THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

May 27, 2016

Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

RE: Docket No. 16-106, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

Dear Chairman Wheeler:

I am J. Howard Beales III, Professor of Strategic Management and Public Policy at the George Washington School of Business.[1] This comment is a public interest comment, submitted through the George Washington University Regulatory Studies Center.[2] The Center improves regulatory policy through research, education, and outreach. As part of its mission, the Center conducts careful and independent analyses to assess rulemaking proposals from the perspective of the public interest. This comment does not represent the views of any particular affected party or special interest, but is designed to evaluate the effect of the FCC's proposal on overall consumer welfare.

The FCC has proposed detailed rules governing privacy practices of broadband Internet access service ("BIAS") providers. The rule would establish new, and different, privacy standards, beyond those that apply to other Internet companies ("edge" providers such as Facebook or ESPN that offer content). It would regulate privacy practices for Customer proprietary network

[1] I have an extensive career in government service, most recently as Director of the Bureau of Consumer Protection at the Federal Trade Commission from 2001-2004. During my tenure, the Commission promulgated and implemented the National Do Not Call Registry. I have published extensively on privacy and consumer protection regulation.

[2] This comment reflects the views of the author, and does not represent an official position of the GW Regulatory Studies Center or the George Washington University. The Center's policy on research integrity is available at http://regulatorystudies.columbian.gwu.edu/policy-research-integrity.

information (CPNI) (such as service plan information, geo-location, MAC addresses, and source and destination IP addresses) and customer proprietary information (CPI) (CPNI plus personally identifiable information acquired in connection with provision of BIAS). Providers would have to disclose the types of CPI they collect, how they use and when they disclose this information, the categories of entities to whom it is disclosed and purposes for which those entities use the information. Providers could use CPI without consent when necessary for providing services. The rule would require "opt out" consent for marketing communications related services to their customers, and "opt in" consent for all other uses of CPI. Thus, BIAS providers would have to obtain "opt in" consent for many uses of information for which other Internet companies either offer no choice or offer an "opt out" choice. The rule includes specific requirements for notifications in the event of a data breach, and imposes information security standards. It would prohibit certain practices, such as conditioning services on waiver of privacy rights or offering financial incentives for such waivers.

At present, BIAS providers are subject to the same privacy standards and requirements as every other company involved in the Internet economy, enforced by the Federal Trade Commission. Companies post privacy policies identifying the information they collect, how they use it, how they share information and with whom, and offering consumers a degree of choice about certain uses of certain information. For most information, most companies offer consumers the ability to "opt out" of some uses; a few require "opt in" consent to uses of sensitive information. Practices inconsistent with those privacy promises are deceptive practices, subject to enforcement actions by the FTC. In addition, the FTC has held that inadequate data security practices can constitute unfair practices, subject to enforcement actions even if there are no specific security promises.

The FTC's approach to privacy regulation has worked well. Importantly, it applies a uniform regulatory approach to different technologies and different business models. It has largely avoided creating artificial barriers to either competition or innovation. The FTC has brought numerous enforcement actions involving privacy and data security, but none have involved the provision of broadband Internet services.[3]

The FCC offers *no* evidence of *any* inadequacies in this privacy regime. It notes that all of the largest broadband providers already have publicly available privacy policies, but it makes *no* substantive case at all as to why those policies are inadequate. It identifies no adverse consequences to consumers that have resulted from broadband provider privacy practices. It identifies no privacy problems that have resulted from either accidental or deliberate sharing of

[3] In Level 3 Communications LLC, the Commission challenged claims that an Internet service provider was a "current" participant in the U.S.-EU Safe Harbor program, when in fact its self-certification of compliance had lapsed. The complaint alleges no substantive violations. Level 3 Communications LLC, File No. 142 3028 (June 25, 2014), available at https://www.ftc.gov/enforcement/cases-proceedings/142-3028/level-3-communications-llc-matter.

information by broadband provides. It asserts there is a "gap" between traditional privacy practices that "must be closed," but the only apparent "gaps" are the absence of a detailed and burdensome regulation, and the gap in legal authority created by the FCC's reclassification of broadband services. Rather than establishing a problem in need of a solution as the predicate for regulation, the rationale for the rule is succinctly stated in paragraph 7 of the notice: "the Commission is empowered to protect the private information," and therefore it will, whether that information needs protection or not. Instead, the FCC should forbear from creating a new regulatory framework for privacy practices, and defer to the successful FTC regime.

Data collection and analysis play an essential role in the modern economy. The commercial use of information contributes to reducing the incidence of credit card fraud, democratizing the availability of consumer credit, and creating fraud detection tools to reduce the risk of identity theft.[4] It is essential not only for the basic functioning of the Internet, but also in creating value for consumers by supporting advertising, which underwrites the cost of content and services, tailoring both commercial and non-commercial information to meet consumers' specific preferences, and facilitating innovation by new and existing suppliers. Consumer data and feedback also enables the increased customization and personalization of online experiences and offerings for consumers, which is helping to fuel growth in broadband usage and e-commerce. The Commission should not risk undermining these numerous benefits without clear evidence of a problem that needs to be solved.

This comment argues first that the FCC's rationales for treating BIAS providers differently are flawed. Broadband providers do not pose a unique or more comprehensive privacy risk than other participants in the Internet ecosystem, they are unlikely to engage in harmful conduct, and they are not protected by uniquely high costs of switching that might justify different treatment. Second, the proposed separate regulatory regime for broadband providers would inhibit innovation, reduce competition, and harm consumers. Third, if it feels it must regulate, the FCC should adopt a functionality based approach to privacy regulation to maximize consumer welfare.

I. BIAS Providers Do Not Pose Unique Threats to Privacy

A. Concerns about "comprehensiveness" of data collection do not justify a separate regulatory regime

As a starting point, it is crucial for the Commission to consider what problems it is seeking to prevent by imposing unique burdens on a sector of the Internet economy that it fears has greater

[4] For an extended discussion, see e.g., J. Howard Beales, III and Timothy J. Muris, "Choice or Consequences: Protecting Privacy in Commercial Information," *University of Chicago Law Review* 75 (2008) 109-135, especially at 115-117.

access to consumer information. The answer cannot be that targeted advertising is such a problem. To be sure, use of information about a consumer's web surfing behavior for targeting advertising is a practice that has garnered much attention, but there is no apparent reason why targeting advertising based on *more* data is somehow worse than targeting marketing based on only a *fragment* of Internet behavior. If targeting advertising based on visits to *some* websites is acceptable, as the Commission seems to acknowledge, the Commission has offered no coherent reason why targeting advertising based on visits to *more* websites visited becomes problematic. Access to more information in deciding which computer should receive which advertisement is highly likely to increase the *benefits* of targeting based on past history, but the Commission has articulated *no* reason to believe that it increases the costs. If a more comprehensive set of data poses a greater risk of harm in the event of a security breach, requirements for greater security precautions would be appropriate. More stringent requirements are already implicit in the FTC's approach, however, which requires security precautions that are "reasonable and appropriate in the circumstances."

The Commission cites the claim in the Federal Trade Commission's March 2012 Privacy Report[5] that ISPs can "develop highly detailed and comprehensive profiles of their customers." The FTC also noted, however, that operating systems and browsers are in a similar position to develop extensive data. More importantly, the Commission does not refer to any of the data presented in the FTC's December workshop[6] that explored concerns about "large platform providers." I presented data indicating that ISPs in fact lack a "comprehensive" view of their customers' online behavior for a number of reasons. Consumers employ multiple devices, on multiple networks, from multiple locations, each of which may involve a different communications provider. Moreover, I noted the increasing use of encryption, which limits the information available to broadband providers.[7]

Professor Peter Swire recently conducted a similar analysis. He concluded:

> First, ISP access to user data is not *comprehensive* – technological developments place substantial limits on ISPs' visibility. Second, ISP access to user data is not

[5] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012).

[6] Federal Trade Commission, The Big Picture: Comprehensive Online Data Collection (December 2012). Archived Webcasts of the event and public comments submitted are available at https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection.

[7] Beales, Howard and Eisenach, Jeffrey A., Putting Consumers First: A Functionality-Based Approach to Online Privacy (January 1, 2013). Available at SSRN: http://ssrn.com/abstract=2211540 orhttp://dx.doi.org/10.2139/ssrn.2211540

unique – other companies often have access to more information and a wider range of user information than ISPs.[8]

Of course, broadband providers have access to a substantial amount of information about browsing behavior. But so do many other players in the Internet ecosystem that would not be subject to a special privacy regime. Each provider has particular insights into the consumer's online activities, but there is no entity in a "unique" position to assemble a "comprehensive" picture of online behavior.[9]

For example, one analysis found that Facebook has an icon on an estimated one third of all top websites, and DoubleClick tracks visits to nearly 20 percent of top 1000 web pages.[10] Either company likely covers an even greater percentage of the most popular websites that account for a substantial fraction of Internet page views. A *Wall Street Journal* analysis found that 75 percent of the top 1,000 web sites include code from one or more social networks.[11] Of course, such networks can track their members' activities regardless of how or where they are accessing the Internet.

To be sure, at a given point in time, some firms or types of firms likely have the ability to capture a "more comprehensive" view of individual consumers' browsing behavior than others. But in the dynamic world of the Internet, any such "advantage" is likely to be short-lived: In 2000, ISPs may have had the greatest potential ability to track online behavior (though there is no evidence they did so in any systematic way); in 2005 it may have been Microsoft (through the IE browser); and today it may be login services such as Google or Facebook. Thus, even if the Commission could single out a firm or group of firms as having great capability to gather comprehensive information than others, those firms may not be subject to the Commission's jurisdiction. Moreover, technology and market developments would soon make such a finding obsolete.

---

[8] Peter Swire, Justin Hemmings, and Alana Kirkland, Online Privacy and ISPS: ISP Access to Consumer Data is Limited and Often Less than Access by Others, Working Paper of the Institute for Information Security and Privacy at Georgia Tech, Feb. 29, 2016.

[9] The exceptions are law enforcement agencies, which can use search warrants or, in many cases, merely subpoenas to obtain data from multiple online and offline sources (e.g., content providers, ISPs, credit card companies, etc.) to assemble a "comprehensive" picture of some portion of a citizen's life. No private sector firm is or is likely in the foreseeable future to be able legally to obtain such comprehensive information, nor would a commercial firm have an incentive to do so.

[10] See e.g. Jeff Blagdon, "Do Not Track: An Uncertain Future for the Web's Most Ambitious Privacy Initiative," *The Verge* (October 12, 2012) (available at http://www.theverge.com/2012/10/12/3485590/do-not-track-explained).

[11] See Jennifer Valentino-Devries and Jeremy Singer-Vine, "They Know What You're Shopping For," *The Wall Street Journal* (December 7, 2012) (available at http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html).

Whether comprehensive or not, it is worth noting that *every* piece of information a broadband provider obtains about a consumer's web surfing behavior is also obtained by at least one other entity – the owner of the web page visited. More commonly, in an ecosystem with numerous advertising networks using cookies to track web surfing behavior and numerous data analytics companies, *many* entities have access to that same piece of information. All of them can now use that information on equal terms. Under the FCC's proposed rules, everyone *except* the broadband service provider can use it. At best, the proposal closes one of the holes in a sieve. It does nothing to enhance consumer privacy.

B. Broadband Service Providers Are Unlikely To Engage In Harmful Conduct

Broadband service providers typically are large, publicly traded corporations with high levels of firm-specific reputational capital. Such firms are subject to reputational damage if they are seen as engaging in conduct that is harmful to consumers, and are thus less likely than other firms, *ceteris paribus*, to do so.[12] In addition, unlike edge providers, ad networks and other online entities that have only ephemeral relationships with consumers, broadband providers have ongoing business relationships with their subscribers and therefore must safeguard their privacy in order to retain their trust and their business. The fact that firms with high levels of repeat purchasers are relatively unlikely to engage in opportunistic behavior towards consumers is widely agreed upon in the consumer protection literature.[13]

Despite favorable incentives, violations can occur, and enforcement action in such cases is appropriate. There is, however, no reason to impose the *strongest* regulatory requirements on the sector of the industry where problems are *least* likely.

---

[12] See generally Benjamin Klein and Keith B. Leffler, "The Role of Market Forces in Assuring Contractual Performance," *Journal of Political Economy* 89;4 (1981) 615-641.

[13] See generally Philip Nelson, "Information and Consumer Behavior," *Journal of Political Economy* 78;2 (March/April 1970) 311-329 and Philip Nelson, "Advertising as Information," *Journal of Political Economy* 82;4 (July/August 1974) 729-754. From an economic perspective, the month-to-month nature of ISP service is equivalent to a high rate of repeat purchases. Markets with high rates of repeat purchases are generally not susceptible to quality assurance problems. See, for example, Klein and Leffler (1981) at 624 (discussing "the familiar recognition that, given a particular quality level, quality-cheating problems are less severe the higher the level of quality that can be detected pre-purchase and *the shorter the period of repurchase*."); and Nelson (1974) at 730 ("The major control that consumers have over the market for experience qualities is whether they repeat the purchase of a brand or not.")

C. Consumers Do Not Face Unique Switching Costs In Dealing With Broadband Providers

Switching costs are ubiquitous, particularly in the internet economy. Moving from one cloud service provider to another requires moving data to a new platform, and may complicate the ability to share documents with other users. Shifting from Facebook to another social network requires both moving data and abandoning a network of friends. Switching costs may be higher for leaving a network like LinkedIn, where a significant part of the value is a broad range of contacts. Even changing search engines requires some adjustments to the different order in which results are likely to appear.

There are also costs of switching broadband providers, but the question is whether those switching costs are high compared to the costs of switching between edge providers. Unless there are significant differences in switching costs, there is no basis for creating a special regulatory regime for broadband providers. The evidence regarding turnover statistics indicates that if anything, switching costs are lower for broadband providers than for some other edge providers.

Based on turnover rates of broadband customers, switching is not particularly difficult. Parks Associates reported that 9% of all broadband households switched providers within the past 12 months.[14] Turnover rates are higher for the national facilities-based wireless service providers, with rates implying that each of the four major carriers loses 14 to 27% of its customers each year.[15] The FCC's last report on wireline providers in 2010 indicated that one out of six customers switch providers every year, and 36% switched in the last three years.[16] These turnover rates for broadband providers are substantially higher than the roughly 5% of Android and iOS consumers who change their smartphone operating systems each year.[17]

Although not completely comparable, turnover rates also appear larger than the annual shifts in browser market share between February 2015 and 2016 (-5.5% for Internet Explorer; +6.6% for

[14] http://www.parksassociates.com/blog/article/pr-11302015-needforspeed.

[15] FCC, Eighteenth Wireless Competition Report, Dec. 2015, Chart II.B.6.

[16] See *Broadband Decisions: What Drives Consumers to Switch – or Stick With – their Broadband Internet Provider* (Federal Communications Commission Working Paper, December 2010) (available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-303264A1.pdf).

[17] Ericsson, Smartphone Switching Patterns, November 2015. https://www.ericsson.com/res/docs/2015/mobility-report/emr-nov-2015-smartphone-switching-patterns.pdf.

Chrome)[18] or the shift in search engine market shares between October 2015 and 2014 (-3.4% for Google, smaller increases for Bing and Yahoo).[19]

These data indicate a level of competition and consumer churn that ensures that the privacy options offered by broadband providers adequately meet consumers' needs. They should alleviate concerns that providers could successfully engage in "one-sided" business practices, such as offering "take-it-or-leave-it" choices that violate the preferences of a substantial proportion of consumers. They certainly provide no basis for regulating communications providers and edge providers differently.

II. A Separate Regulatory Regime For Broadband Providers Would Inhibit Innovation, Reduce Competition, And Harm Consumers

The online market is a multi-sided market, comprised of consumers, information collectors, information aggregators, and information users (i.e., advertisers and vendors). Firms both compete and cooperate to create value through participation in platforms, with each firm and each platform seeking to capture as much of the resulting value as possible through innovation to differentiate its product. Competition takes place along multiple dimensions: information collectors and aggregators compete to provide the highest value to consumers, but also to create value for advertisers and other information users. A separate regulatory regime for broadband providers, especially to the extent it effectively "grandfathers in" existing business practices for other firms but precludes similar practices for potential entrants, threatens to both slow and distort innovation and, by so doing, inadvertently create or perpetuate market power in one or more sectors of the market.

Regulating broadband providers raises their costs, but does not raise the costs of their competitors or potential competitors. Because it protects the less regulated firms from actual or potential competition, the proposed regulation can be a source of monopoly power and its consequences of higher prices, lower quality, and less innovation. Thus, the Commission should be extremely cautious about imposing regulatory burdens on some firms but not others. Restrictions on information use are no different. As Randal Picker explains,

> An uneven playing field that allows one firm to use the information that it sees while blocking others from doing the same thing creates market power through limiting competition. We rarely want to do that. And privacy rules that limit how information can be used and shared across firms will artificially push towards

[18] Craig Buckler, Browser Trends March 2016, https://www.sitepoint.com/browser-trends-march-2016-operating-system-surprises/ (March 2, 2016).

[19] Eli Schwartz, Is Google's Search Market Share Actually Dropping, December 10, 2015 (Reporting comScore's share statistics) http://searchengineland.com/googles-search-market-share-actually-dropping-237045.

> greater consolidation, something that usually works against maintaining robust competition.[20]

The ability to match messages to interested consumers plays a central role in today's online display advertising markets. Advertisers increasingly utilize information about web browsing histories. There is substantial evidence that interest-based advertising increases advertising efficiency. A 2014 study of auction markets for display advertising found that advertising availabilities associated with a new cookie (30 days old) sold for roughly three times the price that won the auction if there was no cookie. Older cookies were more valuable. For an ad with a 90 day cookie, the price was 3.7 to 7.1 times higher than with no cookie, depending on the particular company studied.[21] Similarly, a 2010 survey of major advertising networks found the price of behaviorally targeted advertising was 2.68 times higher than the price for run-of-network advertising, and that behaviorally targeted advertising also had higher conversion rates.[22] A study of European privacy regulation supports the same conclusion, concluding that restrictions on behavioral advertising reduced advertising effectiveness by approximately 65 percent. Moreover, the adverse impact was greatest on general content websites such as news outlets, where there is no obvious alternative way to determine who might be interested in which offers.[23]

Advertising plays a key role in supporting online content. From an economic perspective, Internet content, like broadcast television or radio, is a public good. One person's consumption does not reduce the availability of that content to other consumers to any meaningful extent. In a market economy, the tendency is to produce too little of a public good, because it is difficult for the creator to capture the returns from his or her effort.

For decades, a key part of the solution to this economic dilemma has been to link the public good to a private good that can be sold to someone else. By embedding advertising in web pages, the public good of Internet content is linked to the private good of advertising time and space, which in turn can be sold to advertisers seeking to reach consumers. Advertising made possible radio and television broadcasting, provided essential support for the newspaper industry, and facilitated the expansion of hundreds of cable and satellite television channels by helping to underwrite their costs. Online advertising revenue reached a record $59.6 billion in 2015,[24]

---

[20] See Randal C. Picker, "Competition and Privacy in Web 2.0 and the Cloud," *Northwestern University Law Review Colloquy* 103 (July 2008) at 7.

[21] J. Howard Beales and Jeffrey A. Eisenach, "An Empirical Analysis of the Value of Information Sharing in the Market for Online Content," with Jeffrey A. Eisenach, published online by Digital Advertising Alliance, available at http://www.aboutads.info/resource/fullvalueinfostudy.pdf, January, 2014.

[22] See J. Howard Beales, *The Value of Behavioral Advertising* (Network Advertising Initiative) (2010).

[23] Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," *Management Science* 57 (2011), 57-71.

[24] See *IAB Internet advertising revenue report*, 2015 Full Year Results (April 2016), available at http://www.iab.com/wp-content/uploads/2016/04/IAB-Internet-Advertising-Revenue-Report-FY-2015.pdf.

money that is available to support a wide range of content, applications and services for consumers. Approximately 40% of this advertising was display advertising, including mobile display advertising.[25] In short, advertising plays a vital role in the Internet economy, and the ability to sell advertising depends on information that allows advertisers to select audiences that are most likely to be interested in their products.

Prudence is especially important here. Markets for consumer information, online advertising, and digital content are all part of the larger Internet ecosystem.[26] Competition is both direct, in the provision of comparable goods and services, and indirect, through participation in Internet platforms comprised of complementary goods.[27] Competition is also quite dynamic. Unrecoverable expenditures on R&D or plant and equipment generate rapid innovation must be recovered through product differentiation and the resulting ability to charge prices above short run marginal costs (often near zero). With dynamic competition, efficient outcomes result from the ability of firms not already "in the market" to threaten entry, rather than from large numbers of firms producing close substitutes. Raising costs for potential entrants but not incumbents is a true barrier to entry, which can have immediate adverse effects on market performance.[28]

In platform markets, the firms with both the incentives and the capacity to enter are those in neighboring sectors. Cable television operators entered voice telephony. Telephone companies and e-commerce firms such as Amazon entered the market for video. Google entered the market for broadband service, and Apple entered the market for Internet radio. Such actual or threatened entry into markets for complementary products is a central feature of the competitive dynamics of Internet platforms.[29] Regulations that disadvantage one type of platform participant (e.g., BIAS providers) relative to another (e.g., content provider, or social networks) discourage one of the most likely entrants in to the latter's market. Inevitably, that disadvantage will impair competition.

The proposed regulation is harmful to consumers in another way as well. The rule does not protect information, but instead protects a certain channel for obtaining information. Whether consumers decline to "opt in" or actively "opt out" under the Commission's proposal, they are likely to think that the information will not be used for those purposes. In fact, however, the same information will be used by other participants in the Internet ecosystem, because it is not uniquely in the hands of the BIAS provider.

---

[25] *Id.*

[26] See generally Jeffrey A. Eisenach, *Broadband Competition in the Internet Ecosystem* (American Enterprise Institute for Public Policy Research, October 2012) at Chapter 3.

[27] See e.g. Timothy F. Bresnahan and Shane Greenstein, "Technological Competition and the Structure of the Computer Industry," *The Journal of Industrial Economics*, 47;1 (March 1999) 1-40 (As Bresnahan and Greenstein explain, "a firm in one layer [of the platform] has every incentive to grab the rents of a firm in another layer.").

[28] See George J. Stigler, *The Organization of Industry* (University of Chicago Press, 1968) at 67-70.

[29] See e.g., Eisenach, *Broadband Competition* at 22.

In this regard, the presumed "extra protection" of an opt-in rule is an illusion. Consumers who do not opt in prevent the broadband provider's use of that information. To prevent others from using the information, they have to do what they do now – opt out at each of the entities (or a centralized opt out mechanism like the Digital Advertising Alliance) that may have access to the information.

With privacy preferences, the most important cost of exercising choice may well be the cost of considering the issue at all. The costs of reading privacy policies to obtain the necessary information are significant, and for most consumers, the stakes in considering commercial privacy issues are small, and not worth the time and attention that would be required to make careful decisions about the optimal choice. Consumers may decide that a decision is not worth the cognitive costs of thinking about an issue at all, particularly when the stakes are small. The default rule is therefore likely to dominate choices.[30] If the default is no sharing, most consumers will end up not sharing.

Default rules should be designed to impose the costs of transactions on consumers who think these costs are worth paying. An "opt-out" default rule means that consumers who do not think that decision-making costs are worthwhile do not need to bear those costs. Consumers who care more intensely, however, will face the costs of making a decision. In contrast, an "opt-in" default rule enables those who care the most about the issue to avoid the decision costs, because the default will match their preferences. For example, experiments have found that among consumers who are more concerned about privacy, there is no difference in participation whether the default rule is opt in or opt out.[31]

III. Any Regulation Should Adopt A Functionality-Based Approach

Privacy protection should put consumers first. Its goal should be to avoid the adverse consequences to consumers than can result from data breaches or information misuse. Consequences, however, arise from uses of information, and not from the mere fact that

[30] Eric Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, 302 Science 1338 (2003) (stating that countries with opt in default rules for organ donation have substantially lower donation rates than countries with opt out rules). As Richard Posner notes in explaining this result, "When the consequences of making a 'correct' decision are slight, ignorance is rational, and therefore one expects default rules to have their greatest effect on behavior …" Richard Posner, *Organ Sales – Posner's Comment*, The Becker-Posner Blog (Jan. 1, 2006), *available at* http://www.becker-posner-blog.com/2006/01/page/2/. (last visited May 13, 2015).

[31] *See* Yee-Lin Lai & Kai-Lung Hui, *Internet Opt-in and Opt-out: Investigating the Roles of Frames, Defaults and Privacy Concerns*, in PROCEEDINGS OF THE 2006 ACM SIGMIS CPR CONFERENCE ON COMPUTER PERSONNEL RESEARCH 253 (2006). On the other hand, among consumers who were less concerned about privacy, the default rule mattered. Thus, opt out is a preferable default rule, because it avoids imposing costs on consumers who do not think the issue is worth the costs of making a decision.

information is collected. Nor do the consequences depend on the business model of the entity collecting the information.

The policy framework for online information practices should therefore be tied to the nature of the information collected and the uses to which it is put. Such an approach ties privacy protections to the potential for consumer harm. "Sensitive" information, with a greater potential to harm consumers, should be subject to more oversight than information that is not sensitive or is not personally identifiable. Information uses with more potential for harm, such as using website visits to set insurance rates, should similarly be subject to greater oversight. When information uses likely generate net benefits, however, as when information is used to reduce the risk of fraud or to better target advertising, there is little reason for regulatory scrutiny.

As in any regulatory endeavor, the goal should be to maximize the net benefits of the intervention.[32] Focusing on the nature of information and its uses is consistent with this goal in the context of privacy. The technology used to collect information, or the business model of the company that does so, has no impact at all on the consequences, good or bad. The costs of intervening based on technology or business models, however, are likely to be particularly high. The Internet era has been characterized by phenomenally rapid change, a pace that is likely to continue for the foreseeable future. Facebook or Twitter may be the most recent "big things," but it is exceedingly unlikely that they are the last big things.

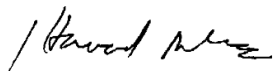
Precisely because no one can reliably predict how technology or economic organization will change, any regulatory approach based on those considerations is likely to channel, and distort, the continued improvement of the Internet as a tool for consumers and the information economy. The Commission should therefore avoid singling out business models or technologies as either "the" or a "special" problem.

[32] *See* Executive Order 13563, *Improving Regulation and Regulatory Review* (January 18, 2011) ("[T]o the extent permitted by law, each agency must, among other things: (1) propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); (2) tailor its regulations to impose the least burden on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations; (3) select, in choosing among alternative regulatory approaches, those approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity); (4) to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt; and (5) identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public."). *See also* Thomas M. Lenard and Paul H. Rubin, "In Defense of Data: Information and the Costs of Privacy" *Policy & Internet* 2;1 (2010) 149-183, 179 ("Good public policy requires that proposals for additional regulation be based on a showing that consumers are being harmed and that new regulation would alleviate those harms in a way that the benefits are greater than the costs.").

Approaching privacy issues by focusing on information and its uses also minimizes regulatory ambiguity and uncertainty, which again facilitates innovation. A company with a new and better way to collect information that is already collected knows that it can do so without regulatory risk, since it is the nature of the information that matters, not the manner of its collection. By the same token, a company contemplating new uses of existing information knows that it must consider whether that use is likely to create consumer harms. Consumers benefit in precisely the same sense: they can form expectations regarding privacy practices knowing that certain types of information will be protected regardless of how or where it is collected, and that certain types of uses are limited or proscribed no matter what type of platform is involved.

Thank you for considering this comment.

Respectfully submitted,



J. Howard Beales III
Professor, Strategic Management and Public Policy
George Washington School of Business