should also be obvious that the US regime is never going to appeal to a global audience as much as Europe's privacy regime for the same reason that many other US policy regimes don't appeal to certain countries

127. Fleischer.

128. Thierer, *The Pursuit of Privacy*, at 437.

129. Fleischer.

or their leaders: our systems aren't regulatory enough in character for them! But while those top-down, centralized, preemptive regulatory regimes will almost always be more "aspirational, horizontal and concise"—and, therefore, have greater appeal to activist-minded lawmakers and regulators"—that also means those regimes will likely leave less breathing room for social evolution (i.e., evolving norms about safety and privacy) and economic innovation (new digital goods and services that potentially disrupt those regulatory expectations). That has real consequences for long-term growth and overall consumer welfare.

Regardless, to the extent we need "a better, simpler narrative for US privacy policy" as Fleischer suggests, I believe we can boil it down to a few words: *bottom-up*, *evolutionary*, *flexible,* and *reactive*. What this means for public policy is clear: **We need diverse tools and solutions for a diverse citizenry, while leaving plenty of breathing room for ongoing innovation and the evolution of social norms and market responses.** Whether it's online safety or digital privacy, public policy should take into account the extraordinary diversity of citizen needs and tastes and leave the ultimate decision about acceptable online content and interactions to them. We should look to educate and empower citizens so that they can make decisions about their online safety and privacy for themselves so that policymakers are not constantly trying to make decisions on their behalf.

This is a model worth defending, even if it is sometimes hard to delineate its contours. Please read my *Harvard Journal of Law & Public Policy* article for a fuller exploration of that model and a defense of it.

ABOUT THE AUTHOR

Adam Thierer is a senior research fellow at the Mercatus Center at George Mason University with the Technology Policy Program. Views expressed here are his own.