A FRAMEWORK FOR BENEFIT-COST ANALYSIS IN DIGITAL PRIVACY DEBATES

Adam Thierer[*]

INTRODUCTION

Policy debates surrounding online child safety and digital privacy share much in common. Both are complicated by thorny definitional disputes and highly subjective valuations of "harm." Both issues can be subject to intense cultural overreactions, or "technopanics."[1] It is common to hear demands for technical quick fixes or silver bullet solutions that are simple yet sophisticated.[2] In both cases, the purpose of regulation is some form of information control.[3] Preventing exposure to objectionable content or communications is the primary goal of online safety regulation, whereas preventing the release of personal information is typically the goal of online privacy regulation.[4] The common response is regulation of business practices or default service settings.[5]

---

[*] Senior Research Fellow at the Mercatus Center at George Mason University. The Author wishes to thank Sherzod Abdukadirov, Jerry Brito, Eli Dourado, Jerry Ellig, Patrick McLaughlin, and Richard Williams for their input on this paper.

[1] Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309, 311 (2013).

[2] Comments of Adam Thierer, Senior Fellow, Progress & Freedom Found., Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming, MB Docket No. 09-26, at v (FCC Apr. 16, 2009), *available at* http://www.pff.org/issues-pubs/filings/2009/041509-[FCC-FILING]-Adam-Thierer-PFF-re-FCC-Child-Safe-Viewing-Act-NOI-(MB-09-26).pdf ("There is a trade-off between complexity and convenience for both tools and ratings: Some critics argue parental control tools need to be more sophisticated; others claim parents can't understand the ones already at their disposal. But there is no magical 'Goldilocks' formula for getting it 'just right.' There will *always* be a trade-off between sophistication and simplicity; between intricacy and ease-of-use.").

[3] *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 868 (2012); Adam Thierer, *When It Comes to Information Control, Everybody Has a Pet Issue & Everyone Will Be Disappointed*, TECH. LIBERATION FRONT (Apr. 29, 2011), http://techliberation.com/2011/04/29/when-it-comes-to-information-control-everybody-has-a-pet-issue-everyone-will-be-disappointed.

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

[5] *See* Eric J. Johnson et al., *Defaults, Framing and Privacy: Why Opting In-Opting Out*, 13 MARKETING LETTERS 5, 5 (2002), *available at* http://www8.gsb.columbia.edu/sites/decisionsciences//files/defaults_framing_and_privacy.pdf; Adam Thierer, *The Perils of Mandatory Parental Controls and*

Once we recognize that online child safety and digital privacy concerns are linked by many similar factors, we can consider whether common solutions exist. Many of the solutions proposed to enhance online safety and privacy are regulatory in character. But information regulation is not a costless exercise. It entails both economic and social costs.[6] Measuring those costs is an extraordinarily complicated and contentious matter, since both online child safety and digital privacy are riddled with emotional appeals and highly subjective assertions of harm.

This Article will make a seemingly contradictory argument: benefit-cost analysis ("BCA") is extremely challenging in online child safety and digital privacy debates, yet it remains essential that analysts and policymakers attempt to conduct such reviews. While we will never be able to perfectly determine either the benefits or costs of online safety or privacy controls, the very act of conducting a regulatory impact analysis ("RIA") will help us to better understand the trade-offs associated with various regulatory proposals.[7] However, precisely because those benefits and costs remain so remarkably subjective and contentious, this Article will argue that we should look to employ less restrictive solutions—education and awareness efforts, empowerment tools, alternative enforcement mechanisms, etc.—before resorting to potentially costly and cumbersome legal and regulatory regimes that could disrupt the digital economy and the efficient provision of services that consumers desire.[8] This model has worked fairly effectively in the online safety context and can be applied to digital privacy concerns as well.

This Article focuses primarily on digital privacy policy and sketches out a framework for applying BCA to proposals aimed at limiting commercial online data collection, aggregation, and use. Information about online users is regularly collected by online operators to tailor advertising to them (so-called "targeted" or "behavioral" advertising), to offer them expanded

---

Restrictive Defaults, PROGRESS & FREEDOM FOUND. 1 (Apr. 2008), http://www.pff.org/issues-pubs/pops/pop15.4defaultdanger.pdf.

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

7 *See* Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 1, 23 ("Before rushing to the absolutist position that individuals should always control 'their' information, both regulators and individuals need to consider the trade-offs and nuances.").

8 *See* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 109 (2008) (arguing that "information exchange is valuable and . . . regulators should be cautious about restricting it").

functionality, or to provide them with additional service options.[9] Such operators include social networking services, online search and e-mail providers, online advertisers, and other digital content providers. While this produces many benefits for consumers—namely, a broad and growing diversity of online content and services for little or no charge[10]—it also raises privacy concerns and results in calls for regulatory limitations on commercial data collection or reuse of personal information.[11]

This Article does not focus on assertions of privacy rights against government, however. The benefit-cost calculus is clearly different when state actors, as opposed to private actors, are the focus of regulation.[12] Governments have unique powers and responsibilities that qualify them for a different type of scrutiny.[13]

To offer a more concrete example of how privacy-related BCA should work in practice, the recent actions of the Obama administration and the Federal Trade Commission ("FTC") are considered throughout the Article.[14] The Obama administration has been remarkably active on commercial privacy issues over the past three years yet has largely failed to adequately consider the full range of costs associated with increased government activity on this front.[15] It has also failed to conclusively show that any sort of market failure exists as it relates to commercial data collection or targeted online advertising or services.

At a minimum, this Article will make it clear why independent agencies should be required to carry out BCA of any privacy-related policies

---

9 *See* David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSP. 37, 50 (2009) ("[I]t is possible for online entities to gather data on what people have done on line, including their previous searches, what websites they have browsed, and perhaps even what they have purchased online. Those data, together with other information, can be used to target advertisements to people based on their behavior.").

10 *See* Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 30-33 (2011) (describing benefits of behaviorally targeted advertising).

11 *See* Slade Bond, *Doctor Zuckerberg: Or, How I Learned to Stop Worrying and Love Behavioral Advertising*, 20 KAN. J.L. & PUB. POL'Y 129, 152 (2010); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1821 (2011); David Auerbach, *You Are What You Click: On Microtargeting*, THE NATION, Feb. 13, 2013, at 28, *available at* http://www.thenation.com/article/172887/you-are-what-you-click-microtargeting.

12 *Cf.* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 119 (1997).

13 *See* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 140 (2011).

14 *See* Maureen K. Ohlhausen, *The FTC's New Privacy Framework*, 25 ANTITRUST 43, 43 (2011).

15 *See* Josh Dreller, *A Marketer's Guide to the Privacy Debate*, IMEDIA CONNECTION (Dec. 8, 2011), http://www.imediaconnection.com/content/30629.asp.

they are considering.[16] Currently, many agencies, including the FTC and the Federal Communications Commission ("FCC"), are not required to conduct BCA or have their rulemaking activities approved by the White House Office of Information and Regulatory Affairs ("OIRA"), which oversees federal regulations issued by executive agencies.[17] Regulatory impact analysis is important even if there are problems in defining, quantifying, and monetizing benefits—as is certainly the case for commercial online privacy concerns.[18]

In Part I, this Article examines the use of BCA by federal agencies to assess the utility of government regulations. Part II considers how BCA can be applied to online privacy regulation and the challenges federal officials face when determining the potential benefits of regulation. Part III then elaborates on the cost considerations and other trade-offs that regulators face when evaluating the impact of privacy-related regulations. In Part IV, this Article will discuss alternative measures that can be taken by government regulators when attempting to address online safety and privacy concerns. This Article concludes that policymakers must consider BCA when proposing new rules but also recognize the utility of alternative remedies, such as education and awareness campaigns, to address consumer concerns about online safety and privacy.

---

16 *See* Robert W. Hahn & Cass R. Sunstein, *A New Executive Order for Improving Federal Regulation? Deeper and Wider Cost-Benefit Analysis* 3 (Univ. Chi. Law Sch. John M. Olin Law & Econ., Working Paper No. 150, 2002), *available at* http://www.law.uchicago.edu/files/files/150.CRS_.Cost-Benefit.pdf ("[T]he commitment to cost-benefit analysis has been far too narrow; it should be widened through efforts to incorporate independent regulatory commissions within its reach.").

17 *See* Arthur Fraas & Randall Lutter, *On the Economic Analysis of Regulations at Independent Regulatory Commissions*, 63 ADMIN. L. REV. 213, 224 (2011); Richard Williams & Sherzod Abdukadirov, *Blueprint for Regulatory Reform* 16 (Mercatus Ctr., Working Paper No. 12-07, 2012), *available at* http://mercatus.org/publication/blueprint-regulatory-reform ("Independent agencies are encouraged but not required to consider regulation's costs and benefits. Numerous regulations are therefore not subject to the executive's economic efficiency requirements. . . . Since independent agencies are becoming a bigger factor in regulation . . . requiring economic analysis make sense. While this requirement may impose additional costs on independent agencies, the better quality of analysis would almost certainly be worth the cost.").

18 *See* Susan Dudley & Arthur Fraas, *The Future of Regulatory Oversight and Analysis*, MERCATUS CTR., 3 (May 2009), http://mercatus.org/sites/default/files/publication/MOP51_OIRA.pdf (noting that "some of the most highly publicized regulatory problems today stem from so-called independent regulatory agencies. . . . [which] have never been subject to the analytical or procedural requirements of executive oversight.").

I. THE TRIUMPH OF BENEFIT-COST ANALYSIS

A. *The "Extraordinary Development" of Benefit-Cost Analysis*

Shortly after stepping down as administrator of the OIRA in 2012, Professor Cass Sunstein made the following observation:

> It is not exactly news that we live in an era of polarized politics. But Republicans and Democrats have come to agree on one issue: the essential need for cost- benefit analysis in the regulatory process. In fact, cost-benefit analysis has become part of the informal constitution of the U.S. regulatory state. This is an extraordinary development.[19]

What made the development extraordinary, in Sunstein's opinion, was that almost all government regulations "are being addressed under a framework that is now broadly shared. Endorsed for more than three decades and by five presidents, cost-benefit analysis is here to stay."[20]

Indeed, the use of BCA by regulators is an extraordinary development. Although not all government agencies are doing regulatory review equally well,[21] BCA is now such a routine feature of federal regulatory policymaking that it is difficult to imagine a time when rules were not subjected to such review, and, as Sunstein suggests, it is even more challenging to imagine a future in which BCA would not continue to be a regular fixture of the policymaking process.[22]

Benefit-cost analysis prospers because "the rationale for the benefit-cost approach seems quite compelling" to most economists and policy analysts.[23] Indeed, the logic is impeccable since "[a]t a very minimum, society should not pursue policies that do not advance our interests," observe the authors of a leading textbook on regulatory economics.[24] "If the benefits of a policy are not in excess of the costs, then clearly it should not be pursued, because such efforts do more harm than good."[25]

---

19 Cass R. Sunstein, *The Stunning Triumph of Cost-Benefit Analysis*, BLOOMBERG VIEW (Sept. 12, 2012), http://www.bloomberg.com/news/2012-09-12/the-stunning-triumph-of-cost-benefit-analysis.

20 *Id.*

21 *See* OFFICE OF MGMT. & BUDGET, 2011 REPORT TO CONGRESS ON THE BENEFITS AND COSTS OF FEDERAL REGULATIONS AND UNFUNDED MANDATES ON STATE, LOCAL, AND TRIBAL ENTITIES 22 (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/inforeg/2011_cb/2011_cba_.pdf (noting that of the 66 major regulations passed in fiscal year 2010, only 18 fully quantified and monetized both benefits and costs).

22 *See* Sunstein, *supra* note 19.

23 *See* W. KIP VISCUSI, JOHN M. VERNON & JOSEPH E. HARRINGTON, JR., ECONOMICS OF REGULATION AND ANTITRUST 664 (2d ed. 1995).

24 *Id.*

25 *Id.*

B. *Basic Benefit-Cost Framework*

BCA represents an effort to formally identify the trade-offs or opportunity costs associated with regulatory proposals and, to the maximum extent feasible, quantify those benefits and costs.[26] At the federal level in the United States, regulatory policymaking and the BCA process is guided by various presidential executive orders and guidance issued by the OIRA.[27] The OIRA was created as part of the Paperwork Reduction Act of 1980 and made part of the Office of Management and Budget ("OMB").[28] "OIRA reviews . . . significant proposed and final rules from all federal agencies (other than independent regulatory agencies) before they are [finalized and] published in the *Federal Register*."[29]

Various presidential executive orders, beginning with Executive Order 12291 issued by President Reagan in 1981, have required executive branch agencies to utilize BCA in the regulatory policymaking process.[30] "Every subsequent president has continued the regulatory review order with only slight modifications," notes Professor John O. McGinnis.[31]

The most important recent regulatory policymaking guidance comes from Executive Order 12866, issued by President Clinton in September 1993,[32] and the OMB's Circular A-4, issued in September 2003.[33] Circulars are "[i]nstructions or information issued by OMB to Federal agencies" to help guide their rulemaking activities.[34] Circular A-4 and subsequent agen-

---

26 *See* SUSAN E. DUDLEY & JERRY BRITO, REGULATION: A PRIMER 97-98 (2d ed. 2012) ("The cost of a regulation is the opportunity cost—whatever desirable things society gives up in order to get the good things the regulation produces. The opportunity cost of alternative approaches is the appropriate measure of costs. This measure should reflect the benefits foregone when a particular action is selected and should include the change in consumer and producer surplus."); Jerry Ellig & Patrick A. McLaughlin, *The Quality and Use of Regulatory Analysis in 2008*, 32 RISK ANALYSIS 855, 855 (2012).

27 *See* Richard B. Belzer, *Risk Assessment, Safety Assessment, and the Estimation of Regulatory Benefits*, MERCATUS CTR., 5 (2012), http://mercatus.org/publication/risk-assessment-safety-assessment-and-estimation-regulatory-benefits.

28 Curtis W. Copeland, *The Role of the Office of Information and Regulatory Affairs in Federal Rulemaking*, 33 FORDHAM URB. L.J. 101, 102 (2005).

29 U.S. GEN. ACCOUNTING OFFICE, GAO-03-929, OMB'S ROLE IN REVIEWS OF AGENCIES' DRAFT RULES AND THE TRANSPARENCY OF THOSE REVIEWS 3 (2003), *available at* http://www.gao.gov//160/157476.pdf.

30 *See* Exec. Order No. 12291, 46 Fed. Reg. 13193 (Feb. 19, 1981).

31 JOHN O. MCGINNIS, ACCELERATING DEMOCRACY: TRANSFORMING GOVERNANCE THROUGH TECHNOLOGY 110 (2013).

32 *See* Exec. Order No. 12866, 58 Fed. Reg. 51735 (Oct. 4, 1993).

33 *See* OFFICE OF MGMT. & BUDGET, CIRCULAR A-4, Regulatory Analysis (2003) [hereinafter OMB, CIRCULAR A-4], *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb//a004/a-4.pdf.

34 *See Circulars*, WHITE HOUSE, OFFICE OF MGMT. & BUDGET, http://www.whitehouse.gov//circulars_default (last visited June 23, 2013).

cy guidance issued by the OIRA list the steps agencies must follow when conducting an RIA.[35]

The OIRA identifies the three core elements of an RIA. First, "[a] statement of the need for the regulatory action" is required that includes "a clear explanation of the need for the regulatory action, including a description of the problem that the agency seeks to address."[36] As part of this step, "Agencies should explain whether the action is intended to address a market failure or to promote some other goal."[37]

Second, "[a] clear identification of a range of regulatory approaches" is required, "including the option of not regulating."[38] Agencies must also consider other alternatives to federal regulation, such as "State or local regulation, voluntary action on the part of the private sector, antitrust enforcement, consumer-initiated litigation in the product liability system, and administrative compensation systems."[39] Agencies are supposed to assess the benefits and costs of all these alternatives.[40] If federal regulation is still deemed necessary, flexible approaches are strongly encouraged by the OIRA.[41]

Finally, "[a]n estimate of the benefits and costs—both quantitative and qualitative" is required.[42] The quantification of benefits and costs is strongly encouraged but, when impossible, agencies are required to describe them qualitatively and make a clear case for action.[43]

President Obama has issued several executive orders attempting to clarify and improve the federal regulatory rulemaking process.[44] Executive Order 13563, issued in January 2012, focuses on "Improving Regulation and Regulatory Review" and requires agencies to engage in "periodic review of existing significant regulations" and retrospectively review existing

---

35 *See* OFFICE OF MGMT. & BUDGET, OFFICE OF INFO. & REGULATORY AFFAIRS, REGULATORY IMPACT ANALYSIS: A PRIMER (2011) [hereinafter OIRA, RIA PRIMER], *available at* http://www.whitehouse.gov/sites/default/files/omb/inforeg/regpol/circular-a-4_regulatory-impact-analysis-a-primer.pdf; Richard Williams & Jerry Ellig, *Regulatory Oversight: The Basics of Regulatory Impact Analysis*, MERCATUS CTR., 17 (2011), *available at* http://mercatus.org/sites/default/files/Regulatory-Impact-Analysis-Toolkit.pdf.

36 OIRA, RIA PRIMER, *supra* note 35, at 2.

37 *Id.*

38 *Id.*

39 *Id.*

40 *Id.* at 7.

41 *Id.* at 2, 5.

42 OIRA, RIA PRIMER, *supra* note 35 at 3.

43 *Id.* at 3-4.

44 *Regulatory Matters*, WHITE HOUSE, http://www.whitehouse.gov/omb/inforeg_regmatters (last visited June 24, 2013). *See, e.g.*, Exec. Order No. 13610, 77 Fed. Reg. 28,469 (May 14, 2012); Exec. Order No. 13,563, 76 Fed. Reg. 3,821 (Jan. 21, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/inforeg/eo12866/eo13563_01182011.pdf.

significant regulations in order to "determine whether any such regulations should be modified, streamlined, expanded, or repealed."[45]

Subsequently, in May 2012, President Obama issued Executive Order 13610 on "Identifying and Reducing Regulatory Burdens."[46] It specified that "it is particularly important for agencies to conduct retrospective analyses of existing rules to examine whether they remain justified and whether they should be modified or streamlined in light of changed circumstances, including the rise of new technologies."[47] This reflects the fact that throughout these executive orders and OIRA guidance statements there is a strong presumption in favor of using market mechanisms instead of command-and-control regulatory methods.[48]

C. *Application to Privacy Proposals*

The following Sections will use the BCA framework described above to consider how commercial privacy regulations should be evaluated going forward. It will also be referenced when examining recent calls for privacy regulation by the Obama administration and other policymakers.[49] The FTC has issued two major privacy reports during the Obama presidency[50] and has been pushing for industry adoption of a "Do Not Track" mechanism, which is a browser-based tool that can help consumers defeat online data collection and targeted advertising.[51] In late 2010, the Department of Commerce ("DOC") also issued a report on *Commercial Data Privacy and Innovation in the Internet Economy*, which recommended the adoption of

---

45 76 Fed. Reg. 3,821, 3,822.

46 77 Fed. Reg. 28,469.

47 *Id.* at 28,469.

48 DUDLEY & BRITO, *supra* note 26, at 93 ("By harnessing market forces, market-based approaches are likely to achieve desired goals at lower social costs than command-and-control approaches.").

49 Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J. L. SCI. & TECH. 281, 319-20 (2012).

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

51 Stephanie A. Kuhlmann, Comment, *Do Not Track Me Online: The Logistical Struggles over the Right "to Be Let Alone" Online*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 229, 252-53 (2011); Sara Forden, *FTC's Leibowitz Foresees Do-Not-Track Privacy Option in 2012*, BLOOMBERG BUSINESSWEEK (Mar. 29, 2012), http://www.businessweek.com/news/2012-03-29/ftc-s-leibowitz-foresees-do-not-track-privacy-option-in-2012; Edward Wyatt, *F.T.C. and White House Push for Online Privacy Laws*, N.Y. TIMES (May 9, 2012), http://www.nytimes.com/2012/05/10/business/ftc-and-white-house-push-for-online-privacy-laws.html.

comprehensive fair information practice principles ("FIPPs").[52] As part of this framework, the administration called for federal legislation that would include a "Consumer Privacy Bill of Rights" as well as the formation of a "multi-stakeholder process" that includes industry, civil society, and academic members.[53] The administration hoped that a consensus could be reached on an enforceable code of conduct for commercial digital privacy through this process. Such multi-stakeholder negotiations were initiated by the DOC in the summer of 2012, and the agency continues to work to craft a consensus on a set of standards as of the time of this writing.[54] Legislation has been floated in Congress that would endorse many of these ideas.[55]

The FTC has also recently issued revisions to the regulations it crafted pursuant to the Children's Online Privacy Protection Act ("COPPA") of 1998.[56] COPPA requires that child-oriented website operators or service providers "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children [under 13]."[57] Finally, the FTC has released "best practices" guidelines to encourage improved priva-

---

52 U.S. DEP'T OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK vii (2010) [hereinafter COMMERCE PRIVACY & INNOVATION REPORT].

53 *Id.* at iii, vi ("The government can coordinate this process, not necessarily by acting as a regulator, but rather as a convener of the many stakeholders—industry, civil society, academia—that share our interest in strengthening commercial data privacy protections. The Department of Commerce has successfully convened multi-stakeholder groups to develop and implement other aspects of Internet policy."); WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1 (2012).

54 *Commerce Department's NTIA Announces First Privacy Multistakeholder Process Topic*, COMMERCE.GOV (June 18, 2012, 10:43 AM), http://www.commerce.gov/os/ogc/developments/department%E2%80%99s-ntia-announces-first-privacy-multistakeholder-process-topi; John Eggerton, *Privacy Stakeholders Air Public Differences*, BROAD. & CABLE (July 12, 2012, 6:00 PM), http://www.broadcastingcable.com/article/487101-Privacy_Stakeholders_Air_Public_Differences.php; Molly Bernhart Walker, *NTIA-Led Group Inches Closer to Mobile App Code of Conduct*, FIERCEMOBILEGOVERNMENT (Apr. 9, 2013), http://www.fiercemobilegovernment.com/story/ntia-led-group-inches-closer-mobile-app-code-conduct/2013-04-09.

55 Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899, 907-13 (2011) (summarizing recent privacy-related legislative proposals).

56 Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Children's Online Privacy Protection Rule (Dec. 19, 2012), http://www.ftc.gov/opa/2012/12/coppa.shtm.

57 15 U.S.C. §§ 6501–6506 (2006).

cy for digital advertising disclosures,[58] mobile apps for kids,[59] mobile technology generally,[60] and facial recognition technologies.[61]

Importantly, with the exception of the COPPA rule revision, these recent privacy-related policy activities have not yet taken the form of formal regulatory enactments. Although the Obama administration has advocated that Congress implement new "baseline privacy protections" as part of a new comprehensive privacy law,[62] at least thus far neither the Obama administration nor congressional lawmakers have implemented formal regulations that could be subjected to BCA.[63] Complicating matters further is the fact that the administration has seemed content to "nudge" industry actors in various ways to achieve greater industry self-regulation through recommended best practices or "multistakeholder" agreements, instead of relying on formal regulatory enactments.[64]

The lack of formal regulatory enactments makes applying BCA to proposed regulations more challenging, but it does not excuse the almost complete absence of it in the process thus far.[65] The Obama administration has generally avoided a serious analysis of the benefits and costs of regulation in the context of commercial data collection practices and online privacy. Unfortunately, this also seems to be a trend with the FTC over time on this issue. In 2000, when the FTC released its first major digital privacy report, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, Commissioner Orson Swindle remarked that, "Shockingly, there

---

58 FED. TRADE COMM'N, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING 16 (2013), *available at* http://www.ftc.gov/os/2013/03/130312dotcom.pdf.

59 Press Release, Fed. Trade Comm'n, FTC Publishes Guide to Help Mobile App Developers Observe Truth-in-Advertising, Privacy Principles (Sept. 5, 2012), http://www.ftc.gov/opa/2012/09/.shtm.

60 Press Release, Fed. Trade Comm'n, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm.

61 Press Release, Fed. Trade Comm'n, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), http://www.ftc.gov/opa/2012/10/facial.shtm.

62 Alex Howard, *FTC Calls on Congress to Enact Baseline Privacy Legislation and More Transparency of Data Brokers*, STRATA (Mar. 27, 2012), http://strata.oreilly.com/2012/03/ftc-calls-on-congress-to-enact.html.

63 Several bills have been floated, however, that would step up privacy regulation in various ways. *See, e.g.*, Katy Bachman, *Rockefeller Reintroduces Do Not Track Act: Privacy Heats Up Again in Congress*, ADWEEK (Feb. 28, 2013, 5:46 PM), http://www.adweek.com/news/technology/rockefeller-reintroduces-do-not-track-act-147610.

64 Adam Thierer, Op-Ed., *The Problem with Obama's "Let's Be More Like Europe" Privacy Plan*, FORBES (Feb. 23, 2012, 3:37 PM), http://www.forbes.com/sites/adamthierer/2012/02/23/the-problem-with-obamas-lets-be-more-like-europe-privacy-plan.

65 The lack of BCA in the digital privacy policy discussion may be due to a general distaste for weighing the benefits against the costs which exists among privacy advocates and privacy-concerned policymakers. *See, e.g.*, James P. Nehf, The Limits of Cost-Benefit Analysis in the Development of Database Privacy Policy in the United States 1 (2007) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1001044 (opposing benefit-cost analysis in online privacy debates as the dominant decisionmaking tool.

is absolutely no consideration of the costs and benefits of regulation [in the report]."[66] The agency's more recent flurry of privacy reports, all issued during the Obama administration, likewise reflect the same general indifference toward serious BCA witnessed during previous administrations.[67]

To the extent that commercial data collection and advertising practices continue to be a pressing issue of governmental concern, BCA should be taken more seriously. In 2001, regulatory scholars Robert W. Hahn and Anne Layne-Farrar noted that "[g]iven the number of information privacy laws proposed, and the far-reaching implications on Internet commerce that some of these proposals seem to entail, one might expect a rich body of cost-benefit analysis. The surprising, and dismaying, reality is that not much in the way of quantification exists."[68] Sadly, not much has changed in the ensuing decade.

The following Sections outline the range of issues that legislators and regulatory agencies should consider when pondering more aggressive privacy regulations or even policy "nudges" and guidance documents that could alter existing marketplace practices.[69]

II. ANALYZING THE ASSERTED BENEFITS OF PRIVACY REGULATION

While Sunstein is correct that regulatory impact analysis at the federal level in the United States is "being addressed under a framework that is now broadly shared,"[70] that does not mean that BCA is without complication or controversy. This is particularly true for various forms of social regulation, such as online safety or privacy regulation.

This Section discusses the complexities of applying the benefit-cost framework to these issues and specifically examines the challenges of determining the benefits of regulatory enactments aimed at improving privacy online. Unfortunately, in the context of online privacy policy, federal offi-

---

66 FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, app. at 16 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (dissenting statement of Commissioner Orson Swindle).

67 Thomas M. Lenard & Paul H. Rubin, *The FTC and Privacy: We Don't Need No Stinking Data*, ANTITRUST SOURCE.COM 3-4 (Oct. 2012), http://www.americanbar.org/content/dam/aba/publishing/_source/oct12_lenard_10_22f.authcheckdam.pdf.

68 Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation* 51 (AEI-Brookings Joint Ctr. for Regulatory Studies, Working Paper No. 01-14, 2001), *available at* http://papers.ssrn.com/abstract=292649.

69 Executive Order 13422, issued by President Bush in 2007, specified that BCA should also cover guidance documents, which were defined as "an agency statement of general applicability and future effect, other than a regulatory action, that sets forth a policy on a statutory, regulatory, or technical issue or an interpretation of a statutory or regulatory issue." Exec. Order No. 13422, 72 Fed. Reg. 2,763 (Jan. 23, 2007), *available at* http://www.gpo.gov/fdsys/pkg/FR-2007-01-23/pdf/07-293.pdf.

70 Sunstein, *supra* note 19.

cials have not engaged in a rigorous effort to define how a state of "market failure" might currently exist.[71] Regardless, the Section considers some of the complaints or concerns often heard in privacy policy debates.

A. *The Challenge of Defining the Problem and/or Harm*

The fundamental problem with applying BCA to digital privacy proposals is that—as with online safety policy—it is riddled with emotional appeals[72] and highly subjective assertions of harm.[73] This makes it challenging to satisfy the first prerequisite of BCA: to provide "a clear explanation of the need for the regulatory action, including a description of the problem that the agency seeks to address."[74] Further complicating matters is the fact that, as Professor Alessandro Acquisti has noted, "[t]here may be privacy considerations that affect individuals' well-being and are not merely intangible, but in fact immeasurable."[75] Again, the same is true for online safety. What constitutes optimal "safety" and "privacy" online is both hopelessly subjective[76] and difficult to quantify.[77]

Estimating the supposed benefits of privacy regulation is also challenging when the asserted harm is that targeted online advertising or data collection is "creepy," which is an increasingly common claim.[78] Elsewhere, I have documented the problems associated with reducing privacy harms to allegations of "creepiness," "annoyance," or "unwanted solicita-

---

71 Lenard & Rubin, *supra* note 67, at 2. ("The Commission and Staff Reports do not provide a rigorous analysis of whether market failures exist with respect to privacy.").

72 Larry Downes, *A Rational Response to the Privacy "Crisis,"* CATO INST., 6 (Jan. 7, 2013), http://www.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf ("[F]or most consumers and policymakers, privacy is not a rational topic. It's a visceral subject, one on which logical arguments are largely wasted. Americans seem wired to react strongly and emotionally just at the mention of the word 'privacy,' or the suggestion that some new technology is challenging it.").

73 Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978) ("The concept of 'privacy' is elusive and ill defined. Much ink has been spilled in trying to clarify its meaning."); Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 295 (1975) ("Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.").

74 OIRA, RIA PRIMER, *supra* note 35, at 2.

75 Alessandro Acquisti, *The Economics of Personal Data and the Economics of Privacy*, ORG. FOR ECON. CO-OPERATION & DEV. 3 (2010), http://www.oecd.org/sti/ieconomy/46968784.pdf.

76 Thomson, *supra* note 73.

77 Michael A. Turner, *Measuring the True Cost of Privacy: A Rebuttal to "Privacy, Consumers, and Costs,"* INFO. POLICY INST., 12 (Oct. 2002), http://perc.net/files/downloads/gellmanlong.pdf ("Interpersonal comparisons of relative gains to utility from each additional unit of privacy enhancement (measuring how much more I enjoy additional privacy legislation versus my neighbor) is impossible, and can only be roughly estimated through a proxy measure—such as a monetary unit.").

78 Stacey Higginbotham, *Apps: It's Time to Talk About the Creepy Factor*, BLOOMBERG BUSINESSWEEK (Apr. 13, 2012), http://www.businessweek.com/articles/2012-04-13/apps-its-time-to-talk-about-the-creepy-factor.

tions."[79] Such theories of harm make BCA virtually impossible, since the debate becomes purely about emotion instead of anything empirical.[80]

Others try to describe privacy harms in terms of negative externalities[81]—"when one person's revelation of information reveals something about someone else"[82]—but typically fail to explain the concrete harm or consider the corresponding positive externalities that might also be associated with increased information sharing.[83]

Another complication with safety and privacy valuation lies in the nature of BCA itself. BCA often "implicitly assumes a risk-neutral decision-maker," even though "[t]here are many circumstances in which this is not appropriate."[84] In the context of online safety and digital privacy, this is clearly the case. Risk-takers abound with web users placing more information online about themselves and others with each passing year,[85] making it clear that many consumers derive benefits from information sharing.[86]

Consumers' apparent lack of concern about sharing information leads some academics and regulatory advocates to worry that people may not be acting in their own best self-interest when it comes to online safety and digital privacy choices.[87] For example, Professor Siva Vaidhyanathan says

---

79 Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 419 (2013).

80 J.R. SMITH & SIOBHAN MACDERMOTT, WIDE OPEN PRIVACY: STRATEGIES FOR THE DIGITAL LIFE 91 (2012) ("Overwhelmingly, the harms alleged are vague and inadequately supported.").

81 Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 23 (2006) (discussing how privacy-related externalities are similar to environmental externalities).

82 Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y INFO. SOC'Y 425, 446 (2011).

83 *Id.* at 447-48.

84 Roger Clarke, *Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism*, ROGERCLARKE.COM (Nov. 1994), http://www.rogerclarke.com//MatchCBA.html.

85 Ken Deeter, *Live Commenting: Behind the Scenes*, FACEBOOK (Feb. 7, 2011, 10:00 AM), http://www.facebook.com/note.php?note_id=496077348919 (noting that, in 2011, Facebook users submitted around 650,000 comments on the 100 million pieces of content served up every minute on the site).

86 Richard Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 251 (2008) ("[A]s long as people do not expect that the details of their health, love life, finances, and so forth, will be used to harm them in their interactions with other people, they are content to reveal those details to strangers when they derive benefits from the revelation.").

87 *See, e.g.*, Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999); MacCarthy, *supra* note 82, at 443 ("The idea is that individual choice in this area would lead, in a piecemeal fashion, to the erosion of privacy protections that are the foundation of the democratic regime, which is the heart of our political system. Individuals are making an assessment—at least implicitly—of the advantages and disadvantages to them of sharing information. They are determining that information sharing is, on balance, a net gain for them. But the aggregate effect of these decisions is to erode the expectation of privacy and also the role of privacy in fostering self-development, personhood, and other values that

consumers are being tricked by the "smokescreen" of "free" online services and "freedom of choice."[88] Although he admits that no one is forced to use online services and that consumers are also able to opt out of most of its services or data collection practices, Professor Vaidhyanathan argues that "such choices mean very little" because "the design of the system rigs it in favor of the interests of the company and against the interests of users."[89] He suggests that online operators are sedating consumers using the false hope of consumer choice.[90] "Celebrating freedom and user autonomy is one of the great rhetorical ploys of the global information economy," he says.[91] "We are conditioned to believe that having more choices—empty though they may be—is the very essence of human freedom. But meaningful freedom implies real control over the conditions of one's life."[92]

Paternalistic claims clash mightily with the foundational principles of a free society—namely, that individuals are autonomous agents that should be left free to make choices for themselves, even when some of those choices strike others as unwise. The larger problem with such claims is: where does one draw the line in terms of the policy action they seemingly counsel? Taken to the extreme, such reasoning would open the door to almost boundless controls on the activities of consumers online.

For purposes of this Article, we can set aside the liberty constraints sanctioned by such thinking and instead merely note here that such reasoning has no place in serious BCA. That is, assertions that people cannot be trusted to look out for themselves would make the entire project of BCA a meaningless exercise. It would imply that the benefits of regulation are virtually boundless and that the costs should generally be ignored in order to essentially save consumers from their own choices.[93]

These factors might explain why the Obama administration and other public officials have failed to fully grapple with the question of privacy harms in their recent privacy reports and statements. Under traditional harms-based analysis, agencies consider whether concrete harms exist and then weigh the benefits of regulation against its costs.[94] The FTC formalized

---

underlie the liberal way of life. In this way, individual choices are not sufficient to justify information practices that collectively undermine widely shared public values." (footnote omitted)).

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

89 *Id.* at 84.

90 *Id.*

91 *Id.* at 89.

92 *Id.*

93 Benjamin R. Sachs, Comment, *Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us from Ourselves*, 95 VA. L. REV. 205, 223-26 (2009) (arguing that regulation is needed due to the complexity of the information economy and the limits of consumer competence).

94 OMB, CIRCULAR A-4, *supra* note 33, at 2.

this process in its 1984 *Policy Statement on Unfairness*.[95] This statement clarified for members of Congress how the FTC interpreted and enforced its statutorily granted authority under Section 5 of the Federal Trade Commission Act.[96] Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[97]

In its unfairness policy statement, the agency noted that, "To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[98] As two former FTC officials have noted, this "is essentially a cost-benefit test."[99]

Of particular relevance to BCA for privacy enactments is the agency's requirement in the policy statement that "the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms. . . . Emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair."[100] But the FTC no longer seems interested in pursuing that approach, at least as it pertains to commercial privacy regulation. Commenting on the FTC's two recent privacy reports, economists Paul Rubin and Thomas Lenard observe that "[n]either FTC report contains any data on any harm, however defined. Demonstrating, and to the extent feasible quantifying, harm is important because it can be the starting point for assessing benefits, which are the reduced harms associated with increased privacy protection."[101]

Yet, in its preliminary privacy report issued in 2010, the FTC walked away from traditional harms-based analysis, arguing that:

> The FTC's harm-based approach also has limitations. In general, it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being

---

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

96 *See, e.g.*, Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 828-32 (2011); J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM'N (June 2003), http://www.ftc.gov/speeches/beales/unfair0603.shtm; J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Deceptive and Unfair Acts and Practices Principles: Evolution and Convergence, Speech at the Cal. State Bar (May 18, 2007), *available at* http://www.ftc.gov/speeches/rosch/070518.pdf.

97 15 U.S.C. § 45(a) (2006).

98 FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 95.

99 Beales & Muris, *supra* note 8, at 132.

100 FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 95 (footnotes omitted).

101 Lenard & Rubin, *supra* note 67, at 4.

> monitored or simply having private information "out there." Consumers may feel harmed when their personal information—particularly sensitive health or financial information—is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations.[102]

In one sense, the FTC's abandonment of strict harms-based analysis is understandable. Elsewhere I have argued that efforts to delineate the scope of privacy rights and associated harms may prove a quixotic quest, similar to a hypothetical effort to define a "right to happiness" and "happiness harms."[103] This is not to say that privacy, safety, or even happiness are unimportant values. To the contrary, everyone would agree that these values are important and that we have the right *to pursue* them.[104] But efforts to define them as "rights" and to delineate associated "harms" will always be extraordinarily challenging.

On the other hand, it is unwise to casually abandon the entire exercise of classifying privacy harms. It has been done in other contexts, even by the FTC.[105] In recent years, the FTC has brought and settled many cases involving its Section 5 authority to address identity theft and data security matters and, generally speaking, has been able to identify clear harms in each case.[106] Moreover, targeted legislation already addresses the special concerns raised by the collection or use of certain types of health information,[107] financial information,[108] or information about children.[109] Of course, it is true that the potential harms in those contexts are somewhat more concrete in nature. For health and financial information, for example, privacy violations can pose a more direct and quantifiable threat to personal well-being or property.

By contrast, the supposed harm associated with online advertising and commercial data collection is typically far more ambiguous and difficult to quantify. At a minimum, when conducting regulatory impact analysis for any new privacy proposals, policymakers should follow the advice set forth by OMB Circular A-4, which specifies:

---

102 FTC PRELIMINARY PRIVACY REPORT, *supra* note 50, at 20 (footnote omitted).

103 Thierer, *supra* note 79, at 414-17.

104 *Id.*

105 *See infra* Section IV.E.

106 FTC FINAL PRIVACY REPORT, *supra* note 50, at ii-iii; *see also* MacCarthy, *supra* note 82, at 483 ("There is . . . substantial case law on the FTC's use of unfairness that can be brought to bear on the question of whether specific acts or practices involving the collection and use of information are unfair.").

107 *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

108 *See, e.g.*, Truth in Lending Act, 15 U.S.C. §§ 1601–1667(f) (2006); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681(u) (2006).

109 *See, e.g.*, Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501-6506 (2006).

> You should exercise professional judgment in identifying the importance of non-quantified factors and assess as best you can how they might change the ranking of alternatives based on estimated net benefits. If the non-quantified benefits and costs are likely to be important, you should recommend which of the non-quantified factors are of sufficient importance to justify consideration in the regulatory decision. This discussion should also include a clear explanation that support designating these non-quantified factors as important. In this case, you should also consider conducting a threshold analysis to help decision makers and other users of the analysis to understand the potential significance of these factors to the overall analysis.[110]

B. *Enhancing Consumer Trust*

One commonly asserted benefit of commercial privacy regulation which is also found in recent reports from the FTC and the DOC is that it will "build trust" and encourage more citizens and companies to use online services.[111] For example, the FTC has argued that new privacy protections "not only will help consumers but also will benefit businesses by building consumer trust in the marketplace. Businesses frequently acknowledge the importance of consumer trust to the growth of digital commerce and surveys support this view."[112]

The FTC says it is particularly concerned that "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."[113] A similar claim was found in the DOC's 2010 privacy report, which asserted 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."[114]

Yet, in that same DOC report, the agency noted that "The Internet is also increasingly important to the personal and working lives of individual Americans. According to the report, 96 percent of working Americans use the Internet as part of their daily life, while 62 percent of working Americans use the Internet as an integral part of their jobs."[115] More recently, the digital analytics company comScore, Inc. reported that "[t]otal U.S. e-commerce spending reached $289.1 billion in 2012, representing an in-

---

110 OMB, CIRCULAR A-4, *supra* note 33, at 10.

111 Leslie Harris, *The Best Practices Act of 2010 and Other Federal Privacy Legislation*, CTR. FOR DEMOCRACY & TECH., 1 (July 22, 2010), http://www.cdt.org/files/pdfs/CDT_privacy_bill_testimony.pdf (arguing that privacy "is an essential building block of trust in the digital age").

112 FTC FINAL PRIVACY REPORT, *supra* note 50, at 8 (footnote omitted).

113 FTC PRELIMINARY PRIVACY REPORT, *supra* note 50, at 32.

114 COMMERCE PRIVACY & INNOVATION REPORT, *supra* note 52, at 15.

115 *Id.* at 14 (footnote omitted).

crease of 13 percent from 2011."[116] The statistics make it clear that online activity and commerce continues to grow at a healthy clip.

Moreover, the DOC's claim that "an erosion of trust will inhibit the adoption of new technologies"[117] does not seem credible when more than one billion people have registered Facebook accounts[118] despite the heightened privacy concerns surrounding that popular social networking site.[119] Consumers are using many other online sites and services in record numbers despite privacy and security concerns. Survey data from the Pew Internet & American Life Project, which tracks consumer trends, shows that broadband adoption, digital device ownership, and online participation continue to grow steadily over time.[120] comScore has also noted that, in 2012, "[a] staggering 5.3 trillion display ad impressions were delivered in the U.S.," a 6 percent increase over the previous year, and that "more than 450 billion U.S. content video views occurred via a desktop computer, representing an all-time high and an increase of 7 percent over 2011."[121] Also, a 2009 study of 2,600 consumers conducted by the National Retail Federation asked online shoppers the reasons they might not be spending as much online during the holiday season that year.[122] Of those who said they would be spending less online, the leading reasons were expensive shipping charges (22.8%), a preference to see or handle items before they buy them (12.5%), or a preference for buying in physical stores (10.8%).[123] By contrast, consumers expressed far less concern about online security (1.1%), credit card theft (0.6%), privacy (0.1%), or concerns about retailers tracking online activity (0.1%).[124]

These statistics call into question the assertion that expanded privacy regulation is needed to achieve greater consumer online trust or enhance online commerce. It is likely that there will always exist a handful of individuals who fear online interactions because of a theoretical loss of privacy or security, but neither FTC officials nor any other policymakers have pro-

---

116 COMSCORE, U.S. DIGITAL FUTURE IN FOCUS 2013: KEY INSIGHTS FROM 2012 AND WHAT THEY MEAN FOR THE COMING YEAR 27 (2013), *available at* http://www.comscore.com/Insights/Blog/2013__Future_in_Focus_Series.

117 COMMERCE PRIVACY & INNOVATION REPORT, *supra* note 52, at 15.

118 Barbara Ortutay, *Facebook Tops 1 Billion Users*, USA TODAY (Oct. 4, 2012), http://www.usatoday.com/story/tech/2012/10/04/facebook-tops-1-billion-users/1612613.

119 *See, e.g.*, Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, DEEPLINKS BLOG (Apr. 28, 2010), http://www.eff.org/deeplinks/2010/04/facebook-timeline.

120 Trend Data (Adults), PEW INTERNET & AM. LIFE PROJECT, http://www.pewinternet.org/Trend-Data-(Adults).aspx (last visited June 22, 2013).

121 COMSCORE, *supra* note 116, at 20, 23.

122 Press Release, Nat'l Retail Fed'n, Online Retailers to Emphasize Free Shipping, Social Media this Holiday Season (Oct. 22, 2009), http://www.nrf.com/modules.php?name=News&op=&sp_id=808.

123 *Id.*

124 *Id.*

duced compelling evidence that large numbers of citizens are waiting to get online until new privacy regulations are put on the books.

Finally, even if it is the case that the data collection and use practices of *some* online sites or services discourage consumer adoption, that does not constitute market failure. Consumers have the ability to pressure online providers to change their policies and then shop around for other options as needed. In other words, just because consumers might distrust particular sites does not necessarily mean they distrust the Internet as a whole.

C. *Regulatory Harmonization*

Some policymakers and privacy advocates claim that regulation can also benefit both consumers and companies by promoting greater harmonization of privacy policies internationally, which in turn would facilitate more efficient online commercial interactions or data flows.[125] The DOC has argued that America should look to "prevent conflicting policy regimes from serving as trade barriers."[126] The agency claims 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."[127]

Regulatory harmonization could have such benefits, but at least thus far no serious effort has been made to estimate those possible savings or efficiency gains. In fact, in the same report calling for regulatory harmonization to boost trade or data flows, the DOC notes that "[a] considerable amount of global commerce takes place on the Internet [and] [g]lobal online transactions currently total an estimated $10 trillion annually" and are growing.[128]

Moreover, regulatory equalization could also have costs if it is achieved by harmonizing in the direction of the more restrictive legal regimes. For example, if the American privacy regime was adjusted to look more like the one found in the European Union, which is far more regulatory in character, it is likely that compliance costs would increase for many online operators.[129] "If applied to American companies, these European laws would restrict the breakneck innovation of the commercial web," argues the NetChoice Coalition, which represents a variety of online ven-

---

125 Christopher Wolf & Winston Maxwell, *So Close, Yet So Far Apart: The EU and U.S. Visions of a New Privacy Framework*, 26 ANTITRUST 8, 10 (2012).

126 COMMERCE PRIVACY & INNOVATION REPORT, *supra* note 52, at 20.

127 *Id.* at 14.

128 *Id.* at 13.

129 Natasha Singer, *Data Protection Laws, an Ocean Apart*, N.Y. TIMES (Feb. 2, 2013), http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html.

dors.[130] Section III.C outlines other ways that privacy regulation could affect the global competitiveness of US firms and diminish their competitive advantage in the global digital arena.[131]

Finally, even if harmonization was considered a benefit of privacy regulation, there is no reason that it could not be achieved by encouraging the rest of the world to harmonize in the direction of the less regulatory approach that the United States has thus far utilized. That would achieve the benefits of harmonization without imposing new costs on US companies or users.

D. *Information Asymmetries*

Another commonly asserted benefit of privacy regulation is that it could help remedy information asymmetries in the online marketplace.[132] Economist Hal Varian has noted that "several of the problems with personal privacy arise because of the *lack* of information available between concerned parties."[133] Other scholars have argued that consumers lack knowledge about how their data might be used after it is shared or collected, leading to an information asymmetry.[134]

---

130 *NetChoice Reply Comments on Department of Commerce Green Paper* – Commercial Data Privacy in the Internet Economy: A Dynamic Policy Framework, NETCHOICE, 7 (Jan. 28, 2011), http://ssl.ntia.doc.gov/comments/101214614-0614-01/attachments/NetChoice%20Comments%20on%20%20Green%20Paper%20FINAL.pdf.

131 *See infra* Section III.C.

132 *See, e.g.*, Justin Zhan & Vaidyanathan Rajamani, *The Economics of Privacy*, INT'L J. SEC. & ITS APPLICATIONS, July 2008, at 101, 104 ("[T]he unpredictability of the consequences of information asymmetry is a big challenge in evaluating the economic impact of information disclosure and in developing a proper mechanism of incentives for the stakeholders."); MacCarthy, *supra* note 106, at 443-44 ("Others look at imbalances of bargaining power and knowledge asymmetries in the marketplace and conclude that choice in those circumstances is not reflective of consent. Collectors of information know what can be done with it or how it can be combined with other pieces of information to create profiles that have substantial economic value. Data subjects typically have no such knowledge and it is unreasonable to expect them to acquire it. This imbalance in the marketplace suggests that relying on individual choice alone will not protect people from harms in the use of information. Once again, consent does not render the underlying information practice legitimate.").

133 Hal R. Varian, *Economic Aspects of Personal Privacy*, *in* INTERNET POLICY AND ECONOMICS 101, 104 (William H. Lehr & Lorenzo Maria Pupillo eds., 2d ed. 2009), *available at* http://link.springer.com/content/pdf/10.1007%2Fb104899_7.pdf.

134 *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1253 (1998) ("[I]ndividuals today are largely clueless about how personal information is processed through cyberspace."); Acquisti, *supra* note 75, at 38 ("[A]fter an individual has released control on her personal information, she is in a position of information asymmetry with respect to the party with whom she is transacting. In particular, the subject might not know if, when, and how often the information she has provided will be used. For example, a customer might not know how the merchant will use the information that she has just provided to him through a website.").

Compared to other asserted privacy "harms," which remain highly controversial because of their ambiguous, amorphous nature, information asymmetry is a more widely accepted rationale for making a determination that "market failure" exists.[135] OMB Circular A-4 notes that "[m]arket failures may . . . result from inadequate or asymmetric information."[136] OMB also admits that "[e]ven when adequate information is available, people can make mistakes by processing it poorly."[137]

Importantly, however, Circular A-4 also notes that "the mere possibility of poor information processing is not enough to justify regulation" and that top-down regulation is not the only way to overcome informational asymmetries.[138] "If intervention is contemplated to address a market failure that arises from inadequate or asymmetric information, informational remedies will often be preferred."[139] The great advantage of such remedies is that they "leave consumers free to make their own choices, thus introducing less rigidity into the market," while at the same time they "leave the market free to respond as consumer preferences and production technologies change over time."[140] More importantly, the costs associated with potential regulatory error decreases significantly with informational remedies since they are not as sweeping in scope or impactful as other forms of regulation.[141]

Part IV discusses some of the less restrictive means that exist to educate and inform consumers and help overcome whatever information asymmetries may exist.[142] Another method of overcoming this problem is for firms, privacy advocates, and government to develop "smart disclosure" policies[143] that "can empower consumers by letting software do the work of

---

135 OMB, CIRCULAR A-4, *supra* note 33, at 5.

136 *Id.*

137 *Id.*

138 *Id.*

139 *Id.* at 9.

140 Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491, 513 (1981).

141 *Id.* ("[I]nformation remedies pose less risk of serious harm if the regulator turns out to have been mistaken.").

142 *See infra* Part IV.

143 Memorandum from Cass R. Sunstein, Adm'r, Office of Info. & Regulatory Affairs, to the Heads of the Exec. Dep'ts & Agencies (Sept. 8, 2011), *available at* http://www.whitehouse.gov//default/files/omb/inforeg/for-agencies/informing-consumers-through-smart-disclosure.pdf (defining "smart disclosure" as "the timely release of complex information and data in standardized, machine readable formats in ways that enable consumers to make informed decisions," and noting that "[s]mart disclosure will typically take the form of providing individual consumers of goods and services with direct access to relevant information and data sets. Such information might involve, for example, the range of costs associated with various products and services, including costs that might not otherwise be transparent. . . . In many cases, smart disclosure enables third parties to analyze, repackage, and reuse information to build tools that help individual consumers to make more informed choices in the marketplace").

reading privacy policies for them—and then implement their privacy preferences."[144]

As Section IV.B notes, whenever possible, transparency, and disclosure policies and efforts should be used instead of restrictive rules to address privacy concerns.[145] Consider how useful they have already been in the context of online safety. Voluntary media content ratings and labels for movies, music, video games, and smartphone apps have given parents and others more information to make determinations about the appropriateness of content they and their families may want to consume.[146] Regarding privacy, consumers are better served when they are informed about online privacy and data collection policies of the sites they visit and the devices they utilize. They are then in a better position to determine for themselves whether to utilize those services.

One must also consider how advertising and data collection actually help to alleviate different types of information asymmetries, such as a lack of consumer knowledge about new products and services.[147] Advertising and data collection communicates information to consumers and can educate and empower them in the process.[148] Nobel Prize-winning economist

---

144 Berin Szoka, *Responses to Questions for the Record of Berin Szoka on Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?*, TECHFREEDOM, 10 (Mar. 29, 2012), http://techfreedom.org/sites/default/files/QFR%20Szoka%20Privacy%20Hearing.pdf.

145 Howard Beales et al., *Information Remedies for Consumer Protection*, 71 AM. ECON. REV. (PAPERS & PROC.) 410, 413 (1981); Beales et al., *supra* note 140, at 522-23 ("[T]here is usually an advantage in designing disclosure remedies that leave as large a role as possible to normal market forces, to restrict the market as little as possible. The goal should be not to specify the exact information to be disclosed and the exact manner in which it will be disclosed but to give sellers the proper incentives to make these decisions on their own. This reduces the consequences of a bad decision by the government since it avoids forcing sellers to disclose information in an ineffective manner or to disclose information which, because of a change in circumstances, is no longer desired by consumers. It also increases the effectiveness of the remedy by harnessing sellers' own incentives to develop the most effective ways of informing consumers."); *see also infra* Section IV.B.

146 *See generally* Adam Thierer, *Parental Controls & Online Child Protection: A Survey of Tools & Methods*, PROGRESS & FREEDOM FOUND., 45-144 (Summer 2009), http://www.pff.org/parental/Parental%20Controls%20&%20Online%20Child%20Protection%20[VERSION%204.0].pdf (discussing ratings, labeling systems, and other tools to "help parents manage various media devices or different types of content").

147 J. Howard Beales & Jeffrey A. Eisenach, Putting Consumers First: A Functionality-Based Approach to Online Privacy 5-8 (Jan. 2013) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2211540 (summarizing the benefits of advertising and data collection for consumers and free markets).

148 *See, e.g.*, Fred S. McChesney, *De*-Bates *and Re*-Bates*: The Supreme Court's Latest Commercial Speech Cases*, 5 SUP. CT. ECON. REV. 81, 87 (1997) ("Advertising is a relatively low-cost way of imparting information of general interest . . . ."); Phillip Nelson, *Advertising as Information*, 82 J. POL. ECON. 729, 730 (1974) ("The advertising of search qualities provides information to the consumer, even though he attaches a probability less than one to the truthfulness of these advertisements."); Paul H. Rubin, *Regulation of Information and Advertising*, 4 COMPETITION POL'Y INT'L 169, 183-84 (2008) (identifying benefits associated with the advertisement of pharmaceuticals); Adam Thierer, *Advertising,*

George Stigler noted that advertising is "an immensely powerful instrument for the elimination of ignorance."[149] Similarly, former FTC official John E. Calfee argued, "advertising has an unsuspected power to improve consumer welfare" since it "is an efficient and sometimes irreplaceable mechanism for bringing consumers information that would otherwise languish on the sidelines."[150] Advertising also creates more efficient markets that can better serve consumers. As Calfee noted:

> Advertising's promise of more and better information also generates ripple effects in the market. These include enhanced incentives to create new information and develop better products. Theoretical and empirical research has demonstrated what generations of astute observers had known intuitively, that markets with advertising are far superior to markets without advertising.[151]

The argument in favor of advertising is equally applicable to "targeted" online advertising, which "is also more 'effective and valuable' for consumers, who thereby receive information they can actually use to make informed purchasing decisions."[152]

Finally, online sites and service providers "have a competitive incentive to inform consumers about the privacy protections they provide, and, in fact, are doing so."[153] This incentive can alleviate information asymmetries by offering consumers more information about online services. "You're seeing more companies trying to . . . develop privacy protecting services," notes Professor Joel R. Reidenberg.[154] "Platforms recognize they have to deal with privacy. They're looking at how they can be competitive."[155]

For example, Microsoft has been using privacy to differentiate itself from Google, both for online search and e-mail services. Microsoft has run ads claiming that "You're Getting Scroogled!" when using Gmail because

---

Commercial Speech, and First Amendment Parity, 5 CHARLESTON L. REV. 503, 507-11 (2011) ("Advertising provides important information and signals to consumers about goods and services that are competing for their allegiance.").

149 George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213, 220 (1961). *See also* J. Howard Beales III, *Consumer Protection and Behavioral Economics: To BE or Not to BE?*, 4 COMPETITION POL'Y INT'L 149, 152 (2008) ("Advertising is a particularly important source of information for most consumers in most markets.").

150 JOHN E. CALFEE, FEAR OF PERSUASION: A NEW PERSPECTIVE ON ADVERTISING AND REGULATION 96 (1997).

151 *Id.*

152 SMITH & MACDERMOTT, *supra* note 80, at 85.

153 PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 31 (2002).

154 Somini Sengupta, *Web Privacy Becomes a Business Imperative*, N.Y. TIMES (Mar. 3, 2013), http://www.nytimes.com/2013/03/04/technology/amid-do-not-track-effort-web-companies-race-to-look-privacy-friendly.html (quoting Professor Reidenberg) (internal quotation marks omitted).

155 *Id.*

of supposed privacy violations.[156] Similarly, a relatively new search engine, DuckDuckGo, has won praise for promoting its privacy-enhancing features.[157] "We believe in better search and real privacy at the same time," the site boasts, and it promises not to "track" users in any fashion.[158] In 2011, the company invested in billboards in the San Francisco area that bragged, "Google tracks you. We don't."[159] Free e-mail providers such as HushMail, RiseUp, and Zoho also compete on privacy to differentiate their services from major providers, such as Google's Gmail.[160] The fact that most of these services have not gained more traction suggests that consumers' general demand for privacy-enhancing technologies may be more limited than some privacy advocates suggest. Possible explanations are discussed in the following Section.

E. *The Role of Willingness-to-Pay Analysis*

Public policy discussions about digital privacy often treat privacy as a value that is shared equally by all. This is an error. "In the real world, preferences are rarely so uniform," notes practitioner Meredith Kapushion.[161] "Consumers have wildly divergent preferences based on their individual needs and tempered by the costs they are willing to bear."[162] Analyzing those costs and the consumers' willingness to pay for privacy should be an essential part of any BCA in this arena. Toward that end, OMB Circular A-4 specifies that:

> "Opportunity cost" is the appropriate concept for valuing both benefits and costs. The principle of "willingness-to-pay" (WTP) captures the notion of opportunity cost by measuring what individuals are willing to forgo to enjoy a particular benefit. In general, economists tend to view WTP as the most appropriate measure of opportunity cost, but an individual's "will-

---

156 Nick Wingfield, *Microsoft Attacks Google on Gmail Privacy*, N.Y. TIMES BITS BLOG (Feb. 6, 2013, 11:46 PM), http://bits.blogs.nytimes.com/2013/02/06/microsoft-attacks-google-on-gmail-privacy.

157 Nathan Safran, *Could DuckDuckGo Be the Biggest Long-Term Threat to Google?*, SEARCH ENGINE LAND (Apr. 26, 2012, 9:23 AM), http://searchengineland.com/could-duckduckgo-be-the-biggest-long-term-threat-to-google-118117.

158 *About*, DUCKDUCKGO, https://duckduckgo.com/about (last visited June 22, 2013).

159 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 (internal quotation marks omitted).

160 Kate Murphy, *How to Muddy Your Tracks on the Internet*, N.Y. TIMES (May 2, 2012), http://www.nytimes.com/2012/05/03/technology/personaltech/how-to-muddy-your-tracks-on-the-internet.html.

161 Meredith Kapushion, *Hungry, Hungry HIPPA: When Privacy Regulations Go Too Far*, 31 FORDHAM URB. L.J. 1483, 1491 (2003).

162 *Id.*

> ingness-to-accept" (WTA) compensation for not receiving the improvement can also provide a valid measure of opportunity cost.[163]

As applied to privacy policy consideration, willingness-to-accept "asks how much an individual would need to be compensated to permit a decrease in privacy," while willingness-to-pay "asks how much an individual would pay to experience an increment in privacy protection."[164]

Optimally, some sort of WTP/WTA analysis—using real-world data, not just laboratory experiments—would be conducted as part of any privacy-related BCA. Unfortunately, this is complicated by the fact that, for most online transactions today, no explicit trade or monetary transaction occurs. Moreover, when online sites and services *do* differentiate services to consumers, they are typically competing on something other than privacy or safety. For example, most premium options or "upselling" offers are based on other consumer needs or values, such as increased storage capacity, enhanced functionality, or additional service options. Consequently, there is an unfortunate lack of real-world experiments with competing versions of online sites and services that differentiate based on safety and privacy.[165]

Despite the lack of empirical data, some analysts suggest that paying for online services would help consumers achieve greater privacy protections. "Truly, the only way to get around the privacy problems inherent in advertising-supported social networks is to pay for services that we value," argues Alexis Madrigal of *The Atlantic*.[166] "It's amazing what power we gain in becoming paying customers instead of the product being sold."[167]

It remains unclear, however, whether web users would be willing to pay for what we might think of as a "privacy premium" for online sites and services that would presumably collect less personal information or serve up no targeted advertising. As noted, even if more online operators offered pay-for-service options, it is unclear whether they would differentiate themselves from rivals by focusing on privacy or safety enhancements. Paid offerings are just as likely—perhaps far more likely—to be tailored to other

---

163 OMB, CIRCULAR A-4, *supra* note 33, at 18.

164 Alessandro Acquisti et al., What is Privacy Worth? 5 (2009) (unpublished manuscript), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf.

165 NICOLA JENTZSCH ET AL., EUR. NETWORK & INFO. SEC. AGENCY, STUDY ON MONETIZING PRIVACY 4 (2012) [hereinafter ENISA, STUDY ON MONETIZING PRIVACY], *available at* http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy (noting that "a large share of literature is devoted" to surveys, that "economic experiments that implement real purchase transactions are rather scarce," and that "there are no works in economics that *combine theoretical and experimental methods* for the analysis of the interplay of privacy concerns, product personalisation and competition").

166 Alexis C. Madrigal, *Why You Should Want to Pay for Software, Instagram Edition*, THE ATLANTIC (Dec. 17, 2012, 1:10 PM), http://www.theatlantic.com/technology/archive/2012/12/why-you-should-want-to-pay-for-software-instagram-edition/266367.

167 *Id.*

user desires. In other words, it remains uncertain how much of a market there is for privacy, and this further complicates the question of whether any sort of market failure exists in this context.

The lack of clarity regarding consumer preferences for privacy does not mean the demand for online privacy sites or apps is zero, however. To the contrary, as will be noted in Part IV, a robust market for privacy empowerment tools *does* exist today, meaning that at least *some* segment of the population is willing to pay for such tools or services.[168] But, at least at this time, these privacy-enhancing tools and services tend to be downloads or add-ons that are optimized at the end-user level instead of at the site or platform level.

It could very well be the case that consumers are simply not willing to spend significant sums for greater online safety or privacy while "free" offerings remain viable. To many consumers, online services feel like the ultimate free lunch. Once consumers pay for underlying broadband access, a wide variety of free or extremely inexpensive services is available to them.[169] In essence, the relationship between consumers and online content and service providers is not governed by any formal contract but rather by an unwritten quid pro quo: users must tolerate some ads and a certain amount of data collection (to better target those ads or offer additional services) in exchange for those "free" online sites, services, or content.[170]

It is beyond the scope of this Article to explore the reasons why more pay-per-use or "privacy premium" business models have not developed in the marketplace, but the most compelling rationale is that consumers simply have not expressed a strong willingness to pay for them relative to the "free," ad-supported, data-driven models that currently dominate online.[171] The limited literature that exists in this field seems to bolster that explanation.[172]

---

168 *See infra* Section IV.C.

169 Chris Anderson, *The Economics of Giving It Away*, WALL ST. J. (Jan. 31, 2009), http://online.wsj.com/article/SB123335678420235003.html ("The standard business model for Web companies that don't actually have a business model is advertising. A popular service will have lots of users, and a few ads on the side will pay the bills.").

170 Quentin Fottrell, *Will Privacy Protections Ruin the Internet?*, MARKETWATCH (Feb. 5, 2013, 10:05 AM), http://www.marketwatch.com/story/will-privacy-protections-ruin-the-internet-2013-02-05 ("Consumers 'implicitly agree' to provide advertisers with data in order to receive timely and relevant recommendations for products. . . . Without having users' online habits tracked, experts say, social networks would have to start charging users to post photos, and search engines might be forced to charge for access to news, email services and tools like mapping apps." (quoting attorney Richard B. Newman)).

171 John Shaeffer, Op-Ed., *The Economics of Online Privacy*, FORBES (Mar. 26, 2012, 1:19 PM), http://www.forbes.com/sites/realspin/2012/03/26/the-economics-of-online-privacy ("Consumers have become accustomed to free as it relates to the internet and various failed ventures demonstrate that consumers do not want to change this model.").

172 Acquisti, *supra* note 75, at 36-37 (discussing recent literature on consumer willingness to pay for privacy).

A 2005 experiment by three German analysts from Humboldt-Universität zu Berlin noted that consumers "do not always act in line with their stated privacy preferences, giving away information about themselves without any compelling reason to do so."[173] Yet most WTP studies show that consumers often *do* have a fairly compelling reason to give away personal information: it saves them money. A 2012 study by the European Network & Information Security Agency ("ENISA") which combined laboratory and field experiments revealed a strong interest in privacy-friendly services among consumers when price was not a consideration.[174] However, where price differs among similar services, "the market share of the privacy-friendly service provider drops, below or close to one third" relative to the "privacy-invasive" offering.[175]

Professor Acquisti, who has authored several WTP studies and has simultaneously surveyed the literature in this field, has noted that the "results suggest a privacy paradox: people want privacy, but do not want to pay for it, and in fact are willing to disclose sensitive information for even small rewards."[176] For example, one of Professor Acquisti's co-authored studies revealed that, when confronted with the option to protect or sell their information, "individuals almost always chose to sell their information and almost never elect[ed] to protect their information even for values as little as $0.25."[177]

Generally speaking, while some of the consumers surveyed in these experiments express a greater willingness to pay for services that protect their privacy, for the vast majority of respondents, *price matters.* As Acquisti concluded in another co-authored study:

> [I]ndividuals assign markedly different values to the privacy of their data depending on a) whether they consider the amount of money they would accept to disclose otherwise private information, or the amount of money they would pay to protect otherwise public information; and b) the order in which they consider different offers for that data. Moreover, the gap be-

---

173 Bettina Berendt et al., *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior*, COMM. OF THE ACM, Apr. 2005, at 101, 104, *available at* http://www.wiwi.hu-berlin.de/professuren//wi/personen/hl/downloads/BGS.pdf.

174 ENISA, STUDY ON MONETIZING PRIVACY, *supra* note 165, at 37-39.

175 *Id.* at 1, 5.

176 Acquisti, *supra* note 75, at 37. *See also* Somini Sengupta, *Letting Down Our Guard with Web Privacy*, N.Y. TIMES (Mar. 30, 2013), http://www.nytimes.com/2013/03/31/technology/web-privacy-and-how-consumers-let-down-their-guard.html (summarizing Professor Acquisti's recent research in this area).

177 Jens Grossklags & Alessandro Acquisti, When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information (June 7, 2007) (unpublished manuscript), *available at* http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags_Acquisti-WEIS07.pdf.

> tween such values is larger than that observed in comparable studies of other private goods.[178]

In a sense, there is no more a "privacy paradox" than there is a "milk paradox": people will say they want milk, and they will gladly accept it if it is being offered for free.[179] The fact that they want less of it when they have to pay for it is, therefore, not a paradox. By extension, "if privacy were free, we would all want more."[180] Yet, when faced with real-world trade-offs—higher prices, less service, lower quality products, etc.—many people reveal that they are willing to trade privacy for other benefits.

Importantly, lab experiments,[181] surveys, and public opinion polls[182] represent a poor substitute for real-world WTP analysis. All too often, privacy advocates and policymakers make assertions about online safety and digital privacy based largely upon such polling or survey data.[183] Yet, polls typically fail to offer useful insights regarding how much people actually value safety and privacy relative to the benefits they receive. "Empirical research on [privacy] is still in its infancy,"[184] notes *New York Times* reporter Somini Sengupta. "Most studies ask for personal opinion, rather than measure the digital choices people make, and even there, the results usually find a gap between what people say and what they do about their privacy online."[185]

Often, this discrepancy is because polls ask simplistic questions about whether consumers care about their privacy without requiring the respondents to even bother with the mental calculus of evaluating the trade-offs associated with regulations aimed at enhancing online privacy.[186] Even then,

---

178 Acquisti et al., *supra* note 164, at 1.

179 The Author is indebted to Jerry Ellig for suggesting this analogy.

180 Kapushion, *supra* note 161, at 1487.

181 Beales, *supra* note 149, at 163 ("Experimental economics certainly has a valuable place in the literature, but it is generally unwise to treat public policy as an uncontrolled experiment. Before intervening in admittedly imperfect markets, policymakers should have a sound basis for concluding that the benefits of the intervention will exceed the costs and that the intervention will in fact increase consumer welfare.").

182 Kai-Lung Hui & I.P.L. Png, The Economics of Privacy 17 (2006) (manuscript), *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy_HISE.pdf ("Clearly, it would be misleading to judge the importance of privacy from opinion polls alone. Rigorous experiments are necessary to gauge the actual value that people attach to their personal information under various circumstances.").

183 Berin Szoka, *Privacy Polls v. Real-World Trade-Offs*, PROGRESS & FREEDOM FOUND., 1-7 (Nov. 2009), http://www.pff.org/issues-pubs/ps/2009/pdf/ps5.10-privacy-polls-tradeoffs.pdf.

184 Somini Sengupta, *What Would You Pay for Privacy?*, N.Y. TIMES BITS BLOG (Mar. 19, 2012, 8:30 AM), http://bits.blogs.nytimes.com/2012/03/19/what-would-you-pay-for-privacy.

185 *Id.*

186 Jim Harper & Solveig Singleton, With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us (June 2001) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.?abstract_id=299930 ("[P]rivacy surveys in particular . . . suffer from the 'talk is cheap' problem. It costs a consumer nothing to express a desire for federal law to protect privacy. But if such law became a

some polls suggest privacy isn't as big a concern as some regulatory advocates suggest.[187] Of course, how polling questions are framed likely has a profound bearing on how much people say they value privacy.[188] Regardless, simply because people say they are concerned about privacy does not mean they will pay a premium for it.[189] Further analysis, and more careful WTP/WTA analysis, is necessary when conducting BCA for privacy proposals.[190]

III. COST CONSIDERATIONS FOR PRIVACY REGULATION

The previous Section highlighted some of the issues that must be considered when evaluating the asserted benefits of privacy-related laws and regulations. The benefits side of the BCA analysis for privacy proposals will always be riddled with heated definitional disputes over the scope of privacy rights and harms. In comparison, evaluating the costs of proposed rules is somewhat less controversial. This Section outlines some of the considerations that must be taken into account when evaluating the impact of privacy-related regulatory proposals aimed at limiting data collection or personalized advertising.

---

reality, it will cost the economy as a whole, and consumers in particular, significant amounts that surveys do not and cannot reveal.").

187 Larry Magid, *Most People Taking a Facebook Break Don't Cite Privacy As the Reason*, FORBES (Feb. 5, 2013, 6:47 PM), http://www.forbes.com/sites/larrymagid/2013/02/05/surprise-most-people-taking-a-facebook-break-dont-cite-privacy-as-the-reason.

188 Daniel Castro, *New Survey Shows Some Privacy Scholars Lack Objectivity*, INNOVATION FILES (Oct. 14, 2012), http://www.innovationfiles.org/new-survey-shows-some-privacy-scholars-lack-objectivity.

189 Jessica Guynn, *Gmail is Target of New Microsoft Privacy Campaign Against Google*, L.A. TIMES, (Feb. 6, 2013), http://www.latimes.com/business/technology/la-fi-tn-microsoft-privacy-campaign-against-google-gmail-20130206,0,6815888.story (quoting SearchEngineLand.com founding editor Danny Sullivan as saying, "While people in polls say they are concerned, in reality they are really not that concerned").

190 RUBIN & LENARD, *supra* note 153, at 57 ("Public opinion data are not a good substitute for public policy analysis."); Luc Wathieu & Allan Friedman, *An Empirical Approach to Understanding Privacy Valuation* (Harvard Bus. Sch., Div. of Research, Working Paper No. 07-075, 2007), *available at* http://www.hbs.edu/faculty/Publication%20Files/07-075.pdf ("To understand and model privacy, more information is needed about consumer preferences, beyond 'people want privacy.'").

A. *The Costs to Producers of Digital Services*

Aggregated information, or "big data," is the fuel that powers much of the digital economy.[191] Kenneth Cukier and Professor Viktor Mayer-Schönberger, authors of *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, define "big data" as "the vast quantity of information now available thanks to the Internet, and which can be manipulated in ways never before possible."[192] It "is becoming a backbone of corporate performance and economic growth."[193] For many online operators or digital media firms, information about their customers may be the firm's only monetizable asset or intellectual property.[194] It allows those firms to better tailor services to existing customers while also finding new audiences or customers.[195] Professor Jonathan Ezor explains how data about users can be a valuable asset:

> Knowing the identity of current customers means that companies can offer a faster, more tailored experience, providing those goods or services the customer has previously or regularly purchased in a more prominent location, or being ready to give the customer "her usual." Knowing who one's *potential* customers are enables more effective sales pitches and solicitations; as much as consumers may be jaded when it comes to "personalized" messages in this database age, such messages are still more likely to catch their attention than those without the consumers' names on the envelope or e-mail subject line.
>
> Companies have also long understood that their customer records may have value to *other* firms, and have sought to monetize that value. Whether through sharing, renting or selling customer lists, or by sending third-party solicitations to one's own customers, businesses are able to lower costs and generate revenue well outside their ordinary operations through data mining and marketing, at times beyond the earnings potential from their core businesses.[196]

The FTC acknowledges these realities, noting: "The growth in mobile and social networking services in particular is striking, and is funded, in part, by the growth of targeted advertising that relies on use of consumer

---

191 *See* MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 15 (2011); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63 (2012).

192 Kenneth Cukier & Viktor Mayer-Schönberger, Op-Ed., *The Financial Bonanza of Big Data*, WALL ST. J. (Mar. 7, 2013, 6:58 PM), http://online.wsj.com/article/SB10001424127887324178904578 3.html.

193 *Id.*

194 *Id.* ("Companies world-wide are starting to understand that no matter what industry they are in, data is among their most precious assets. Harnessed cleverly, the data can unleash new forms of economic value."); JONATHAN I. EZOR, PRIVACY AND DATA PROTECTION IN BUSINESS: LAWS AND PRACTICES 7 (2012) ("Ultimately, in an economy driven by knowledge and information, knowing more things, about more people, will always be an asset.").

195 Beales & Muris, *supra* note 8, at 109-12 (summarizing the benefits of information exchange in the digital economy).

196 EZOR, *supra* note 194, at 6.

data."[197] This growth is equally true for the "apps economy," which relies heavily on data collection and advertising.[198]

By disrupting this process, regulation could diminish investment in new forms of news, entertainment, and other information services.[199] Media sector analysts have long stressed the central role of advertising in sustaining newspapers, magazines, broadcast radio, and television.[200] "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.*[201]

The advertising-driven model remains essential in the modern information economy. To reiterate, at least thus far, online advertising—powered by data collection—has proven "to be the only business model with any real staying power."[202] There are other methods of sustaining online sites and services—e.g., pay-per-view, micropayments, and subscription-based business models—but they are far less common than ad-supported sites and services. As technology consultant Larry Downes explains, the lack of success of these options is likely because, "For better or worse (almost certainly better), Internet users are hooked on the 'free' software, content, and services that rely for revenue on information collection and use."[203]

In a privacy-related BCA context, therefore, any regulatory proposal or enactment should be closely scrutinized to determine the impact on the overall health of the digital economy. Correspondingly, regulators should consider the aggregate amount of information and content that can be produced or supported by those sectors.[204] A 2010 study by Howard Beales,

---

197 FTC PRELIMINARY PRIVACY REPORT, *supra* note 50, at 21.

198 John Manoogian III, *How Free Apps Can Make More Money Than Paid Apps*, TECH CRUNCH (Aug. 26, 2012), http://techcrunch.com/2012/08/26/how-free-apps-can-make-more-money-than-paid-apps.

199 *See, e.g.*, Adam Thierer, *Unappreciated Benefits of Advertising & Commercial Speech*, MERCATUS CTR., 1-4 (Jan. 14, 2011), http://mercatus.org/publication/unappreciated-benefits-advertising-and-commercial-speech (surveying what various economists and market analysts have said about the role of advertising in sustaining media content and enterprises).

200 Mary Alice Shaver, *The Economics of the Advertising Industry*, *in* MEDIA ECONOMICS: THEORY AND PRACTICE 249, 250 (Alison Alexander et al. eds., 3d ed. 2004) ("Advertising revenues pay for virtually all broadcast media, 70% to 80% of support for newspapers and an equally high percentage for magazines.").

201 ROBERT G. PICARD, THE ECONOMICS AND FINANCING OF MEDIA COMPANIES 122 (2002).

202 Berin Szoka & Adam Thierer, *Targeted Online Advertising: What's the Harm & Where Are We Heading?*, PROGRESS & FREEDOM FOUND., 9 (June 2009), http://www.pff.org/issues-pubs/pops/2009/.2targetonlinead.pdf.

203 Downes, *supra* note 72, at 16.

204 LARRY DOWNES, THE LAWS OF DISRUPTION: HARNESSING THE NEW FORCES THAT GOVERN LIFE AND BUSINESS IN THE DIGITAL AGE 83-84 (2009) ("Much of the valuable information content available on the Internet, and so many of the useful services we use every day, is free. Why? Not because of some utopian dream of inventors or even because of the remarkably low transaction costs of 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."[205] 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 because of the increased conversion of ads into sales."[206] "Finally," Beales continues, "a majority of network advertisers' revenue is spent acquiring inventory, making [behavioral targeting] an important source of revenue for publishers as well as ad networks."[207]

Again, this finding is in line with the earlier generation of media economists who noted how advertising can cross-subsidize and sustain content and culture and ensure more and better services are made available to consumers.[208] Beales notes this development is particularly important to keep in mind today because, "[a]s 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."[209]

Regulatory agencies are not blind to the danger of decreased media output. In recent years, both the FTC and the FCC have conducted investigations on the health of media and the future of journalism. The FTC conducted a series of workshops and produced a staff report pondering the question, "*How Will Journalism Survive the Internet Age?*"[210] The FCC also hosted a series of workshops on the future of media which considered similar questions and concerns about the future viability of media enterprises and resulted in a major report on the issue.[211] When these or other agencies are conducting BCA for privacy-related regulatory enactments, the potential costs of regulation for digital media and content-producing sectors should be taken into account.

---

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.").

205 Howard Beales, *The Value of Behavioral Targeting*, NETWORK ADVER. INITIATIVE, 3 (Mar. 2010), www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

206 *Id.* at 6.

207 *Id.*

208 Thierer, *supra* note 148, at 512-14.

209 Beales, *supra* note 205, at 18.

210 *How Will Journalism Survive the Internet Age?*, FED. TRADE COMM'N, http://www.ftc.gov//workshops/news/index.shtml (last visited June 23, 2013).

211 STEVEN WALDMAN, FED. COMMC'NS COMM'N, THE INFORMATION NEEDS OF COMMUNITIES: THE CHANGING MEDIA LANDSCAPE IN A BROADBAND AGE 8-9 (2011), *available at* http://transition.fcc.gov/osp/inc-report/The_Information_Needs_of_Communities.pdf.

B. *Costs to Consumers*

If regulation prohibits information collection or makes it easier for consumers to opt out of the current online value exchange (i.e., trading personal information for online services, most of which are free of charge), it would have both benefits and costs. The benefit is that those consumers who desire greater privacy might be able to achieve it. The downside is that it could result in higher prices, fewer services, lower-quality services, more "annoying" forms of advertising (such as "pop-up" banners or video ads), or some combination of all of the above.[212]

In other words, as suggested above, if privacy regulation imposes costs on producers of digital media services by breaking the current monetization model that powers most online activity, those costs could be passed along to consumers. This change would be problematic since "customers have come to expect personalized services and simple access to information systems."[213] As part of any BCA for privacy-related proposals, these costs should be evaluated and quantified.

C. *Market Structure / Competition*

Privacy regulation could also have an impact on market structure and the competitive health of various online sectors. "In a setting where first-party marketing is allowable but third-party marketing is not, substantial advantages may be created for large incumbent firms," argue Professors Avi Goldfarb and Catherine Tucker.[214]

> 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.[215]

Professors Goldfarb and Tucker found that "after the [European Union's] Privacy Directive was passed [in 2002], advertising effectiveness decreased on average by around 65% in Europe relative to the rest of the

---

212 Vineeth Narayanan, Negative Externalities of Enhanced Choice, Comment Submitted for Consideration in Fed. Trade Comm'n Draft Report on Consumer Privacy 14, 15 (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00359-57966.pdf ("[E]very consumer that decides to withhold their data decreases the value the vendor may retrieve from advertising and creates a negative externality for the rest of the users.").

213 Zhan & Rajamani, *supra* note 132, at 101.

214 Avi Goldfarb & Catherine Tucker, Comments on 'Information Privacy and Innovation in the Internet Economy' 4 (Jan. 24, 2011), *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/NTIA_comments_2011_01_24.pdf.

215 *Id.*

world."[216] They argue that because regulation decreases ad effectiveness, "this may change the number and types of businesses sustained by the advertising-supported Internet."[217] 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.[218] This could also have antitrust implications that the FTC or other agencies would need to take into account when considering new privacy rules.

To the extent privacy *has* been considered in an antitrust context in recent years, however, it has often been with an eye toward making greater privacy protection part of formal antitrust reviews (or even as a prerequisite of merger approval).[219] From an antitrust perspective, the introduction of privacy as a metric for evaluating policy complicates traditional competition policy analysis. The fundamental subjectivity of privacy means that consumer harm cannot be evaluated as objectively as it can when price and output are the primary focus of consideration, as is traditionally the case for antitrust policy. Moreover, the introduction of privacy as a variable in antitrust analysis raises the specter of extremely broad regulatory discretion, the possibility of regulatory overdeterrence, and even potential rent-seeking opportunities.

However, to the extent that privacy *is* introduced as a consideration in antitrust reviews, the issues raised in this Section must be taken into account. That is, policymakers must consider the impact new privacy rules will have on market structure and competition and whether that negatively affects consumer welfare in other ways.[220]

---

216 Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. 57, 58 (2011), *available at* http://mansci.journal.informs.org/content/57/1/57.full.pdf+html. *See also* Catherine Tucker, *Empirical Research on the Economic Effects of Privacy Regulation*, 10 J. ON TELECOMM. & HIGH TECH. L. 265, 265 (2012).

217 Goldfarb & Tucker, *supra* note 216.

218 Fottrell, *supra* note 170.

219 Peter P. Swire, Submitted Testimony to the Federal Trade Commission, Behavioral Advertising Town Hall 1 (Oct. 18, 2007), http://ftc.gov/os/comments/behavioraladvertising/071018peterswire.pdf (explaining "as a general matter how privacy harms are relevant to antitrust analysis" and stating that "it is logical to consider privacy remedies as part of merger analysis").

220 Lydia Parnes & Edward Holman, *The Role of Competition in Analysing a Consumer Protection Remedy: Should Regulators Consider Competition Law in Urging a 'Do Not Track' Solution?*, COMPETITION L. INT'L, Nov. 2011, at 72, 74 ("Competition among these companies will help develop the most effective means of providing notice and choice that balances consumer privacy concerns with the needs of advertisers and publishers. Choosing a winning Do Not Track implementation too early, however, effectively kills this emerging market before it has the opportunity to meet consumer privacy demands.").

D. *Other Costs & Constitutional Values*

While BCA is primarily concerned with economic trade-offs associated with regulation, in the context of social regulation it is often necessary to evaluate other values or constitutional constraints implicated by government action. In the case of privacy-related regulatory enactments, for example, free speech concerns might be raised by some regulatory proposals.[221]

Information technology is, by definition, tied up with the production and dissemination of speech. Consequently, First Amendment values may be affected by administrative regulation that limits data collection or reporting.[222] Professor Eugene Volokh has noted that "the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me."[223] But in the United States, he notes, "We already have a code of 'fair information practices,' and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits), whether the communication is 'fair' or not."[224]

Press rights are also implicated by stronger commercial privacy controls. Philosopher Judith Jarvis Thomson has argued:

> [E]ven if there is a right to not be caused distress by the publication of personal information, it is mostly, if not always, overridden by what seems to me a more stringent right, namely the public's right to a press which prints any and all information, personal or impersonal, which it deems newsworthy . . . .[225]

In the wake of the Supreme Court's 2011 decision in *Sorrell v. IMS Health Inc.*,[226] these First Amendment concerns are even more relevant.[227] *Sorrell* dealt with a state law prohibiting data aggregators from selling personal information to pharmaceutical companies, which in turn use the data

---

221 Walker, *supra* note 6, at 123 ("Recognizing that we are legislating in the shadow of the First Amendment suggests a powerful guiding principle for framing privacy regulations. Like any laws encroaching on the freedom of information, privacy regulations must be narrowly tailored and powerfully justified.").

222 Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 51 (2002) ("[T]o the extent that privacy laws restrict expression, even if that expression is commercial, the First Amendment imposes a considerable burden on the government to demonstrate the need and effectiveness of those laws.").

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

224 *Id.* at 1051 (footnote omitted).

225 Thomson, *supra* note 73, at 310.

226 131 S. Ct. 2653 (2011).

227 *Id.* at 2659.

to customize their marketing pitches to doctors.[228] The Court held that restrictions on the sale, disclosure, and use of personally-identifying information were subject to heightened judicial scrutiny.[229] Agreeing with the lower court, the Supreme Court found that the regulation violated the First Amendment because it restricts the speech rights of data miners without directly advancing legitimate state interests.[230] In line with its ruling in *Thompson v. Western States Medical Center*,[231] the Court noted that "'the fear that people would make bad decisions if given truthful information' cannot justify content-based burdens on speech."[232]

A related concern involves the impact of data collection limitations on scholarly research, including public health studies, social science, and humanities research.[233] Restrictions on data collection could limit legitimate scientific research that has real benefits for citizens. Professors Daniel Barth-Jones[234] and Jane Yakowitz[235] have argued that "[p]ublic research data produces rich contributions to our collective pursuit of knowledge and justice" and that the risk posed by data collection and identification are negligible.[236] While some privacy theorists argue that data is not speech,[237] other scholars, echoing the Court in *Sorrell*, recognize that restrictions on data collection are restrictions on the free flow of information, which implicate the First Amendment.[238]

---

228 *Id.* at 2660.

229 *Id.* at 2659.

230 *Id.* at 2672; Yara Tercero-Parker, *US Supreme Court Questions State Drug Data Restrictions*, ETHICS ILLUSTRATED (Apr. 27, 2011), http://www.bioethicsinternational.org/blog/2011/04/27/us-supreme-court-questions-state-drug-data-restrictions/.

231 535 U.S. 357 (2002).

232 *Sorrell*, 131 S. Ct. at 2658 (quoting Thompson v. W. States Med. Ctr., 535 U.S. at 374).

233 David Erdos, *Mustn't Ask, Mustn't Tell*, TIMES HIGHER EDUC. (Feb. 14, 2013), http://www.timeshighereducation.co.uk/comment/opinion/mustnt-ask-mustnt-tell/2001494.article (describing the "radical underestimation of the threat these [data protection] regulations pose to the enjoyment of other fundamental rights and the pursuit of legitimate activities").

234 Daniel C. Barth-Jones, The "Re-Identification" of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now 12-13 (July 24, 2012) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/.cfm?abstract_id=2076397.

235 Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 4 (2011).

236 *Id.*

237 Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1173-74 (2005); Tim Wu, Op-Ed., *Free Speech for Computers?*, N.Y. TIMES (June 19, 2012), http://www.nytimes.com/2012/06/20/opinion/free-speech-for-computers.html.

238 Jane Yakowitz Bambauer, *Is Data Speech?*, 66 STAN. L. REV. (forthcoming 2014) (manuscript at 1), *available at* http://ssrn.com/abstract=2231821 ("Data privacy laws regulate minds, not technology. Thus, for all practical purposes, and in every context relevant to the privacy debates, data is speech.").

IV. ALTERNATIVES TO ADMINISTRATIVE REGULATION

As specified by OMB Circular A-4 and other OIRA guidance, the other crucial part of any regulatory impact analysis is a clear identification of a range of regulatory approaches as well as alternatives to formal regulation.[239]

This Section will briefly outline some of those alternatives and argue that it is particularly wise to consider such less restrictive approaches for online safety and digital privacy. This is because preemptive regulation of information technology can be costly, complicated, and overly constraining.[240] Education and empowerment-oriented strategies also avoid the legal and constitutional controversies often associated with regulatory enactments. Such strategies also avoid an over-reliance on regulatory nostrums that will likely fail to adequately address online safety and privacy concerns over the long haul.[241] Thus, such strategies can help build resiliency among citizens and ensure easier assimilation of new technologies into society.[242]

A. *Education and Awareness-Building*

To the extent "[t]here are reasons to believe that consumers act myopically when trading off the short term benefits and long term costs of information revelation and privacy invasions,"[243] education and awareness-building efforts offer a cost-effective way of remedying that problem.[244]

The United States has been tapping education and awareness-based efforts on the online safety front for many years. After years of efforts to devise legislative and regulatory responses to online safety concerns, policymakers and online safety experts have instead increasingly looked to expand traditional online education and media literacy strategies to focus on "digital citizenship" and critical thinking as the primary defense against unwanted or objectionable online content and communications.[245] Such

---

239 OMB, CIRCULAR A-4, *supra* note 33, at 7-9.

240 Thierer, *supra* note 1, at 376-79.

241 SMITH & MACDERMOTT, *supra* note 80, at 165-66 ("[A]t this point, the attempt to impose one-size-fits-all regulation on an as-yet-to-be-fully-known Internet strikes us as impractical, ineffective, and quite possibly counterproductive to continued innovation.").

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

243 Acquisti, *supra* note 75, at 6.

244 Beales et. al., *supra* note 140, at 531 ("Consumer education is often overlooked as a means of dealing with incomplete information.").

245 Nancy Willard, *Comprehensive Layered Approach to Address Digital Citizenship and Youth Risk Online*, CTR. FOR SAFE & RESPONSIBLE INTERNET USE, 1 (Nov. 2008), http://internet-safety-issues.wikispaces.com/file/view/yrocomprehensiveapproach.pdf; Anne Collier, *From Users to Citizens:*

steps also encourage greater personal responsibility by incentivizing users to be more vigilant about protecting their own privacy.[246] As Professor Fred Cate has observed, "Individual responsibility, not regulation, is the principal and most effective form of privacy protection in most settings."[247]

Many privacy activists and privacy professionals already offer extensive educational programs and advice.[248] Elsewhere I have summarized in much greater detail how such educational and awareness-building efforts offer a constructive alternative to administrative regulation, whether for online safety[249] or privacy.[250] When conducting BCA for online safety or privacy-related rules, these educational efforts must be taken into account before rules are imposed.

Importantly, a focus on education and awareness-based alternatives does not mean governments have no role to play. To the contrary, governments at all levels—federal, state, and local—can work together and with third parties to develop privacy messaging. In its *Strategic Plan*, the FTC notes that "Consumer and business education serves as the first line of defense against fraud, deception, and unfair practices."[251] The FTC already partners with several other federal agencies to offer OnGuardOnline, a site that offers wide-ranging security, safety, and privacy tips for consumers and businesses. As part of that effort, the FTC produces dozens of informational

---

How to Make Digital Citizenship Relevant, NET FAMILY NEWS (Nov. 16, 2009), http://www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html; Larry Magid, *We Need to Rethink Online Safety*, HUFFINGTON POST (Jan. 22, 2010, 4:19 PM), www.huffingtonpost.com/larry-magid/we-need-to-rethink-online_b_433421.html.

246 SMITH & MACDERMOTT, *supra* note 80, at 43 ("[W]ith liberty for all comes the necessity for discipline of the self. Put another way, the greater the freedom, the greater the need for a disciplined approach to that freedom. No technology in the history of civilization has demanded a greater degree of self-regulation than the Internet."); Tom W. Bell, *Free Speech, Strict Scrutiny, and Self-Help: How Technology Upgrades Constitutional Jurisprudence*, 87 MINN. L. REV. 743, 743-44 (2003) ("The state ought not to help those who can better help themselves.").

247 FRED H. CATE, PRIVACY IN THE INFORMATION AGE 131 (1997).

248 David Hoffman, *What's One Way Organizations Can Be More Accountable? Educate! Educate! Educate!*, INT'L ASS'N PRIVACY PROF'LS BLOG (Apr. 2, 2013), https://www.privacyassociation.org/privacy_perspectives/post/whats_one_way_organizations_can_be_more_accountable_educate_educate_educate.

249 Thierer, *supra* note 146.

250 Thierer, *supra* note 79, at 437-40.

251 FED. TRADE COMM'N, STRATEGIC PLAN FOR FISCAL YEARS 2009 TO 2014, at 4 (2009), *available at* http://www.ftc.gov/opp/gpra/spfy09fy14.pdf ("Most FTC law enforcement initiatives include a consumer and/or business education component aimed at preventing consumer injury and unlawful business practices, and mitigating financial losses. From time to time, the agency conducts pre-emptive consumer and business education campaigns to raise awareness of new or emerging marketplace issues that have the potential to cause harm. The agency creatively uses new technologies and private and public partnerships to reach new and under-served audiences, particularly those who may not seek information directly from the FTC.").

videos that are also available on a dedicated YouTube page.[252] Similarly, the FCC offers smartphone security advice on its website.[253] State and local officials can also take steps to integrate privacy and security lessons and messaging into school curricula. Of course, the most important form of education—for online safety and privacy alike—comes from the home through mentoring by parents and guardians.[254]

B. *Transparency/Disclosure Solutions*

As noted in Section II.D, transparency and disclosure mandates also offer governments an alternative to more restrictive forms of administrative regulation.[255] Transparency-related requirements are less costly for industries, consumers, and government alike and also facilitate improved information-sharing about commercial practices important to consumers.[256]

In the context of broadband policy, for example, the FCC has gradually moved away from restrictive regulatory schemes for broadband markets and instead pushed for improved transparency about broadband practices and speeds.[257] Starting in August 2011, the agency began surveying residential broadband speeds "to improve the availability of information for consumers about their broadband service."[258] As part of those reports, the agen-

---

252 *Federal Trade Commission*, YOUTUBE, http://www.youtube.com/user/FTCvideos (last visited June 23, 2013).

253 *FCC Smartphone Security Checker*, FED. COMMC'NS COMM'N, http://www.fcc.gov/security (last visited June 23, 2013).

254 Press Release, Car Ins. iNet, GPS Car Devices for Teenage Drivers Reports Car Insurance iNet (Jan. 6, 2013), *available at* http://www.emailwire.com/release/110791-GPS-Car-Devices-For-Teenage-Drivers-reports-Car-Insurance-iNet.html (quoting Woodrow Hartzog, assistant professor of law at Cumberland School of Law at Samford University in Birmingham, Alabama, as saying, "I tend to draw comparisons between the parental use of monitoring technology for driving with the parental monitoring of their children's use of social networking. . . Young adults are notoriously protective of their privacy. I think the best way to approach the situation is to have a conversation with them if you want to use the technology. It would set a dangerous precedent to employ this technology without letting the children know.").

255 *See supra* Section II.D.

256 Thomas H. Davenport, Counterpoint, *No: Stronger Privacy Rules Could Squelch Innovation, in Should the U.S. Adopt European-Style Data-Privacy Protections?*, WALL ST. J. (Mar. 8, 2013, 1:36 PM), http://online.wsj.com/article/SB10001424127887324338604578328393797127094.html ("For a market-based approach to privacy to work, however, companies must be transparent and consistent. They have to inform their customers what they plan to do with their data, and whether they will pass it along to other organizations—and no, they can't change the policy after collecting personal information.").

257 *Measuring Broadband America*, FED. COMMC'NS COMM'N, http://www.fcc.gov/measuring-broadband-america (last visited June 23, 2013) (listing three annual FCC broadband surveys).

258 *Id.*

cy also reviewed the openness and transparency practices of carriers.[259] These reports have not only helped make consumers more aware of broadband service speeds and policies, but also encouraged carriers to compete on speed and boast of their superior service in advertisements and press reports.[260]

The FTC also utilizes transparency reports to monitor industry developments and better inform consumers. Since 2000, the FTC has surveyed the marketing and advertising practices of major media sectors (movies, music and video games) in a report entitled *Marketing Violent Entertainment to Children*.[261] The agency hires a research firm that conducts "secret shopper" surveys to determine how well voluntary media rating systems—for movies, music, and video games—are being enforced at the point of sale. The research firm then recruits 13- to 16-year-olds who attempt to purchase such media without a parent being present.

Using these surveys, the FTC has been able to keep pressure on those sectors to constantly improve their voluntary rating systems. The FTC reports have shown that ratings enforcement has generally been improving over time, and in the case of the video game industry's ESRB system, it has improved dramatically.[262] For example, the 2013 survey found that whereas 85 percent of minors were able to purchase an M-rated video game in 2000, only 13 percent of them were able to do so in 2008.[263]

Such transparency-related measures constitute a less restrictive alternative to administrative regulation of media and communications providers and "allow consumers to protect themselves according to personal preferences rather than place on regulators the difficult task of compromising diverse preferences with a common standard."[264] In a similar way, the FTC and other policymakers could adopt more transparency-oriented techniques to hold industry more accountable to the privacy and data security-related

---

259 *Measuring Broadband America Policy on Openness and Transparency*, FED. COMMC'NS COMM'N, http://www.fcc.gov/measuring-broadband-america/openness-transparency-policy (last visited June 23, 2013).

260 Steve Donohue, *Verizon Expands Lead over Cablevision in FCC Measuring Broadband America Report*, FIERCECABLE (Feb. 15, 2013), http://www.fiercecable.com/story/verizon-expands-lead-over-cablevision-fcc-measuring-broadband-america-repor/2013-02-15.

261 FED. TRADE COMM'N, MARKETING VIOLENT ENTERTAINMENT TO CHILDREN: A REVIEW OF SELF-REGULATION AND INDUSTRY PRACTICES IN THE MOTION PICTURE, MUSIC RECORDING & ELECTRONIC GAME INDUSTRIES (2000), *available at* http://www.ftc.gov/reports/violence/vioreport.pdf. Subsequent versions of this report can be found at http://www.ftc.gov/reports/index.shtm.

262 Press Release, Fed. Trade Comm'n, FTC Undercover Shopper Survey on Entertainment Ratings Enforcement Finds Compliance Highest Among Video Game Sellers and Movie Theaters (Mar. 25, 2013), http://www.ftc.gov/opa/2013/03/mysteryshop.shtm.

263 *Id.*

264 Beales et al., *supra* note 140, at 513.

promises they make to consumers.[265] Importantly, however, excessive mandatory disclosure requirements "may add to the problem of information overload" as "consumers may find plowing through legalese more tedious and worthless than ever."[266]

C. *User Empowerment and Self-Help Solutions*

The market for privacy enhancing technologies and digital "self-help" tools continues to expand rapidly.[267] These tools can help users block or limit various types of advertising and data collection and also ensure a more anonymous browsing experience.

Elsewhere I have provided a more thorough inventory of the privacy enhancing technologies and consumer information already available on the market today.[268] The major type of privacy enhancing technologies include: ad preference managers,[269] "private browsing" tools,[270] advertising blocking technologies, cookie-blockers, web script blockers, Do Not Track tools,[271] and reputation protection services.[272] Apple's "Safari" web browser already blocks third-party cookies and Mozilla's "Firefox" browser is set to do so in a future release.[273] Encryption and proxy tools, which offer the most robust

---

265 Beales & Muris, *supra* note 8, at 132-33 ("Each security breach should teach lessons about potential vulnerabilities. Some of those lessons have been taught before, and companies that have not paid attention can, and should, be held accountable.").

266 Robert A. Hillman, *Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?*, 104 MICH. L. REV. 837, 850 (2006).

267 *See* Tom W. Bell, *Pornography, Privacy, and Digital Self Help*, 19 J. MARSHALL J. COMPUTER & INFO. L. 133, 139 (2000).

268 Thierer, *supra* note 79, at 440-46.

269 All major online search and advertising providers (Google, Facebook, Yahoo!, etc.) offer ad preference managers to help users manage their advertising preferences. *See, e.g.*, *Ad Settings*, GOOGLE, https://www.google.com/settings/ads/plugin (last visited June 23, 2013).

270 Major browser providers also offer variations on "private browsing" mode, which allows users to turn on a stealth browsing mode to avoid data collection and other forms of tracking. *See, e.g.*, Gregg Keizer, *Mozilla Refines Firefox's Private Browsing, Patches 13 Browser Bugs*, COMPUTERWORLD (Apr. 3, 2013, 6:31 AM), http://www.computerworld.com/s/article/9238086/Mozilla_refines_Firefox_s_private_browsing patches_13_browser_bugs.

271 All three of those browser makers (Microsoft, Google, and Mozilla) 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. *See, e.g.*, Emil Protalinski, *Everything You Need to Know About Do Not Track: Microsoft vs. Google & Mozilla*, THE NEXT WEB (Nov. 25, 2012, 4:56 AM), http://thenextweb.com/apps/2012/11/25/everything-you-need-to-know-about-do-not-track-currently-featuring-microsoft-vs-google-and-mozilla/.

272 Dennis O'Reilly, *Privacy Check, Part Three: Online Reputation Services*, CNET NEWS (Jan. 24, 2011, 11:03 AM), http://news.cnet.com/8301-13880_3-20029211-68.html.

273 Megan Geuss, *Firefox Will Block Third-Party Cookies in a Future Version*, ARS TECHNICA (Feb. 23, 2013, 10:00 PM), http://arstechnica.com/business/2013/02/firefox-22-will-block-third-party-cookies.

level of online privacy possible, continue to grow more powerful and accessible as well.[274]

A wide variety of digital security tools—anti-virus and other anti-malware technologies, for example—also exist today. Such security tools can help protect a user's privacy by guarding information they wish to keep private. Importantly, there are many other mundane steps that users can take to protect their privacy, such as using strong passwords and multifactor authentication techniques for digital devices and online accounts (especially e-mail and digital hosting services), frequently clearing web browser history and cookies to eliminate digital tracking, and deleting unused or redundant accounts when possible.[275] Another simple step users can take is to configure a second web browser for occasional anonymous surfing by adjusting all its settings to tightly limit all data collection.[276]

The existence of such a diverse array of privacy-enhancing tools and strategies should call into question any accusation that a state of "market failure" exists in this arena. Indeed, it may be the case that privacy-sensitive users already have all the tools at their disposal needed to adequately secure their online data and privacy but simply are not aware of all of them. The availability of privacy tools may be one reason that the FTC and officials in the Obama administration have not yet made a serious effort to define how a state of market failure might exist, rendering the regulation necessary.[277]

Importantly, although a great diversity of online safety and privacy empowerment tools exists today, it is also clear that most consumers do not take advantage of those tools.[278] "A lot of companies have started with idealism about empowering the online user, only to find that the user wouldn't pay," notes technology investor Esther Dyson.[279]

However, the relative unpopularity of various privacy tools cannot be used as a determination of market failure or of the need for government regulation. Nor should the effort or inconvenience associated with using

---

274 *See* Ryan Gallagher, *The Threat of Silence*, SLATE (Feb. 4, 2013, 12:21 PM), http://www.slate.com/articles/technology/future_tense/2013/02/silent_circle_s_latest_app_democratizes_encryption_governments_won_t_be.single.html.

275 *See, e.g.*, Kashmir Hill, *10 Incredibly Simple Things You Should Be Doing to Protect Your Privacy*, FORBES (Aug. 23, 2012, 8:01 AM), http://www.forbes.com/sites/kashmirhill/2012/08/23/10-incredibly-simple-things-you-should-be-doing-to-protect-your-privacy.

276 Brad Chacos, *How (and Why) to Surf the Web in Secret*, PC WORLD (Nov. 7, 2012, 3:30 AM), http://www.pcworld.com/article/2013534/how-and-why-to-surf-the-web-in-secret.html.

277 Lenard & Rubin, *supra* note 67, at 2 ("The Commission and Staff Reports do not provide a rigorous analysis of whether market failures exist with respect to privacy.").

278 Adam Thierer, *Who Needs Parental Controls? Assessing the Relevant Market for Parental Control Technologies*, PROGRESS & FREEDOM FOUND., 1 (Feb. 2009), http://www.pff.org/issues-pubs/pops/2009/pop16.5parentalcontrolsmarket.pdf.

279 *The Price of Reputation*, ECONOMIST, Feb. 23, 2013, at 64-65, *available at* http://www.economist.com/news/business/21572240-market-protected-personal-information-about-take-price-reputation (quoting Dyson) (internal quotation marks omitted).

such tools be used as a determination of market failure. 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.

This principle is already the standard that the US Supreme Court has adopted in relation to child protection tools. In *United States v. Playboy Entertainment Group, Inc.*,[280] the Court struck down a law requiring cable companies to "fully scramble" video signals transmitted over their networks if those signals included any sexually explicit content.[281] Echoing its earlier holding in *Reno v. ACLU*,[282] the Court found that less restrictive means were available to parents looking to block those signals in the home.[283] Specifically, in the *Playboy* case, the Court argued that "targeted blocking is less restrictive than banning, and the Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests."[284]

More importantly, the Court held:

> 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.[285]

This holding means that the Supreme Court has largely foreclosed efforts to apply top-down, administrative regulations when less restrictive means are available to citizens to address their online safety concerns. This same standard can be applied to privacy-related matters when conducting BCA. If effective privacy-enhancing tools and options exist, they must be factored into the BCA process. The existence of such empowerment tools should weigh heavily against the use of preemptive regulation, especially in the absence of more concrete harms.

Of course, as already noted, many other government efforts are still possible, including user education and empowerment efforts. Government officials can take steps to encourage the use of such tools and methods, such as developing their own websites, online tools, and even privacy-enhancing applications in order to further empower citizens. Such methods would certainly be less restrictive and likely far less costly than top-down regulation of information-gathering and sharing practices.

---

280 529 U.S. 803 (2000).

281 *Id.* at 807.

282 521 U.S. 844 (1997).

283 *Playboy*, 529 U.S. at 807.

284 *Id.* at 815.

285 *Id.* at 824.

D. *Self-Regulation and Codes of Conduct*

Industry self-regulation, best practices, codes of conduct, and informational efforts are also alternatives to administrative regulation that should be considered when conducting BCA for privacy-related proposals.[286]

Self-regulation is already at work in the privacy arena. In 2009, the Digital Advertising Alliance, a collaboration of the leading trade associations, created the "Self-Regulatory Program for Online Behavioral Advertising."[287] The program utilizes an "Advertising Option Icon" to highlight a company's use of targeted advertising and also enables users to opt out of those ads.[288]

The effort includes an educational initiative, www.aboutads.info, which offers consumers additional information about online advertising.[289] The program "has participation from more than 90 percent of the interactive ad business" and "was even recognized by the FTC as a good example of public and private partnership."[290] The primary participants are the 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.[291] These self-regulatory efforts represent a cost-effective and flexible way of addressing privacy concerns when compared to top-down regulatory mandates, which can be more costly and inflexible in character.[292]

E. *Alternative Enforcement Mechanisms*

Before new administrative rules are imposed, alternative legal enforcement mechanisms should also be considered. OMB Circular A-4 spec-

---

286 *See* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y INFO. SOC'Y 355, 368-74 (2011) (surveying self-regulatory systems and applying them to privacy policy).

287 *Self-Regulatory Program for Online Behavioral Advertising*, DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info (last visited June 23, 2013).

288 *Id.*

289 *Self-Regulatory Principles*, DIGITAL ADVERTISING ALLIANCE, http://www.aboutads./principles (last visited June 23, 2013).

290 Bachman, *supra* note 63.

291 Press Release, Am. Ass'n of Adver. Agencies et al., 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), *available at* http://www.networkadvertising.org//Associations104release.pdf.

292 Catherine Schmierer, Comment, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, RICH. J.L. & TECH., Spring 2011, art. no. 13 ¶ 76, at 56 (2011), http://jolt.richmond.edu/v17i4/article13.pdf.

ifies that "Even where a market failure clearly exists, [agencies] should consider other means of dealing with the failure before turning to Federal regulation."[293] Among those alternatives: antitrust enforcement, consumer-initiated litigation in the product liability system, state or local action, flexible standards or performance metrics, and informational measures.[294] It may also be the case that increased reliance on contracts, property rights, torts, class action suits,[295] antifraud statutes, and anti-harassment standards can help alleviate privacy problems.

Finally, as noted in Part II,[296] the FTC already possesses a remarkably powerful remedy for alleged violations of data security standards: its Section 5 authority to police "unfair and deceptive practices." Professors Kenneth A. Bamberger and Deirdre K. Mulligan note:

> [S]ince 1996 the FTC has actively used its broad authority under section 5 . . . 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.[297]

As recent privacy-related enforcement actions against both Google[298] and Facebook[299] illustrate, the FTC already has broad discretion and plenary authority to hold companies to the promises they make to their users as it pertains to information collection and data security.[300] In consent decrees with both those companies, the FTC extracted a wide variety of changes to their privacy and data collection practices while also demanding that they undergo privacy audits for the next twenty years.[301]

---

293 OMB, CIRCULAR A-4, *supra* note 33, at 6.

294 *Id.* at 7-9.

295 *See, e.g.*, Selina Koonar, *Growing Concerns over Online Privacy Lead to Class Action Lawsuits Against Instagram, Facebook and Google*, LEXOLOGY (Mar. 7, 2013), http://www.lexology.com/library/.aspx?g=fe2ba92b-d8ff-439e-a6b9-836e32090520.

296 *See supra* Part II.

297 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273 (2011).

298 Alex Howard, *Google Reaches Agreement with FTC on Buzz Privacy Concerns*, GOVFRESH (Mar. 30, 2011, 11:38 AM), http://gov20.govfresh.com/google-reaches-agreement-with-ftc-on-buzz-privacy-concerns.

299 Brent Kendall, *Facebook Reaches Settlement with FTC on Privacy Issues*, WALL ST. J. (Nov. 29, 2011, 1:29 PM), http://online.wsj.com/article/BT-CO-20111129-710865.html.

300 Berin Szoka, *FTC Enforcement of Corporate Promises & the Path of Privacy Law*, TECH. LIBERATION FRONT (July 13, 2010), http://techliberation.com/2010/07/13/ftc-enforcement-of-corporate-promises-the-path-of-privacy-law.

301 Matthew Sundquist, *Online Privacy Protection: Protecting Privacy, the Social Contract, and the Rule of Law in the Virtual World*, 25 REGENT U. L. REV. 153, 173-75 (2012); Kashmir Hill, *So, What Are These Privacy Audits that Google and Facebook Have to Do for the Next 20 Years?*, FORBES (Nov. 30, 2011, 2:29 PM), http://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years.

F. *Contracting Opportunities*

The hope for better methods of contracting around privacy has long pervaded the literature in this field.[302] But for a variety of reasons, privacy markets have never taken off. One explanation, already discussed above, is that there simply isn't much demand for it. Under the prevailing "take-it-or-leave-it" model of online services, users are given the option to accept the licensed terms of service a site or service provider offers or choose another provider.[303] Many gladly accept such licensing deals, however, because of the low price (usually zero) and the availability of many other service options.[304]

Another explanation is that formal contracting around privacy has always been tied up with the same thorny issues of information ownership and enforcement which have complicated digital copyright policy.[305] Put simply, information control is hard—whether such control is being pursued through top-down regulation or bottom-up contracting methods.[306] Creating the equivalent of property rights in personal information may, therefore, be cumbersome and costly.[307]

---

302 *See, e.g.*, Varian, *supra* note 133, at 104 ("[A]ssign a property rights [sic] in information about an individual to that individual, but then allow contracts to be written that would allow that information to be used for limited times and specified purposes."); A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1505 (2000) ("Perhaps the most promising avenue is to design contracts and technologies that . . . seek to lower the transaction costs of modifying standard form contracts, or of specifying restrictions on reuse of disclosed data."); Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, COLUM. INST. FOR TELE-INFO., http://www.citi.columbia.edu/elinoam//priv_self.htm ("Encryption permits individuals to sell information about themselves directly, instead of letting various market researchers and credit checkers snoop in their demographics, personal history, and garbage cans.").

303 Anita Ramasastry, *Instagram's Terms of Service Revision: Why It Strained the Bounds of Fair Contracting*, VERDICT (Dec. 21, 2012), http://verdict.justia.com/2012/12/21/instagrams-terms-of-service-revision.

304 Berger, *supra* note 10, at 60 ("It is likely too late to suggest that consumers actually do *own* their information, and that we should, therefore, analyze the rights of profilers based on a concept of a license to use the data." (footnote omitted)); Downes, *supra* note 72, at 26 ("Licensing is the perfect model for information transactions, and it has already been used successfully for many different kinds of information products and services.").

305 Hahn & Layne-Farrar, *supra* note 68, at 17 ("There are several practical limitations to the tradable rights theory. These include enforcement of property rights, constitutional issues, and valuation issues."); Kapushion, *supra* note 161, at 1487 (noting that privacy is "intangible, nontransferable, and possesses few, if any, of the characteristics we would traditionally ascribe to property").

306 *Kapushion*, *supra* note 161, at 1489 ("There is a problem, however, in that catering to individual preferences can become very costly, very quickly. While it is conceivable that an individual could contract with every covered entity they come into contact with, the costs could mushroom as providers scrambled to accommodate a variety of needs, and regulatory oversight is replaced by extensive contract enforcement.").

307 *See, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1285-86 (2000) ("Some people adopt silly but vaguely reassuring tactics . . . . Nonetheless, these tactics

The aversion to contracting may be changing, however. Firms such as Reputation.com, Personal.com, and ID3 hope to create "data lockers" or "reputational vaults" that would let consumers keep their personal information in a secure system for a fee and then trade it with others more selectively than they do today.[308] "These ventures each take different approaches toward protecting personal information but are all focused, at their core, on enabling people to better control and leverage data about themselves and their lives," notes technology writer David Bollier.[309]

G. *Societal Adaptation and Evolving Cultural Norms*

Another factor complicating the benefit side of BCA for both online safety and privacy regulation is the rapid evolution of cultural norms with regard to new media content and communications services. 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.[310]

A cycle of initial *resistance*, gradual *adaptation*, and then eventual *assimilation* is well established in the context of popular entertainment.[311] For example, the emergence of dime novels, comic books, movies, rock-and-roll music, video games, and social networking services all led to "moral

---

seem to undermine the reliability of the data, just a little, making this game a little more expensive, and offering a thin but ultimately unpersuasive illusion of control."); Posner, *supra* note 73, at 397 ("The attractiveness of this [property rights] solution depends, however, on (1) the nature and provenance of the information and (2) transaction costs."); Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CALIF. L. REV. 751, 758 (1999) (reviewing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996) and PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998)) ("This [regulation of personal data] produces a market failure that is deepened by the seemingly intractable difficulties in successfully bargaining for the appropriate level of privacy."); Downes, *supra* note 72, at 17-26.

308 DAVID BOLLIER, POWER-CURVE SOCIETY: THE FUTURE OF INNOVATION, OPPORTUNITY AND SOCIAL EQUITY IN THE EMERGING NETWORKED ECONOMY 10-11 (2013), *available at* http://www.aspeninstitute.org/sites/default/files/content/upload/Power-Curve-Society.pdf; *see also The Price of Reputation*, ECONOMIST (Feb. 23, 2013), http://www.economist.com/news/business/21572240-market-protected-personal-information-about-take-price-reputation.

309 BOLLIER, *supra* note 308, at 10.

310 Doug Aamoth, *A Bunch of Tech Things People Have Threatened to Quit Recently*, TIME (Dec. 18, 2012), http://techland.time.com/2012/12/18/a-bunch-of-tech-things-people-have-threatened-to-quit-recently (noting several types of media content and platforms that, despite protestations that users will quit, continue to be very popular).

311 Adam Thierer, Op-Ed., *Why Do We Always Sell the Next Generation Short?*, FORBES (Jan. 8, 2012, 4:14 PM), http://www.forbes.com/sites/adamthierer/2012/01/08/why-do-we-always-sell-the-next-generation-short ("[M]any historians, psychologists, sociologists, and other scholars have documented this seemingly never-ending cycle of generational clashes . . . .").

panics"[312] or "technopanics."[313] Over time, however, society generally came to accept and then even embrace these new forms of media or communications technologies.[314]

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."[315] 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, "The Right to Privacy."[316] 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."[317] 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.'"[318]

The article's observation probably reflected the initial reaction—even revulsion—that many citizens felt toward this new technology.[319] 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 regu-

---

312 Robert Corn-Revere, *Moral Panics, the First Amendment, and the Limits of Social Science*, COMM. LAW., Nov. 2011, at 4, 4-5.

313 Thierer, *supra* note 1, at 311.

314 *Id.* at 364-68.

315 Downes, *supra* note 72, at 10.

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

317 *Id.* at 196.

318 *Id.* at 195.

319 Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1301 (2010) ("[T]he 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." (footnote omitted)).

lated.[320] A bill was floated in California that would have banned the service.[321] Some privacy advocates worried that Google's contextually targeted advertisements, which were based on keywords that appeared in e-mail messages, were tantamount to reading users' e-mail and constituted a massive privacy violation.[322] Users quickly adapted their privacy expectations to accommodate this new service, however, and the service grew rapidly.[323] By the summer of 2012, Google was announcing that 425 million people were actively using Gmail.[324]

Sometimes, however, companies push too aggressively against established privacy norms, 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 which would have allowed it to more easily share user information and even their photographs with Facebook and advertisers.[325] Within hours of announcing the changes, Instagram found itself embroiled in a consumer and media firestorm.[326] The uproar also "helped a number of [competing] photo-sharing applications garner unprecedented amounts of traffic and new users."[327] One rival called EyeEm reported that daily sign-ups had increased a thousand percent by the morning after the Instagram announcement.[328] According to some estimates, Instagram "may have shed nearly a quarter of its daily active users in the wake of the debacle."[329]

Instagram's experience serves as an example of how consumers often "vote with their feet" and respond to privacy violations by moving to other

---

320 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.

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

322 *See* Letter from Chris Jay Hoofnagle, Assoc. Dir., Elec. Privacy Info. Ctr., et al. to Bill Lockyer, Attorney Gen., Cal. (May 3, 2004), *available at* http://epic.org/privacy/gmail/agltr5.3.04.html.

323 Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 984-85 (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").

324 Dante D'Orazio, *Gmail Now Has 425 Million Active Users*, THE VERGE (June 28, 2012, 1:26 PM), http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users.

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

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

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

328 *Id.*

329 Garett Sloane, *Rage Against Rules*, N.Y. POST (Dec. 29, 2012, 12:24 AM) http://www.nypost.com/p/news/business/rage_against_Dh05rPifiXBIJRE1rCOyML.

services, or at least threatening to do so unless changes are made by the offending company.[330] Just three days after announcing those changes, Instagram relented and revised its privacy policy.[331] In an apology posted on its corporate blog, Instagram co-founder Kevin Systrom said, "[W]e respect that your photos are your photos. Period."[332] Despite the rapid reversal, a class action lawsuit was filed less than a week later.[333] Although experts agreed the lawsuit was unlikely to succeed, such legal threats can have a profound impact on current and future corporate behavior.[334]

Episodes such as these should have a bearing on BCA for privacy matters. Time and time again, humans have proven to be resilient in the face of rapid technological change by utilizing a variety of adaptation and coping mechanisms to gradually assimilate new technologies and business practices into their lives.[335] Other times they push back against firms disrupting established privacy norms and encourage companies to take a more gradual approach to technological change.

CONCLUSION

Controversial value judgments often complicate benefit-cost analysis. Nowhere is this more evident than in debates over privacy and online safety policy, which are encumbered by emotional appeals to highly subjective values and asserted (intangible and non-economic) harms. Consequently, quantifying the benefits of proposed rules often gets bogged down in a hopeless philosophical tangle. The cost side of the equation can, however, offer greater insights into potential economic trade-offs in terms of forgone opportunities (such as free online sites, services, apps, and content). But weighing those costs alongside asserted benefits that are so radically subjective in character will continue to be controversial.

---

330 Downes, *supra* note 72, at 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 co-opted for use in such campaigns, consumers have proven increasingly able to leverage and enforce their preferences.").

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

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

333 Zach Epstein, *Instagram Slapped with Class Action Lawsuit over Terms of Service Fiasco*, BGR.COM (Dec. 25, 2012, 11:35 AM), http://bgr.com/2012/12/25/instagram-slapped-with-class-action-lawsuit-over-terms-of-service-fiasco-267480/.

334 Jeff John Roberts, *Instagram Privacy Lawsuit is Nonsense Say Experts*, GIGAOM (Dec. 26, 2012, 7:57 AM), http://gigaom.com/2012/12/26/instagram-privacy-lawsuit-is-nonsense-say-experts.

335 Thierer, *supra* note 1, at 359.

It is only when we turn to the analysis of regulatory alternatives that we find a way out of this quandary. Luckily, a diverse array of education- and empowerment-based solutions exist that can help individuals enhance their online safety and privacy. To the extent anxieties about these issues discourage some people from utilizing certain online services, remedies centered on education and empowerment are preferable to prescriptive regulation. This "educate and empower" approach is particularly wise for Internet policy concerns, since it can adapt more rapidly and flexibly than administrative regulation.[336]

Policymakers must also take into account the strong likelihood that citizens, as in the past, will adjust their privacy expectations in response to ongoing marketplace and technological change. They must also understand that not everyone shares the same sensitivities or values[337] and therefore that "one-size-fits-all" policy solutions are misguided.[338]

If, however, additional regulatory actions are pursued, it remains vital that policymakers conduct a careful analysis of the potential benefits and costs of regulation to ensure that the opportunity costs of governmental action are better understood. It is not enough to simply invoke the importance of values like "privacy" and "safety" without thinking through the consequences of regulations aimed at preserving or enhancing them, especially when "there are less expensive or burdensome ways of accomplishing the same end."[339]

---

336 Goldman, *supra* note 321, at 1158 ("Technology and business practices evolve, exposing deficiencies in the regulatory framework. Regulators correct these deficiencies with targeted amendments that become outdated with continued advances in technology and business practices, and the cycle continues indefinitely. This regulatory cycle is predictably (and almost comically) futile because it is not possible to craft rigorous statutory definitions of communication media.").

337 SMITH & MACDERMOTT, *supra* note 80, at 110 ("[P]rivacy is by commonsense definition private; therefore, control of privacy should be a product of individual decision making. Privacy is not just a word or an abstract concept; rather, it is the product of a series of decisions and the actions and consequences that flow from them.").

338 *Id.* at 111. ("[I]ndividuals are in the best position to make decisions about commercial demands on their privacy . . . . It relieves government of the Sisyphean labor of attempting to impose one-size-fits-all regulation on millions of individuals in billions of cases.").

339 Fred H. Cate, *Principles for Protecting Privacy*, 22 CATO J. 33, 35 (2002) ("[T]he breadth and malleability of the term 'privacy' has had a remarkable effect on the political debate over the role of law in protecting it. Because 'privacy' can mean almost anything to anybody, and because the term carries such emotional weight . . . legislators can generate broad support for so-called privacy laws just by invoking the word. Yet without any specificity as to what privacy interest a proposed law or regulation is intended to serve, neither legislators nor the public can determine whether a need exists, whether the law in fact meets that need, and whether there are less expensive or burdensome ways of accomplishing the same end.").