NAVIGANT
ECONOMICS

PUTTING CONSUMERS FIRST: A FUNCTIONALITY-BASED APPROACH TO ONLINE PRIVACY

J. Howard Beales
Jeffrey A. Eisenach[†]

January 2013

[†] J. Howard Beales III is a Professor at George Washington University School of Business. Jeffrey A. Eisenach is Managing Director and Principal, Navigant Economics, LLC, a Visiting Scholar at the American Enterprise Institute and an Adjunct Professor at George Mason University Law School. The authors are grateful to Andrew Card for research assistance and to Broadband for America for financial support. The views expressed are the authors' and do not necessarily reflect those of Navigant Economics LLC or any of its affiliates, or of the other institutions with which the authors are affiliated.

EXECUTIVE SUMMARY

U.S. privacy policy has long embraced a functionality-based approach which calibrates privacy protections to the types of information collected and the uses to which it is put. The functionality-based approach targets attention to areas where harm to consumers is most likely to occur, and hence where the potential benefits from oversight are greatest.

In its March 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*, the Federal Trade Commission expressed concerns about the comprehensiveness of data collected by some online service providers (i.e., "large platform providers," including internet service providers (ISPs)) and also about whether there is sufficient competition or choice to protect consumers' interests with respect to privacy practices. Based on those concerns, the Commission discussed the possibility of subjecting some types of business models or technologies to heightened scrutiny or a distinct framework.

In this report, we assess the issues raised by the Commission and conclude that they do not justify a departure from a functionality-based framework. Specifically, we conclude:

- The Commission has not proffered a clear definition of comprehensive data collection or an explanation of why the comprehensiveness of information collection activities poses public policy concerns. Whatever valid concerns may exist are best addressed within a functionality-based framework.
- Consumers access the Internet using multiple paths and multiple technologies. For example, more than half of all consumers now have both smartphones and computers, and use both for Internet access; and, consumer Internet access increasingly occurs over encrypted connections. As a result, no single firm has the ability to gather "comprehensive" data on consumers' online activities.
- Consumers have, and exercise, a high degree of choice when it comes to online service providers. One out of six customers switch wireline providers every year, and 37 percent switch every three years; among wireless providers, between a fifth and a third of all customers switch every year. Moreover, ISPs offer consumers significant privacy choices.
- Asymmetric regulation – i.e., imposing more stringent regulations based on the technologies or business models of certain online service providers – would harm consumers in a variety of ways:
    - Applying a different privacy oversight framework based on technologies or business models would lead to consumer confusion about which protections apply under which circumstances.
    - Prohibiting or limiting information collection or use could reduce the efficiency of the markets for consumer information, advertising and online services, leading to less useful services, less informed consumers and reducing the ability of advertisers to support free online content and other services.
    - Regulation based on technologies or business models is inherently inflexible and thus impedes innovation while protecting incumbents.
    - Regulating some firms but not others would reduce the ability of the regulated firms to compete in the market for information, thereby raising barriers to entry, reducing competition overall, slowing innovation, and raising prices.

The Commission's concerns about comprehensiveness and choice, or about large platform providers and ISPs, do not justify departing from the functionality-based framework that has characterized U.S. privacy policy heretofore. Doing so would harm both competition and consumers.

CONTENTS

I. INTRODUCTION

The Federal Trade Commission's March 2012 report on *Protecting Consumer Privacy in an Era of Rapid Change* ("*Final Report*" or "*Report*") proposes a policy framework for addressing consumer protection and privacy issues associated with the commercial collection and use of consumer information. For the most part, the proposed privacy framework appropriately embraces a commercially and technologically neutral approach that "applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device."[1] However, the *Report* also raises questions about whether firms that engage in "comprehensive" data collection, pursue certain types of business models, or utilize certain types of technology, raise special concerns.[2] The *Final Report* recognizes that "[t]hese are complex and rapidly evolving areas, and more work should be done to learn about the practices of all platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data."[3] Accordingly, the Commission has asked for further information on these and related issues.[4]

In this study, we explain why a functionality-based approach, which calibrates oversight to the nature of the data being collected and the uses to which it is put, best protects consumer interests; and we show why attempts to impose an asymmetric privacy framework or regulatory approach targeted at particular technologies, business models or types of firms would be counterproductive. As we explain, the functionality-based approach is consistent with existing U.S. privacy policy, and allows consumers to form consistent expectations about how

---

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012) at vii (hereafter *Final Report*).

[2] See e.g., *Final Report* at v, 55.

[3] *Final Report* at 56.

[4] See "FTC to Host Workshop to Explore Practices and Privacy Implications of Comprehensive Collection of Internet Users' Data," (October 15, 2012) (available at http://ftc.gov/opa/2012/10/collection.shtm) (hereafter *December 6 Workshop Notice*).

information is collected and used, rather than trying to keep track of different regimes depending on the type of technology or business model involved. Moreover, because a functionality-based approach is not tied to specific technologies or business models, it is capable of adapting to the rapidly changing online environment. Asymmetric regulation, on the other hand, would confuse consumers by imposing different rules for similar uses of data or similar online activities, while locking in business models, deterring innovation and distorting competition.

Asymmetric treatment is not justified on the basis of either the scope (or "comprehensiveness") of data collection or by concerns about consumer choice. With respect to scope, it is far from obvious which firms or types of firms currently have the most comprehensive view of consumers' online activities. As we demonstrate, consumers' access to the Internet is fragmented across multiple channels, meaning that no online service provider[5] is in a position to collect a comprehensive record for any significant proportion of consumers, and there is no qualitative difference between the comprehensiveness of data available, for instance, to ISPs and what can be and is collected by other types of firms, such as firms that provide as search engines, browsers, operating systems and social media platforms, as well as data brokers and large advertising networks.

Equally important, technologies and market conditions are constantly evolving. Thus, any attempt to categorize particular providers as uniquely engaged in "comprehensive data collection" about consumers' online activities would quickly prove outdated. As recently as five years ago, for example, few would have thought Facebook would have had the most

[5] Throughout, we use the phrase "online service provider" to refer to the full array of firms that interface with consumers and are an in a position to collect and use consumer information, including online content and applications providers, software producers, ISPs and so forth.

comprehensive picture of consumers' browsing behavior, as some might argue it does today. Although Facebook is a "big thing," it is exceedingly unlikely that it is the *last* big thing.

Finally, it is not obvious that the "comprehensiveness" of information collection raises distinct concerns in the first instance. The Commission has long recognized that consumers benefit from the information made available by relevant, truthful advertising, and information collection practices that allow such information to be provided in ways that are more relevant, or timely, to consumer decisions are thus *prima facie* beneficial. And, even if comprehensiveness does raise distinct concerns, they are not likely a function of whether the information is collected by a single application or service provider rather than by a "large platform provider." To the contrary, as we discuss, to the extent large platform providers are firms with significant reputational capital, and which depend on repeat business, such firms are less likely to violate consumer expectations than less substantial companies.

With respect to consumer choice, the data show that consumers have and exercise choice among providers of various types of online services, including Internet access, content and applications, as the fragmentation of their browsing habits suggests. In fact, the market reflects intense competition between and among a diverse range of companies, some of which increasingly are integrated across the value chain. The evidence shows that competition is providing consumers with a wide (and growing) array of choices and tools that allow them to customize information sharing practices to fit their heterogeneous preferences.

A functionality-based approach promotes competition and consumer choice by providing a stable and level regulatory environment. Regulation that discriminates on the basis of technology or business model, on the other hand, would limit (or eliminate altogether) the ability of certain types of firms (e.g., ISPs) effectively to compete, thereby foreclosing a potentially

important source of competition and innovation in this market. The online market is a classic example of a multi-sided market comprised of consumers, information collectors, information aggregators, and information users (i.e., advertisers and vendors). In such markets, different types of firms both compete and cooperate (through participation in platforms or "ecosystems") to create value, with each firm and each platform seeking to differentiate its product through innovation and, by doing so, capture the largest possible share of the resulting value. Further, and crucially, competition takes place along multiple dimensions, e.g., information collectors and aggregators compete not only to provide the highest value to consumers, but also to create value for information users, such as advertisers. Asymmetric regulation, especially to the extent it effectively "grandfathers in" existing business practices for some firms but precludes or impedes entrants from adopting the same or similar practices, 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.

In this sense, asymmetric treatment of large platform providers would detract from the FTC's mission of protecting competition, which includes not only preventing harmful acts and practices, but also refraining from imposing regulations or taking other actions that create barriers to entry or enhance market power. Simply put, asymmetric regulation of consumer information would harm competition and consumers by raising barriers to entry in the market for online advertising and limiting the universe of entities that can use consumer data to develop innovative new products and services..

For all of these reasons, and others we discuss below, we conclude that a functionality-based approach, which tailors privacy oversight based on the nature (i.e., sensitivity) of the information being collected and the uses to which it is put, will best protect the interests of

consumers. The remainder of this paper is organized as follows. In Section II, we describe the functionality-based approach we recommend and explain why it is consistent with past practices and with the *Final Report*. Section III turns to the issues of scope and choice and their implications, and then discusses the potential harmful effects of asymmetric regulation on consumers and competition. Section IV presents a brief summary of our conclusions.

II. A Functionality-Based Approach to Privacy Oversight

The goal of any privacy policy framework should be to maximize consumer welfare by striking a balance between the benefits and the costs of information collection and use, both today and into the future. With this in mind, the first section below briefly discusses the importance of consumer information to consumer welfare and the economics of the Internet, including security, service quality and the availability of online content that is entirely or partly underwritten by advertising. In the second section, we explain why we believe that a functionality-based approach that calibrates the level of expected privacy protection and regulatory intervention to the nature and sensitivity of the information collected and the ways in which it used is both consistent with the Commission's privacy framework and is preferable, from a consumer welfare perspective, to one that singles out specific technologies or business models.

A. Commercial Applications of Online Data Collection

As the *Final Report* recognizes, 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.[6] 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. The Commission has long recognized, as noted above, that truthful advertising plays a crucial role in providing consumers with the information essential for a well-functioning marketplace. 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.

At the most fundamental level, it is a basic tenet of modern economics that markets function more efficiently when consumers are well informed about the choices available to them in the marketplace.[7] The effect of imperfect information is that consumers make "faulty" decisions: That is, they purchase products from sellers who charge more than the prices being charged for identical products by other sellers; or, if products are differentiated, they purchase products that do not fully meet their needs when a similar product, available for the same price, would provide them with greater satisfaction. Both consumers and competition are harmed as a result.[8] The importance of information to economic efficiency is well-recognized by both the

---

[6] 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 (2009) 109-135, especially at 115-117.

[7] *See*, e.g., Dennis W. Carlton and Jeffrey M. Perloff, *Modern Industrial Organization* (2005) at 440-441. The importance of information to economic efficiency is also well-recognized in the law.

[8] *See* Howard Beales, Richard Craswell and Steven C. Salop, "The Efficient Regulation of Consumer Information," *Journal of Law and Economics* 24 (December 1981) 491-539, 503. ("Additional information induces sellers to compete for the patronage of informed consumers by offering better values – either lower prices or higher qualities. This induced competition also benefits those uninformed consumers who purchase randomly.") (hereafter, Beales, Craswell and Salop.); *see also* Carlton and Perloff at 452 ("Firms can obtain market power from consumers' lack of knowledge about prices and quality. Limited information can lead to a monopolistic price in what would otherwise be a competitive market.")

Commission and the courts.[9] And, it has long been accepted that the ability of advertisers to more efficiently target their advertising increases market competitiveness and causes prices to fall.[10]

The ability to match messages to interested consumers plays a central role in today's online advertising markets. One highly successful method to link advertising content to consumer interests is search advertising. The key information is the search term the consumer entered, which allows advertiser to assess which search terms are most closely linked to the characteristics of the consumers they are trying to reach. Search advertising accounted for 48 percent of online advertising revenue in the first half of 2012.[11]

The other major form of online advertising is display-related ads, which accounted for 33 percent of revenue in the first half of 2012. In order to provide display-related ads that match consumer interests, advertisers increasingly utilize information about web browsing histories. There is substantial evidence that interest-based advertising increases advertising efficiency. For example, a recent survey of major advertising networks found the price of behaviorally targeted advertising to be 2.68 times higher than the price for run-of-network advertising, and that

---

[9] See, e.g., *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council Inc*., 425 US 748, 765 (1976) ("So long as we preserve a predominantly free enterprise economy, the allocation of our resources will be made through numerous private decisions. It is a matter of public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensable."); *Fair Packaging and Labeling Act*, 80 Stat. (1966) 15 U.S.C. §§1451-61. ("Informed consumers are essential to the fair and efficient functioning of a free market economy."); Federal Trade Commission, *Statement of Basis and Purpose, Labeling and Advertising of Home Insulation* 44 FR 50218, 50222 (1979) ("It is a basic tenet of our economic system that information in the hands of consumers facilitates rational purchase decisions; and, moreover, it is an absolute necessity for the efficient functioning of the economy.")

[10] *See* e.g., Gene M. Grossman and Carl Shapiro, "Informative Advertising with Differentiated Products," *The Review of Economic Studies* 51;1. (January 1984), at 63-81, 77 ("We have constructed a model of purely informative advertising with heterogeneous goods. … We have also studied the effects of changes in the advertising technology on equilibrium in product markets. … *[W]e found that improved efficiency of advertising (e.g. a reduction in the cost per exposure) does indeed increase the competitiveness of the market (as measured by demand elasticities) and causes prices to fall.*") (emphasis added).

[11] See Interactive Advertising Bureau, *IAB Internet Advertising Revenue Report* (PricewaterhouseCoopers 2012) **(**available at http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_HY_2012.pdf) (hereafter *IAB Report*).

behaviorally targeted advertising also had higher conversion rates.[12] 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.[13]

Advertising plays a key role in supporting online content. From an economic perspective, Internet content is a public good. One person viewing a web page does not reduce the availability of that same page 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 $17 billion in the first half of 2012,[14] money that is available to support a wide range of content, applications and services for consumers. 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.

---

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

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

[14] See *IAB Report.*

B. Functionality-Based Regulation and the Privacy Framework

The *Final Report* advances a wide-ranging privacy framework with implications for self-regulation, enforcement under existing statutes, and new legislation. In many respects, the framework is consistent with the functionality-based approach we propose. In the first subsection below, we explain why a functionality-based approach is desirable from the perspective of maximizing consumer welfare. In the second subsection, we highlight the ways in which the *Final Report* embraces and adopts a functionality-based approach. Our purpose is to set the stage for explaining, in Section III below, why it would not be in the interests of consumers to depart from a functionality-based approach by singling out particular technologies or business models for asymmetric regulation.

1. A Functionality-Based Approach Maximizes Consumer Welfare

The policy framework for online information practices should be based on the nature of the information being collected and the uses to which it is put, and should not discriminate on the basis of the technologies or business sectors involved. By definition, this approach ties expected privacy protections to the potential for consumer harm, and is in that sense inherently performance-based: information that has the inherent potential to harm consumers (i.e., "sensitive" information) is subject to greater oversight than non-sensitive or non-personally identifiable information; and, information uses that have greater potential to cause harm (e.g., using website visits to set insurance rates) are subject to greater oversight than those (e.g., first-party fraud prevention and behavioral advertising) that likely generate net benefits.

A functionality-based approach has several important advantages. First, such an approach reduces the likelihood of bad outcomes for consumers. For consumers, bad outcomes stem from the type of information collected and the uses to which it is put, not from the technology used to collect it or the business model of the firm that does so. Thus, it makes no difference whether

the innocuous fact that a consumer visited a website selling digital cameras was collected via a cookie or through inspecting the packets of the communication. The technical means of collection is irrelevant. Nor does it matter whether the firm collecting the information also knows which other innocuous web sites the consumer previously visited. By the same token, information about a consumer's visits to a website focused on a sensitive medical condition is sensitive, regardless of the technology used to collect the information. Similarly, the business model of the firm collecting the data is *prima facie* irrelevant: the consumer is concerned that the information be treated with the appropriate level of confidentiality regardless of who collects it.

The risk of consumer harm also depends on the uses of the information that has been collected. Using information about a visit to a website that features articles about street racing to tell consumers about automotive accessories is far less likely to negatively affect a consumer than using the same information to set auto insurance rates.

Thus, focusing on the nature of information and its uses is consistent with the goal of maximizing the net benefits of the overall privacy framework. As in any regulatory endeavor, the goal should be to maximize the net benefits of the intervention.[15] As discussed further

[15] *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.").

below, these concepts are also deeply embedded in existing U.S. privacy law and policy, and are consistent with the FTC's Privacy Framework.

By contrast, the costs of intervention based on technologies and business models are likely to be particularly high. The history of the Internet era is one of rapid change in technologies, business models, and economic organization of the functions necessary to deliver and finance a smoothly functioning Internet. The rapid pace of change is likely to continue for the foreseeable future; there is no evidence that we are at or anywhere near the long run equilibrium organization of the Internet. The first social network site, SixDegrees.com, launched in 1997.[16] Today, Facebook has more than a billion users and bears little resemblance to early social networks.

Indeed, the benefits of any approach that focuses on today's technologies or business models are likely to be small and diminishing over time. 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. In its approach to information security, the Commission has wisely resisted arguments to enshrine particular technological approaches to the problem as "the" solution. For exactly the same reasons, it should avoid singling out business models or technologies as either "the" or a "special" problem.

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

---

[16] See D.M. Boyd and N.B Ellison, N. B. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, 13;1 (2007) (available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html).

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.

Finally, a functionality-based approach minimizes the potential for regulatory rent seeking, i.e., for attempts by firms or industries to use the regulatory process to obtain a competitive advantage over actual or potential competitors. Tying expected privacy protections to the nature and uses of information involved may not guarantee a completely level competitive playing field – firms may still seek to get the Commission to write rules in such a way as to favor their particular technologies or business models – but it is surely superior to rules that directly disadvantage some firms or technologies and advantage others.

Of course, the Commission may wish to establish enforcement priorities. A demonstrated pattern of consumer harm, however, should be a pre-condition for departures from a functionality-based approach, and that is not the case here.

2. The Privacy Framework Embraces Functionality-Based Oversight

The functionality-based approach we recommend is entirely consistent with the Privacy Framework outlined in the *Final Report*. The idea that privacy protections should be tied to the nature and use of information is inherent in the fundamental distinctions made in the report between personally identifiable information and aggregated data, sensitive and non-sensitive information, between information used in the context of a firm's relationship with the customer

and information used for other purposes, and between information used by the firm that collects it and information shared with third parties.

The functionality principle is also reflected in the Commission's recommendations with respect to specific privacy practices. For example, with respect to data retention, the *Report* recommends that retention periods "can be *flexible and scaled according to the type of relationship and use of the data*," noting that "there may be legitimate reasons for certain companies that have a direct relationship with customers to retain some data for an extended period of time,"[17] but that companies should recognize "the *sensitivity of data* such as a particular consumer's real time location" and "take special care to delete this data as soon as possible, consistent with the services they provide to consumers."[18] Similarly, with respect to data accuracy, the Commission finds that "the best approach to improving the accuracy of the consumer data companies collect and maintain is a flexible one, *scaled to the intended use and sensitivity of the information.*"[19]

More broadly, as noted above, the principle of tying privacy policy to the nature and use of information rather than technology is deeply embedded in existing law and policy. Indeed, Congress has put in place specific statutory frameworks for "sensitive" information in a number of areas, including children,[20] credit,[21] and health.[22] Indeed, these statutes further demonstrate

---

[17] *Final Report* at 28 (emphasis added).

[18] *Final Report* at 29 (emphasis added).

[19] *Final Report* at 29 (emphasis added). ("Thus, for example, companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain. Companies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy, including allowing consumers access to the data and the opportunity to correct erroneous information.")

[20] See e.g., 15 U.S.C. §§ 6501–6506 (Children's Online Privacy Protection Act).

[21] See e.g., 15 U.S.C. § 1681 et seq. (Fair Credit Reporting Act).

[22] See e.g., 42 USC § 201 et seq. (Health Insurance Portability and Accountability Act). See also J. Thomas Rosch, "Information and Privacy: In Search of a Data-Driven Policy" (August 22, 2011) at 4-5. ("It is indisputable that consumer harm occurs when [sensitive] information is not treated with the proper deference. Indeed, federal statutes – such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-

the downsides of basing oversight on business models or technologies: To the extent they have done so, policymakers have found themselves scrambling later to catch up with subsequent changes in business practices and technology, for example, by having to pass legislation to extend HIPPA protections to business associates.[23] The Commission should only depart from this fundamental principle of technological and business model neutrality if it has substantial evidence that doing so is necessary to prevent compelling consumer harm. As we next explain, that is not the case here.

III. COMPREHENSIVENESS, CHOICE AND THE TREATMENT OF LARGE PLATFORM PROVIDERS

Despite its embrace of functionality-based principles, the *Final Report* identifies two sets of issues, comprehensiveness and choice, which raise particular concerns for the Commission, and suggests that some types of firms ("large platform providers") and technologies (deep packet inspection, or "DPI") may implicate these issues more than others.[24] As we explain in the first subsection below, the information collection practices of large platform providers do not pose unique threats to consumer welfare on grounds of either comprehensiveness or choice; thus, the underlying premise for asymmetric regulation is lacking: such regulation is not necessary to protect consumers. Moreover, asymmetric treatment of large platform providers could have the unintended effect of raising barriers to entry in markets for consumer information, including the market for advertising as well as in other markets that rely upon consumer information as an input. The impact would be higher costs, reduced output, slower innovation, and a reduction in consumer welfare.

Bliley Act, Fair Credit Reporting Act, and Children's Online Privacy Protection Act – recognize this and regulate certain aspects of the collection, sharing and retention of most of this information.").

[23] See e.g. Kirk J. Nahara, "'New HIPAA' Poses Important Challenges for Business Associates," Wiley Rein LLP (July 2009) (available at http://www.zixcorp.com/documents/white-papers/New-HIPAA-Poses-Important-Business-Challenges.pdf).

[24] Similar issues are raised in Paul Ohm, "The Rise and Fall of Invasive ISP Surveillance," *University of Illinois Law Review* 2009;5 (2009) 1417-1496.

A. Large Platform Providers Do Not Pose Unique Threats to Privacy

The *Final Report* raises two sets of concerns which it suggests might justify heightened privacy protections. First, it suggests that some "large platform providers" – including ISPs, operating systems, browsers, and social media platforms – may engage in (or have the ability to engage in) the collection of more comprehensive data about individual consumers than other types of firms. Second, the *Final Report* expresses concerns that consumers' options with respect to ISPs are constrained in a way that detrimentally affects their privacy. As we explain below, neither of these concerns constitutes a valid basis for departing from a functionality-based framework.

1. Departing from a Functionality-Based Framework is not Justified by Concerns about the "Comprehensiveness" of Data Collection

The first basis upon which the *Final Report* distinguishes large platform providers from other information collectors is with respect to the scope (i.e. the comprehensiveness) of data collected.

As an initial matter, and entirely apart from any notion that large platform providers have a more comprehensive picture of online behavior than other firms, 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 access to consumer information. The answer cannot be marketing. To be sure, use of information about a consumer's web surfing behavior for targeting advertising has been controversial, 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 *some* of the websites a consumer has visited is acceptable, as the Commission seems to acknowledge, the Commission has articulated no coherent reason why targeting advertising based on *more* information about

websites visited becomes problematic. Considering 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 the concern about a more comprehensive picture of a consumer's online behavior is greater risk that the information may be compromised by security breaches, the appropriate remedy, as it is for any sensitive information, is requirements for greater security precautions. That requirement is already implicit in the Commission's information security cases. Companies must take security precautions that are "reasonable and appropriate in the circumstances," including, explicitly, the sensitivity of the information. If the concern is that third parties might access the information for unrelated purposes, such as a legal proceeding that could negatively affect the consumer, or that government might seek to access the information in a law enforcement investigation, the obvious solution is greater restrictions on access rights for third parties and/or government. Moreover, if the real concern is third party access, most of the information already exists, and will continue to exist, in logs that ISPs and others maintain for security and other operational purposes and are frequently the subject of third party subpoenas. This concern provides no basis for restricting the collection of information based on either the technology used to gather the information or the business model of the company that collects it.

In addition, any assessment of the ability of online service providers to collect comprehensive information must take into account the wide range of modalities and tools consumers use to access the Internet today. Each modality gives different parties a particular insight into the consumer's online activities, but our analysis demonstrates that the fragmentation

of consumer Internet access modalities ensures that there is no entity in a "unique" position to assemble a "comprehensive" picture of online behavior.[25]

In particular, our analysis demonstrates that ISPs, about which the Commission seems to have particular concerns,[26] do not likely have a more comprehensive view than other online service providers. 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.[27] 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.[28] 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

---

[25] The exceptions, as recent news reports highlight, 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.

[26] See e.g., *Final Report* at 56 ("ISPs serve as a major gateway to the Internet with access to vast amounts of unencrypted data that their customers send or receive over the ISP's network. ISPs are thus in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible…. The Commission also recognizes that the use of cookies and social widgets to track consumers across unrelated websites may create similar privacy issues. However, while companies such as Google and Facebook are expanding their reach rapidly, they currently are not so widespread that they could track a consumer's every movement across the Internet. Accordingly, although tracking by these entities warrants consumer choice, the Commission does not believe that such tracking currently raises the same level of privacy concerns as those entities that can comprehensively track all or virtually of a consumer's online activity.").

[27] 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).

[28] 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).

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 in 2010, it may have been 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, technology and market developments would soon make such a finding obsolete.

Although it is not possible to describe with complete precision the extent of fragmentation in consumer browsing experiences, it is clear that they vary across at least five dimensions, each of which affects the ability of one or more types of online service providers to collect information: (1) the use by individual consumers of *multiple devices*; (2) the use by individual consumers of *multiple networks*; (3) the use by individual consumers of *multiple browsers*; (4) the fact that individual consumers connect to the Internet from *multiple locations*; and, (5) the widespread and increasing use of *encryption*.

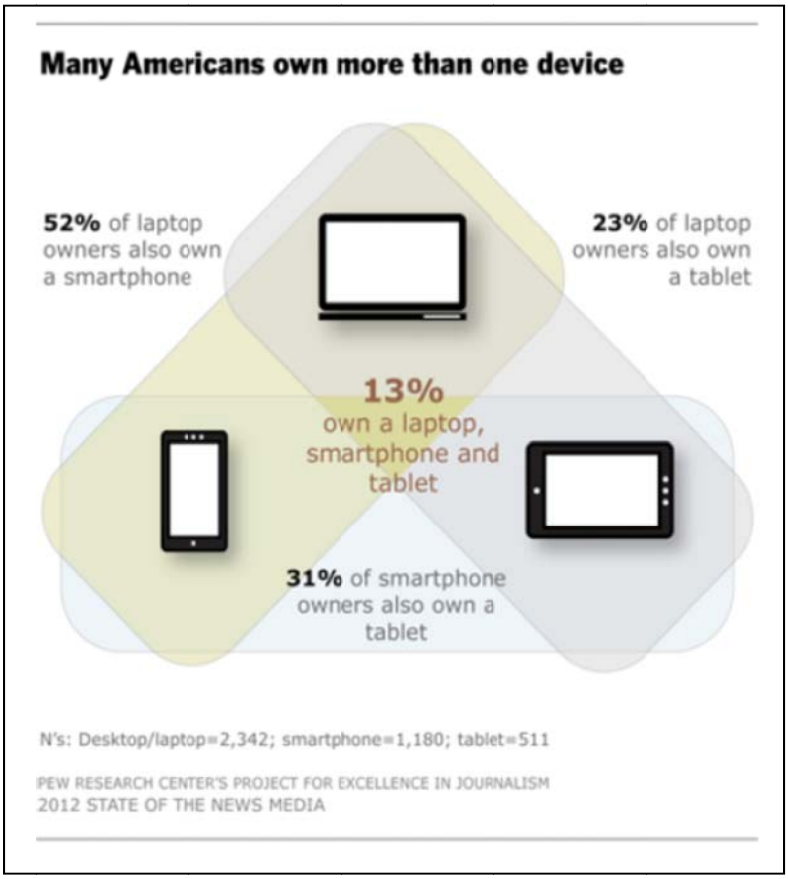
(1) Multiple Devices: When consumers use multiple devices to access the Internet, service providers may not be able to link behavior across those devices. Indeed, the content provider the consumer visits is most likely to be able to link browsing behavior across different devices, particularly if the consumer is (or perhaps has ever) signed in to the service on each of the devices involved. Otherwise, it is difficult to link browsing behavior on one device to browsing behavior on another.[29]

Most Americans own multiple devices with Internet access. According to 2010 survey results from the Pew Research Center, eight in ten (78 percent) American adults own two or

[29] Different devices may, of course, be supported by a common service provider. Consumers may use multiple wifi-enabled devices on a home wireless network, giving the ISP some ability to link across devices. Wifi enabled devices, however, may also be used in other locations on different networks, as discussed below.

more of the following devices: cell phone, desktop computer, laptop computer, mp3 player, gaming console, e-Book reader, and, tablet computer. Furthermore, the typical adult under the age of 45 owns four such devices.[30] As shown in Figure 1, a more recent Pew study, conducted in 2012, found that a majority of laptop owners also own a smart phone, and that 13 percent of adults own at least three devices: A laptop, a smart phone, and a tablet.[31]

FIGURE 1:
MULTIPLE DEVICE OWNERSHIP BY U.S. CONSUMERS, 2012



[30] Aaron Smith, "Americans and Their Gadgets," *Pew Internet & American Life Project* (October 14, 2010) at 3 (*available at* http://pewinternet.org/Reports/2010/Gadgets.aspx).

[31] Pew Research Project State of the Media Project (available at http://stateofthemedia.org/2012/digital-news-gains-audience-but-loses-more-ground-in-chase-for-revenue/digital-by-the-numbers/).

The list of devices Pew studied did not include other Internet-enabled devices, such as HDTVs, Tivo or DVRs, Blu-Ray, and some iPods, all of which at least five percent of consumers use to view streamed TV programs and media delivered via the Internet.[32]

In fact, one study found that smart phones account for 38 percent of all media interactions, compared to 24 percent for personal computers and 9 percent for tablets. Moreover, 90 percent of respondents started a task such as shopping or researching on one device, and continued it on another, usually the same day. Browsing the Internet is the most common activity conducted on multiple devices (81 percent), followed closely by social networking (72 percent) and online shopping (67 percent).[33]

For many, Internet access through a device other than a computer is the *preferred* way to browse the Internet. An estimated 17 percent of all cell phone owners did *most* of their browsing on the phone, rather than on a computer.[34] Moreover, statistics from industry research firm comScore revealed that mobile phone and tablet computers now account for one in eight Internet page views in the U.S.[35]

(2) Multiple Networks: Even on a given device, consumers may access the Internet through different networks. Increasingly, devices that were once specialized to either a broadband mobile network or for Wi-Fi communication are being used on both types of

---

[32] See CTAM, Multi-Platform Connected Devices Project, "Ownership and Viewing of TV Programs/Movies by Specific Device" (October 2012).

[33] Google, "The New Multi-Screen World: Understanding Cross-platform Consumer Behavior," (August, 2012) (available at http://services.google.com/fh/files/misc/multiscreenworld_final.pdf) (hereafter *Multiscreen World*).

[34] Aaron Smith, "17% of Cell Phone Owners Do Most of Their Online Browsing on Their Phone, Rather Than a Computer or Other Device," *Pew Internet & American Life Project* (June 26, 2012) at 2 (available at http://www.pewInternet.org/~/media//Files/Reports/2012/PIP_Cell_Phone_Internet_Access.pdf).

[35] "Mobile Phones and Tablets Now Account for 1 in 8 U.S. Internet Page Views," *comScore* (October 1, 2012) (available at http://www.comscoredatamine.com/2012/10/mobile-phones-and-tablets-now-account-for-1-in-8-u-s-Internet-page-views/).

networks. As discussed above, it is the destination content provider who is most likely to be able to link interactions that occur on multiple networks.

According to a recent comScore study:

> Until recently, mobile phones were the only devices supported by networks for wireless connectivity, confining the use of connected devices to areas with WiFi availability. Accordingly, the use of tablets and other web-enabled devices was predominantly fueled by WiFi connections at home and work locations. However, the growing availability of mobile broadband options and the proliferation of WiFi hotspots in public areas are changing the way people go online today. In August 2011, more than one third (37.2 percent) of digital traffic coming from mobile phones was attributable to a WiFi connection. This percentage grew nearly 3 points from the end of May 2011. On the other hand, tablets, which traditionally required a WiFi connection to access the Internet, are increasingly driving traffic using mobile broadband access. In August 2011, nearly 10 percent of traffic from tablets occurred via a mobile network connection. While tablet traffic coming over mobile broadband has only marginally increased in the past four months (by less than a percent), the general upward trend reflects the market's openness to greater mobile broadband use on tablets.[36]

Like the data on device usage, the comScore results highlight two important points. First, consumer browsing behavior is already highly fragmented; and, second, the degree of fragmentation is increasing rapidly as the number of available Internet access points grows.

(3) Multiple Browsers: Americans use numerous browsers to access the Internet, both on their desktop and laptop computers and on the different devices and networks discussed above. In October, 2012, Internet Explorer accounted for 41 percent of browser usage, followed by Chrome with 24 percent, Firefox with 18 percent, and Safari with 15 percent. Moreover, browser usage is subject to rapid change over time. Two years earlier, IE was 51 percent of the market, Firefox was 26 percent, and Chrome and Safari were each at 10 percent. In October

[36] "Digital Omnivores: How Tablets, Smartphones and Connected Devices are Changing U.S. Digital Media Consumption Habits," *comScore* (October 2011) at 2 (hereafter *Digital Omnivores*).

2008, only 4 years earlier, Internet Explorer had two thirds of the market and Chrome had less than one percent.[37]

A different set of operating systems (and browsers) are used on mobile devices. In August 2011, the Apple iOS operating system (and, likely, the Safari iOS browser) accounted for 27.3 percent of smart phone subscribers (versus 3.8 percent of browser usage on computers in the same month, and 4.3 percent in October 2012), compared to 43.7 percent using the Android operating system, and 19.7 percent using RIM. Microsoft accounted for 5.7 percent of the market.[38] By June 2012, Apple and Android had gained share at the expense of RIM (Blackberry), expanding to approximately 34 percent and 51 percent of the U.S. market, respectively. The share of the market accounted for by the RIM operating system fell to 9 percent.[39]

(4) Multiple Locations: Consumers also access the Internet from multiple locations, further limiting the comprehensiveness of any service provider's ability to comprehensively track a consumer. Data from the National Telecommunications & Information Administration shows that as of 2010, Americans connected to the Internet from multiple locations outside of their homes. For example, approximately 40 percent of respondents reported accessing the Internet from their home, 27 percent from their workplace, 11 percent from school, 1 percent from a public library, and 9 percent from an Internet café or coffee shop.[40]

---

[37] StatCounter Global Stats, "Top 5 Browsers in the United States from July 2008 to October 2012" (available at http://gs.statcounter.com/#browser-US-monthly-200807-201210).

[38] See *Digital Omnivores* at 15.

[39] See "Two Thirds of New Mobile Buyers Now Opting for Smartphones," *Nielsen Wire* (July 12, 2012) (available at: http://blog.nielsen.com/nielsenwire/?p=32494).

[40] United States Department of Commerce, National Telecommunications and Information Administration, "Current Population Survey (CPS) Internet Use 2010," Table 8 (available at http://www.ntia.doc.gov/data/CPS2010_Tables).

Access from multiple locations differs by device, and has likely increased since the NTIA data were collected in 2010. Google's study of multi-platform behavior found that 31 percent of daily media interactions that occurred via personal computers were outside the home. For smart phones, 40 percent of interactions were outside the home, and for tablets, 21 percent were outside the home.[41]

(5) Encryption: The growing use of encryption is directly relevant to the Commission's concerns about ISPs and, specifically the use of DPI technology: When transmissions are encrypted, no one except the recipient generally can look at the information contained in IP transmissions (packets).

SSL Pulse tracks implementation of Secure Socket Layer (SSL) encryption on more than 198,000 websites with valid certificates, just under 20 percent of the Alexa top million websites.[42] In 2011, Facebook made encryption the default for certain services after the release of a hacking tool that allowed snooping Facebook traffic on open Wi-Fi networks and impersonation of a Facebook user. Google and Twitter also moved to encrypt their sessions.[43] The trend toward more encryption is likely to continue. In addition to the need for encryption to protect security, the commercial value of information about users of a particular website provides another incentive for encryption.

To summarize, these five types of fragmentation – the use of multiple devices, use of a particular device on multiple networks, the use of a given device from multiple locations, the widespread availability and usage of alternative browsers, and encryption, – make it highly

---

[41] See *Multiscreen World* at 12-14.

[42] See "Trustworthy Internet Movement Picks SSL Implementation and Governance as First Initiative" (April 26, 2012) (available at https://www.trustworthyInternet.org/docs/tim-first-initiative.pdf).

[43] Mike Coward, "Encryption: Will It Be the Death of DPI?" *Telecoms.com* (n.d.) (available at , http://www.telecoms.com/39718/encryption-will-it-be-the-death-of-dpi/).

unlikely that any entity is in a position to comprehensively track online behavior. Moreover, the trends appear to be in the direction of greater fragmentation, not less, making the possibility of comprehensive data collection ever less likely.

2. Asymmetric Regulation is not Justified on the Basis of Concerns about Competition or Consumer Choice

The second basis upon which the *Final Report* expresses concerns is on the issue of consumer choice, especially with respect to ISPs.[44] Specifically, the Commission has requested comments on whether "there are sufficient choices among online products and services to give consumers meaningful options should they wish to avoid products or services that use comprehensive data collection."[45]

To begin, and as discussed immediately above, the fragmented nature of consumer Internet access means that there do not, as a factual matter, appear to be any "products or services that use comprehensive data collection," at least to the extent "comprehensive" is taken to mean the ability to compile a complete or nearly complete picture of the online activities of most consumers. This said, the question of consumer choice is an important one from a broader perspective, as it goes to the question of whether market forces – i.e., competition – can be relied upon to discipline the privacy practices ("comprehensiveness" included) of online service providers, and to promote better practices and support innovative new services. Choice also refers to the extent to which the market is producing an appropriately diverse set of options to satisfy the heterogeneous preferences of consumers.

---

[44] *Final Report* at 56 ("[I]t may be difficult for some consumers to obtain alternative sources of broadband Internet access, and they may be inhibited from switching broadband providers for reasons such as inconvenience or expense.").

[45] See *December 6 Workshop Notice*.

The first issue – the adequacy of competition to police online privacy practices – is part of a larger debate about the extent and effectiveness of competition in the Internet ecosystem as a whole.[46] As discussed further below, the markets for online services are characterized by dynamic competition among both firms and platforms (groups of firms producing complementary products), and there is powerful evidence that in such markets, firms that fail to meet consumer expectations, or affiliate with platforms that fail to do so, suffer swift and sure punishment in the marketplace.[47]

More specifically, the *Final Report* expressed concern about whether consumers have adequate choices among ISPs. In this regard, four points are worthy of note. First, as noted above, the notion that consumers conduct all or even a majority of their online browsing through a single ISP is incorrect: Most consumers use two, three or more access modalities, depending on their location and device. Second, even thinking narrowly about the choices available to consumers for home Internet access, nearly all households have access to two wireline providers and two or more wireless providers (and the numbers are growing). Third, and finally, the level of "churn" among ISP consumers demonstrates that they can and do exercise choice. According to the Federal Communications Commission, one out of six customers switch wireline providers

[46] For a review of the issues, see Jeffrey A. Eisenach, *Broadband Competition in the Internet Ecosystem* (American Enterprise Institute for Public Policy Research, October 2012) at Chapter 2. See also Howard A. Shelanski, "Adjusting Regulation to Competition: Toward a New Model for U.S. Telecommunications Policy," *Yale Journal on Regulation* 24 (Winter 2007) 55-105 and Joseph Farrell and Philip J. Weiser, "Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age," *Harvard Journal of Law & Technology* 17;1 (Fall 2003) 85-134.

[47] See e.g., Michael L. Katz and Howard A. Shelanski, "'Schumpeterian' Competition and Antitrust Policy in High-Tech Markets," *Competition* 14 (2005) at 10 ("Under the Schumpeterian view that competition consists of repeated waves of innovation that sweep aside 'dominant' incumbents, current product-market shares may indicate very little about the future of the industry or about whether any given firm will possess significant market power.") (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=925707).

every year, and 37 percent switch every three years;[48] for wireless, somewhere between a fifth and a third of all subscribers switch carriers every year.[49] To place these figures in context, wireless subscribers switch carriers approximately twice as often as they switch operating systems (e.g. from iPhone to Android or Windows).[50] These data indicate a level of competition and consumer churn that ensure that the privacy options offered by ISPs adequately meet consumers' needs, and to alleviate concerns that they 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.

The second sense in which choice is implicated in privacy issues is the extent to which the market produces a sufficient variety of choices to satisfy the diverse tastes of heterogeneous consumers. Product differentiation is one of the defining characteristics of dynamic markets, and markets for online services are highly differentiated, meaning that they offer a wide variety of choices which reflect both the costs of producing various product characteristics and the values consumers place on those characteristics.[51] As the *Final Report* notes, there is evidence that privacy is one of the dimensions on which online service providers compete,[52] and the diverse (and constantly improving) set of privacy protection options available in the marketplace suggests that this competition is effective.

---

[48] 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).

[49] See Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services: Fifteenth Report* (June 27, 2011) at ¶¶261-262 (available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-11-103A1.pdf).

[50] See Horace Dediu, *Measuring Mobile Platform Churn in the US Market* (Asymco, July 2011) (available at http://www.asymco.com/2011/07/12/measuring-mobile-platform-churn-in-the-us-market/).

[51] See e.g., Sherwin Rosen. "Hedonic Prices and Implicit Markets: Product Differentiation in Pure Competition," *Journal of Political Economy* 82;1 (January-February 1974) 34-55.

[52] See *Final Report* at 9 ("In addition, some companies appear to be competing on privacy. For example, one company offers an Internet search service that it promotes as being far more privacy-sensitive than other search engines.")

Certainly, there is no evidence documenting market failure or widespread consumer dissatisfaction with the privacy options provided by ISPs.[53] Indeed, there appears to be no question that they allow consumers multiple options for tailoring the ways in which their personal information is handled. In addition, and importantly, consumer choice is enabled by "add on" services as well as by integrated ones. For example, consumers can "choose privacy" by enabling security (HTTPS Everywhere) or by using anonymizers such as TORProject.org, which was originally supported by the U.S. government.[54]

Thus, to summarize, the evidence demonstrates that neither insufficient competition nor a lack of consumer choice provide a basis for departing from a functionality-based framework by imposing asymmetric regulation.

3. Large Platform Providers are Unlikely to Engage in Harmful Conduct

Large platform providers typically are large, publicly traded corporations with high levels of firm-specific reputational capital. As the Commission knows well, 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.[55] Moreover, there is empirical evidence that firms that fail to meet consumer expectations specifically with respect to online privacy suffer significant financial losses as a result.[56] Thus, the ability of the marketplace to discipline the privacy practices of large platform providers is supported by facts as well as theory.

---

[53] See e.g. *Broadband Decisions* at 3 (reporting that poor customer service – of all types, as the survey did not ask about privacy *per se* – ranks fourth out of five major reasons for switching ISPs).

[54] See https://www.torproject.org/.

[55] 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.

[56] Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security* 11 (2003 431-448.

In addition, unlike edge providers, ad networks and other online entities that have only ephemeral relationships with consumers, ISPs 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.[57]

B. Asymmetric Regulation Would Inhibit Innovation, Reduce Competition and Harm Consumers

Asymmetric regulation raises costs for some firms but not for their competitors or potential competitors. By insulating less-regulated firms from competition, or from the threat of entry, asymmetric regulation can be a source of monopoly power and all of its consequences: higher prices, lower quality and less innovation. The Commission should thus be extremely cautious about imposing regulatory burdens on some firms but not others.

With respect to the markets at issue here, prudence is especially appropriate. The markets for consumer information, online advertising, and digital content are part of the larger Internet ecosystem,[58] in which firms compete both directly, in the provision of comparable goods and services, and indirectly, through their participation in Internet platforms comprised of complementary goods.[59]

---

[57] 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.")

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

[59] 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

Moreover, competition in such markets is dynamic, involving rapid innovation generated through unrecoverable (sunk) expenditures on R&D or plant and equipment, which must be recouped through product differentiation and the resulting ability to charge prices above short-run marginal costs. Dynamic competition is often said to occur "for the market" rather than "in the market." That is, efficient outcomes result not from the presence of large numbers of existing competitors contemporaneously producing close substitutes, but rather from the ability of firms not presently "in the market" credibly to threaten entry. Regulations that raise costs for potential entrants but not incumbents are true barriers to entry which, by reducing the likelihood of successful entry, can have immediate adverse effects on market performance.[60]

Finally, in platform markets, firms in neighboring sectors are the most likely to have both the incentives and the capacity to enter. Thus, for example: Cable television operators entered the market for voice telephony; both telephone companies and e-commerce firms (e.g., Amazon) have entered the market for video; Google has entered the market for wireless devices (via its acquisition of Motorola) and is now entering the market for wireline connectivity (through its Google Fiber buildout in Kansas City, Kansas); Microsoft has entered the market for tablet computers; Apple is considering entering the market for Internet radio.[61] The list could go on, since entry (or the threat of entry) into markets for complementary products is central to the competitive dynamics of Internet platforms.[62] Regulations that disadvantage one type of platform participant (e.g., an ISP) relative to another (e.g., a content provider) thus discourage one of the most likely entrants into the latter's market.

Greenstein explain, "a firm in one layer [of the platform] has every incentive to grab the rents of a firm in another layer.").

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

[61] See e.g., Andy Fixmer and Adam Satariano, "Apple's Online Radio Service to Challenge Pandora in 2013," *Bloomberg News* (October 26, 2012) (available at http://www.bloomberg.com/news/2012-10-25/apple-s-online-radio-service-to-challenge-pandora-in-2013.html).

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

The prospect for privacy regulation to have such effects is well-recognized. 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 greater consolidation, something that usually works against maintaining robust competition.[63]

Thus, asymmetric regulation that limits the ability of some firms to collect or share information can harm competition in two ways: (1) by inhibiting direct entry by the regulated firms into downstream markets; and (2) by preventing the regulated firms from providing the inputs (in the form of consumer information) that would allow other firms to enter.[64]

The potential harm from limiting entry by ISPs and other potential competitors into the market for online advertising is significant. First, the market for online advertising is characterized by relatively high concentration and, for the last few years at least, stable market shares, as shown in Table 1 below. To be clear, we are not expressing an opinion on any specific regulatory or competition issues regarding these firms or this market. Our point is more fundamental: Over time, the performance of such markets is directly related to the ability of potential entrants to police market conduct, *whether or not* entry actually occurs.

---

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

[64] Commissioner Rosch has expressed this concern regarding "do not track" mandates. See J. Thomas Rosch, *Advertising Age* (March 28, 2011) (available at http://www.ftc.gov/speeches/rosch/110328offtrack-donottrack.pdf) ("Finally, the implementation of do-not-track mechanisms must not jeopardize competition by injuring potential competitors. I am concerned that some firms with a monopoly or near-monopoly on a relevant market may use do-not-track mechanisms to cripple competitors from constraining their power. More specifically, the browser market is heavily concentrated. Most – though not all – firms in the browser market operate for profit and those firms monetize some of their other businesses by advertising. There is nothing wrong with that as such. But we need to know: 1.) whether any of those firms enjoy monopoly or near-monopoly power in any online advertising market; 2.) whether there is any difference between the advertising in which those firms are invested (including the various kinds and combinations) and the advertising portfolio of competitors that may make the latter more vulnerable in the event do-not-track mechanisms are installed; and 3.) whether there is any other way that a firm that dominates the market may be able to disadvantage a rival if do-not-track mechanisms are adopted.")

TABLE 1:
ONLINE ADVERTISING MARKET SHARES, 2010-2014 (PROJECTED)

Net US Digital Ad Revenue Share at Major Digital Ad-Selling Companies, 2010-2014
% of total digital ad revenues

	2010	2011	2012	2013	2014
Google	38.1%	40.1%	41.3%	42.6%	43.8%
Yahoo!	12.8%	9.6%	8.4%	7.5%	6.9%
Microsoft	5.7%	5.7%	6.0%	6.6%	7.2%
Facebook	4.4%	5.4%	5.8%	6.3%	6.7%
AOL	3.3%	2.8%	2.5%	2.3%	2.2%
Total digital (billions)	**$26.29**	**$31.99**	**$37.31**	**$42.50**	**$47.77**

Note: includes advertising that appears on desktop and laptop computers as well as mobile phones and tablets, and includes all the various formats of advertising on those platforms; data through 2011 is derived from IAB/PwC data; net ad revenues after companies pay traffic acquisition costs (TAC) to partner sites
Source: company reports, 2012; eMarketer, Sep 2012

144451 www.eMarketer.com

Source: http://www.emarketer.com/newsroom/index.php/digital-ad-spending-top-37-billion-2012-market-consolidates/

Second, the online advertising market appears to be in the midst of a major shift associated with the rapid growth of mobile content and, as a direct result, mobile advertising. According to the Interactive Advertising Bureau, mobile advertising revenues increased between the second quarter of 2011 and the second quarter of 2012, from $344 million to $611 million, representing a substantial increase in mobile's share of the online advertising market, from 8 percent to 12 percent.[65] Rapid growth is expected to continue: SNL Kagan projects that U.S. mobile advertising revenue will increase by at least 40 percent annually for each of the next three years.[66] The rapid growth in mobile advertising appears to be causing disruption in the online advertising industry, posing challenges for market leaders such as Facebook (which attributes

[65] See *IAB Report* at 12.
[66] SNL Kagan, *Mobile Advertising Revenue* (2011).

some of the decline in its post-IPO valuation to its slow start in mobile advertising)[67] and Google (which, despite its 95 percent market share of mobile search advertising, is experiencing falling profits partly to "slowing ad-sales growth rates due a shift to less-profitable mobile ads"),[68] and creating an opening for new entrants (such as Pandora Radio, whose mobile ad revenues grew by 476 percent between 2010 and 2011, and which now ranks fifth among all mobile ad networks).[69]

IV. CONCLUSIONS

U.S. privacy policy has long recognized that certain types of information, and certain uses of that information, appropriately call for enhanced scrutiny. This functionality-based approach appropriately targets attention to areas where consumer harm is most likely to occur, and hence where the potential benefits from oversight are greatest. Consumers benefit from a functionality-based framework because it allows them to form consistent expectations about how data will be treated which are valid across platforms and contexts, rather than trying to learn different rules for every circumstance. Unlike regulatory approaches tied to particular business models or technologies, a functionality-based framework provides flexibility in the face of technological change, reduces consumer confusion, and creates a level competitive playing field that fosters the innovation consumers have come to expect from online service providers. Concerns about comprehensiveness and choice, or about large platform providers and ISPs, do

---

[67] See Ina Fried, "Facebook: We Weren't Moving Fast Enough in Mobile," *AllThingsD* (October 19, 2012) (available at http://allthingsd.com/20121019/facebook-we-werent-moving-fast-enough-in-mobile/?KEYWORDS=mobile+advertising).

[68] John Letzing and Evelyn M. Rusli, "The Upside of Google's Mobile Ad Push," *The Wall Street Journal* (October 19, 2012) (available at http://online.wsj.com/article/SB10000872396390444868204578067101716321238.html?KEYWORDS=mobile+advertising).

[69] SNL Kagan, *Mobile Advertising Revenue* (2011). The top four are Google/AdMob, Apple/Quattro, Yahoo! and Twitter.

not provide a basis for imposing an asymmetric privacy framework based on technologies or business models. Doing so would harm both competition and consumers.