THE UNIVERSITY OF CHICAGO
THE LAW SCHOOL
1111 EAST 60TH STREET
CHICAGO • ILLINOIS 60637-2786

RANDAL C. PICKER
PAUL AND THEO LEFFMANN PROFESSOR OF COMMERCIAL LAW
SENIOR FELLOW, THE COMPUTATION INSTITUTE

TELEPHONE: 773-702-0864
FAX: 773-702-0730
r-picker@uchicago.edu

February 18, 2011

Donald S. Clark, Secretary
Federal Trade Commission
Office of the Secretary, Room H-113 (Annex W)
600 Pennsylvania Ave., N.W.
Washington, DC 20580

RE: FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

Dear Secretary Clark:

I attach comments that we ask to be considered in the Commission's evaluation of the draft report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (the "Report"). The students in my Winter, 2011 Technology Policy seminar at the University of Chicago Law School blogged about the Report as part of our readings this quarter. We discussed the Report and their posts in class and students then reconsidered and rewrote their posts to file them with the Commission.

Like most professors I suspect, I find my students to be thoughtful, passionate and remarkably engaging. They are full of ideas and it seemed a shame to not put those ideas before the Commission. As you undoubtedly understand, these are their ideas, not mine. I say that not to evade responsibility but to make sure that credit is assigned appropriately.

Sincerely,

Randal C. Picker

S. James Boumil III, The Need for Comprehensive Privacy Norms[†]

I. Two Distinct Problems

The Commission faces two fundamental problems in crafting a set of guidelines, norms or laws that effectively protect consumer privacy on the Internet. The first is that Internet users' privacy preferences appear to vary substantially. To the extent that not implementing individual preferences imposes real costs on consumers, an ideal regulatory regime should accommodate variety to the greatest practical extent.

A second, unrelated problem is that data collected for one approved purpose may often easily be used for another unapproved purpose. Therefore, policing the spectrum of uses of consumer data is much more complicated than simply restricting the types of data which can be gathered initially. Because the number of potential uses will only increase as technology advances, eliciting appropriate consent as to these uses poses significant new challenges.

II. The Costs of Greater User Control

In responding to the first problem, one might start by trying to afford individual Internet users as much control as possible over their information—both in terms of what can be collected and how it can ultimately be disseminated and processed. But this approach suffers from both practical and theoretical drawbacks. One practical drawback is that increasing customizability will almost necessarily entail greater administrative costs—both in terms of companies' implementing privacy regimes and consumers' learning to navigate them. One theoretical drawback is that implementing individual users' preferences may not yield the socially efficient outcome—i.e. the social value of collecting and using consumer information may be greater than the cost to consumers of providing it.

Greater user control becomes even harder to implement in the face of the second problem. It is all but impossible to predict how a user might respond to a potential data use which nobody could have predicted at the time of collection. Furthermore, eliciting consent after the fact would prove in the best case a huge annoyance and in the worst case a practical impossibility.

III. A Call For Standardization

All of these drawbacks beget greater standardization. Specifically, the Commission should develop a "Reasonable Privacy Expectations" (RPEs) model, or a comprehensive set of norms which would specify all approved uses of potentially gatherable information. This system would ideally be instituted directly as a law, but could also be branded with a trademark, akin to a governmental seal of approval which websites would be free to license if their policies abided by the RPEs.

Standardization will (1) lower the total costs of implementing and policing privacy regulations, and (2) produce greater clarity about the levels of privacy Internet users can expect

[†] BS Physics 2009, Yale University, JD Candidate 2012, The University of Chicago Law School.

under various circumstances. This will empower them to better understand the implications of their choices on the web, and they will in turn be much more able to adjust their behavior accordingly to effect their own preferences. Moreover, the RPEs can evolve dynamically in response to the ever-growing list of uses which technological advancement will spawn, so that users will need only to pay attention to a single source for an iteratively more well-defined picture of what constitutes reasonable privacy practices on the web.

The tradeoff in applying a broad framework to a varied group of consumers is that it may not adequately respond to everyone's preferences. This is the same tradeoff which privacy laws governing offline contexts face. In all other contexts, the law solves the problem by simply deciding when one does and does not have a reasonable expectation of privacy. In every other case, the costs of customization make it practically impossible to implement a customizable regime. If the Internet in fact changes this, certain opt-out procedures could be installed for people who strongly desire to use them. But without conducting the sort of empirical study that would be necessary to define costs appropriately and balance the tradeoff more precisely, my inclination is to think that most busy people will not care much to resist a set of reasonable privacy norms calculated to cater either to the "average" consumer or to implement the "socially efficient" level of privacy expectation.

IV. Conclusion

The Commission should implement a standardized, clear, dynamic set of RPEs governing appropriate uses of consumer data collected online. Under this regime, consumers would be better empowered to understand what expectations of privacy they have under various circumstances. In turn, they will be much better able to understand the implications of their online choices for their data privacy, and will then be able to adjust their behavior accordingly to effect their own preferences.

Kyle Dolan, The Price of Privacy[†]

I. Introduction

The FTC Privacy Report suggests a broader goal of increased notice and consent requirements for consumers, as well as meaningful choice with respect to online privacy. This policy objective places an increased burden on the "ad networks, ISPs, carriers, operating system vendors, software application companies and other organizations that collect Personal Identifiable Information (PII) and sell it to third parties for marketing and behavioral targeting without identification of the collection." Much has been made about the anticipated impact of requiring consent for varying types different data mining and the potential shift this could cause in our conception of online privacy and what rights consumers have when using information technology. The potential market impact is the proper lens for analyzing any negative impacts of the potential FTC Policies, which is why I suggest developing future policy in conjunction with the DOC's recommendations in the Green Paper.[1]

As I understand the FTC's Report, the most recognized forms of data use (targeted advertising) will not be subject to increased FCC protocol.[2] Thus, as the classic example goes, if I purchase razor handles, the company will still be able to offer me blades at a discounted rate. The report refers to these as "commonly accepted practices" for which consent is not needed. This is a logical conclusion, because we allow and expect for this in the context of shopping at a grocery store where we will receive checkout coupons, etc. Therefore, the report is mainly concerned with privacy measures in place for tracking browsing preferences and mining data from social networking sites, etc.

While protecting privacy is ostensibly desirable, as one of the appealing aspects of the internet is the anonymity, requiring informed consent will come at a cost. As it currently stands, privacy interests are not protected with users clicking through a series of lengthy and confusing disclosures in exchange for unfettered access to programming. The report explicitly stated that that the FTC does not want to impact consumer choice through these new requirements, instead it desires a broader range of more meaningful consumer choices. Thus, the FTC envisions, the user will be able to select from a host of options that will use their data in different ways (that will be explicitly spelled out to the user at the outset.)

The FTC Privacy Report does not offer much in the way of take it or leave it approaches that consumers may be faced with. The possibility of meaningful choice strikes me as a doubtful possibility. The market would provide for such options, if demand were truly present. While my position neglects the FTC's obvious point that consumers would prefer a choice if they knew

[†] BA Political Science and Criminology 2009, The Ohio State University, JD Candidate 2012, The University of Chicago Law School.

[1] http://www.ntia.doc.gov//reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[2] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, 53 (2010).

what their data would be used for, I am more inclined to follow the DOC logic in the Green Paper. In specific, the Green Paper recognizes that the entire digital market has grown around use of consumer data in advertising. A vast overhaul of this system could have disastrous effects. Thus, the Green Paper urges adoption of FIPPs (a sort of Electronic Bill of Rights for Consumers.) This would allow consumers to have a reasonable expectation of what their data will be used for, and allow providers to condition their business protocol on practices that they know are acceptable. Further, it would meet the FTC goal of greater notice as there would still be mandatory disclosure for deviations from the accepted data uses. The Green Paper addresses my concern with the FCC recommendations, specifically that implementing a government mandated and complex scheme of notice requirements in order to maintain consent may do nothing more than further confuse consumers. Thus, a system of consistent principles makes sense as a way of insuring to consumers that, unless they hear otherwise, they can know exactly what to expect from the site.

The most important consideration in analyzing the Privacy Report is whether the FTC's policy mandates will address both consumer and corporation trust. While I laud the FTC's efforts to protect consumers, I think the situation in Europe provides a cautionary tale.[3] Generally speaking, providing regulations in a market that is currently evolving due to expansion and innovation will lead to problems with corporation confidence in the system. In 1997, then President Bill Clinton provided a general framework for government involvement with regulating the digital economy, expressing the aforementioned concern.[4] The most pertinent aspect of Clinton's proposal was his urging for minimal government involvement on the regulatory side, coupled with strict enforcement for violations of consumer trust. The private sector has clearly failed to address consumer concerns and provide for self-regulation. Involvement of the FTC should extend only so far as to spur industries to set up self-regulatory privacy systems upon which consumers and corporations can condition their expectations.

[3] See e.g., http://www.privacilla.org/business/eudirective.html.
[4] http://clinton4.nara.gov/WH/New/Commerce/summary.html.

Jesse M. Galdston, Privacy: At What Cost?[†]

As a general matter, I am a strong advocate of privacy and a proponent of extending the reach of laws and regulations that further personal privacy. As such, certain proposals within the FTC report on consumer privacy were, at least initially, music to my ears. The most notable proposal contained within the report is the "Do Not Track" list, something that would be akin to the well-known "Do Not Call" registry.[1] Other, less noteworthy, privacy enhancing ideas within the report would create more transparent privacy policies,[2] would require more specific forms of consumer consent to uses of personal information,[3] and contemplates the creation of a standardized opt-in or opt-out regime.[4] Additionally, while recognizing the utility of things like targeted advertising and other benefits achieved by consumers through the use of their personal data, the report seems to spend a great deal of time lamenting the amazing aggregation of information about consumers that can be easily obtained by data brokers and potential advertisers without any meaningful understanding or consent from consumers. As I mentioned earlier, my intuitive response to these proposals, really any proposals that increase privacy and control of personal data, is positive. However, in thinking about the economy of the internet and the way in which much of the content that I appreciate and enjoy is heavily if not totally reliant on advertising revenue, I want to at least contemplate the idea that, as a society, we may be living in a world in which we can no longer afford the price of privacy as we have known it in the past.

I am voracious consumer of the written word and, for the past couple of years, the vast majority of those words have appeared on a screen and have been transmitted to me, in the form of blog posts, news articles, and posts on message boards, over the internet. Blogs, newspapers, and message boards have at least one thing in common: they are all supported almost entirely, so far as I know, by advertising revenue. The percentage of GNP composed of advertising revenue has remained relatively constant for a significant period of time.[5] However, the number of outputs chasing those advertising dollars can only have proliferated to a massive extent with the advent and widespread use of the internet.

It seems relatively clear that advertising, over the long haul, can only support so much content on the web, as it could only support so many print publications before the internet. In the print age, subscription and circulation numbers served as a rough proxy with which advertisers could choose which consumers to target. However, as should be clear, these were, inevitably, rather crude proxies and they must have along with logistical difficulties such as

---

[†] BA, Wesleyan University 2006; JD Candidate 2011, The University of Chicago Law School.

[1] https://www.donotcall.gov/.

[2] See, e.g., FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (hereinafter FTC Report) at 69.

[3] See FTC Report at 76.

[4] See FTC Report at 59.

[5] See, e.g., http://www.econlib.org/library/Enc1/Advertising.html ("Advertising as a percentage of GNP has stayed relatively constant since the twenties at roughly 2 percent.")

language barriers, differing legal regimes (tariffs, speech restrictions or the lack thereof, etc.), put a limit on the variety of content available to consumers of the printed word. Unlike in the print medium, the internet provides advertisers with many more sophisticated tools with which to understand their consumers and target those consumers with advertisements. The main raw material utilized by those tools consists of personal information about those potential consumers: their location, their habits, their interests, their age, etc. Thus, those very same tools that so massively infringe on our privacy also allow advertisers and content producers/providers to maintain the vast array of content concerning all sorts of different subject matter.

To circle back to the beginning, I worry about the degree to which private information is used by data brokers, sellers, and advertisers on the internet. However, given the value that I (not to mention many others) place on the variety and quality of content available on the internet. I believe it is time for those who would categorize themselves as reflexively pro-privacy to reconsider whether greater privacy is worth the potential trade-off of less diverse and less worthwhile content, especially in "marginal" or non-mainstream, relatively poorly well-supported areas of interest. I believe before the imposition of any new regulations or advocacy of new policies in the privacy realm, the FTC should take seriously the second-order benefits (as opposed to "first-order" benefits enjoyed by consumer like those I mentioned in the first paragraph) to consumers created by more effectively targeted advertising. As such, I would be in favor of imposing measures that have no obvious effect on the ability of advertisers to effectively target consumers. One example is the imposition or use of clearer and more easily understandable privacy policies (perhaps some entity like the FTC should have a regulatory mandate to impose such changes unilaterally in the way that it is anticipated that the new Consumer Financial Protection Bureau will[6]). On the other hand, without extensive research into the effects on the internet advertising market and, further, on the likely outcome such changes would have on the content available on the internet, I would oppose things like the Do Not Track list, despite my strong normative priors in favor of privacy enhancing measures.

[6] http://www.npr.org/blogs/money/2010/09/22/130049045/elizabeth-warren-i-didn-t-want-to-be-in-a-pumpkin-shell.

Jacob Hamann, Problems Inherent in Mandated Disclosure Regimes[†]

In the privacy report, one of the FTC's main tools in their effort to strike a balance between protecting consumer privacy and preserving the benefits of data gathering is a mandated disclosure regime it calls the "notice and choice" model. The FTC proposes that outside of a set of commonly accepted practices, such as product fulfillment and fraud prevention, companies would have to enable consumers to make informed and meaningful choices about whether to allow the company to collect their online data. The report also calls for businesses to provide greater transparency about their data practice by issuing privacy notices and providing consumers with access to the consumer data that the business maintains.

The report recognizes that the notice and choice model has been less than completely successful in the context of internet privacy, noting that businesses have been providing "long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[1] This is a major, longstanding problem and it is good that the FTC report recognizes it. The authors of the report hope to combat this problem by replacing long, incomprehensible privacy notices with simple, streamlined ones. The authors of the report point to the Gramm-Leach-Bliley act as a model as well as calling for input from the academic community to accomplish this goal.[2]

In I would like to direct the commission's attention to the work of two academics who recently surveyed the field of mandated disclosure regimes and whose findings cast doubt on the possibility of simple, easily comprehensible privacy policies. In their paper, *The Failure of Mandated Disclosure*, Omri Ben-Shahar and Carl Schneider argue that it is difficult for regulators to design workable disclosures because there is a constant tendency for regulators, often inspired by anecdotal 'trouble stories,' to mandate disclosure too broadly, and for the disclosees, more concerned with protecting themselves from lawsuits than informing consumers, to resist the mandate.[3] This combination leads to long, incomprehensible disclosures and the accompanying cries for simplification.

Unfortunately, simplification is really, really hard because, as the author's point out, complexity cannot be explained simply—"Sophisticated vocabularies and professional languages encapsulate complex thoughts. If only simple words can be used, everything must be lengthily spelled out."[4] Even if the overload problem can be solved by simplified forms, the FTC's proposed privacy disclosure mandate cannot be looked at in isolation. Consumers are barraged

---

[†] B.A. 2005, University of Notre Dame, JD Candidate 2011 The University of Chicago Law School.

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, iii (2010).

[2] Id at 71.

[3] Omri Ben-Shahar and Carl E. Schneider, *The Failure of Mandated Disclosure*, *23, 34 (University of Chicago, The Law School, John M. Olin Law & Economics Research Paper No. 516, 2010), online at http://www.law.uchicago.edu/Lawecon/index.html (visited Feb 14, 2005).

[4] Id at 43

with disclosures when engaging in almost any transaction-- from using the bank to buying food. This leads to what the authors call an accumulation problem that won't be solved by adding one more simple disclosure to the heap of complex ones.[5]

Disclosure regimes attempt to solve the problem of consumer's lack of information, but ignore the problem of consumers making bad choices in spite of possessing accurate information. The FTC report recognizes this is a problem for teenagers, noting that teens are "heavy users of digital technology and new media, but may not always think clearly about the consequences of their actions."[6] The report seeks further comments to address this problem. According to Ben-Shahar and Schnieder, most of us are not too different from teens—"few people can (or want to) develop finely calibrated preferences in the often-technical mandated disclosure areas quickly and accurately enough to use in making decisions. Few have the ability to identify the fine distinctions about their own preferences and the tradeoffs among them in those technical areas that are subject to many of the disclosure mandates."[7]

In summary, in order for a mandated disclosure regime to work effectively, the authors suggest that regulators will have to overcome the overload problem by simplifying complex concepts into easily understandable language. In addition, they will have to deal with an accumulation problem posed by the proliferation of other disclosure regimes. And finally, this disclosure will somehow have to triumph over a rationally ignorant public who would prefer to be told what to do rather than be given the information and asked to investigate and choose for themselves. Given these difficulties, it might make sense to rely less heavily on the notice and choice model when designing a privacy policy.

[5] Id at 38.

[6] Federal Trade Commission, *A Proposed Framework* at 62.

[7] Ben-Shahar and Schneider, *Failure of Mandated Disclosure* at 50.

Tamara Hill, Enforceability Concerns[†]

The two privacy frameworks currently used by the FTC are the "notice and choice" and "harm-based" approaches. Both approaches raise a number of concerns. But even integrating them into a broad framework won't solve one essential problem: enforcement.

I. Limitations of Notice and Choice

For notice and choice, simplicity, consumer comprehension, and the actual effectiveness of the notice are baseline considerations. If the consumer can't understand the notice (or doesn't think that understanding is worth the time it would take to do so), no real choice can be made. But even if the consumer understands the notice, the choice may not be meaningful. Future development of information use, negative externalities, or limited options (e.g., the mandatory applications installed by Verizon on my Android phone) prevent the consumer from offering fully informed consent.

II. Limitations of the Harm-Based Approach

For the harm-based approach, the limited types of harm considered and the nature of the technology industry make it less useful in protecting online privacy.[1] The harm-based approach only deals with problems after the fact; in an industry of rapid growth and evolution, protecting information too late is often the same as not protecting it at all. (For identity theft, "[a] victim with an identity theft report documenting actual misuse of the consumer information is entitled to place a 7-year alert on his file," as compared with the usual 90 day alert, which indicates how difficult it is to protect information after it has become public.)

In creating an integrated framework, the FTC acknowledges that the two former models are incomplete and proposes a broader scope, incorporating simplified notice, expanded choice, consumer access to their mined data and required security measures. The FTC also discusses a Do Not Track concept that follows the idea of the "Do Not Call" registry—but instead of adding the consumer's name to the list, the consumer inversely adds the list to his name by downloading blocking software on his computer.

III. Do Not Track Approach and Enforceability

Other commenters herein discuss some of the problems with a binary Do Not Track list and the negative externalities of an opt-out system promoting free-riding. But it seems that despite these problems, the Do Not Track list has one major factor in its favor: enforceability.

The FTC acknowledges that enforceability is an issue for its proposed policy. ("The Commission also identified enforcement – the use of a reliable mechanism to impose sanctions for noncompliance—as a critical component of any regulatory or self-regulatory program."[2])

[†] B.S., Physics, Santa Clara University, 2003; J.D. Candidate 2012, The University of Chicago Law School.

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, 20 (2010).

[2] Id at 7.

Beyond discussing its past enforcement practices, however, the FTC provides no information on how it plans to enforce its new policy. It discusses enforcement of past policies and asserts that it plans to use Section 5 of the FTC Act to enforce the new framework. But the FTC acknowledges that while violations of the "notice and choice" and "harm-based" approaches likely constitute violations of Section 5, many of the other proscribed act in the framework do not. For cases where notice is adequate, "consumers have generally not had any choice other than to 'take or leave it,' and that choice has never been considered to be a Section 5 violation unless what was represented in the notice was different than what was actually done in practice."[3]

IV. Enforcing Compliance for Internet Activity is Particularly Challenging

Even if the FTC's new framework is entirely enforceable (and within the agency's statutory right to regulate), how does it plan to do so? The FTC cites to its prior enforcement actions, including the Spyware enforcement actions around 2006; while they effectively stopped the targeted enterprises, I'm pretty sure not a single computer user decided that 2006 was a good time to uninstall their anti-spyware programs. The CANSPAM Act, which required that spam emails comply with certain rules, is ineffective and unenforced: neither the FCC nor the FTC believes that targeting spam companies with lawsuits is an effective use of their time. Will targeting third-party advertisers with tracking cookies be different?

Instead, I propose broadening the regulatory reach. Companies that track and sell data, such as social networking sites, mobile phone application designers and web-based companies in general, should be targeted by the framework; but include internet browsers and mobile service providers in the action. The Do Not Track list allows consumers one type of screen to keep information private.

V. A Multi-Pronged Approach Is More Likely to Be Successful

Internet browsers, which the FTC does not include in the privacy report, offer another screen on consumer privacy. Mozilla's No-Script offers another; both Mozilla and Microsoft are offering no-track features in future browser updates. (Google has little incentive to offer this feature in its Chrome browser – sales of Google Analytics, AdWords and other targeted marketing, like Gmail content-specific ads – would be hindered.) Browsers already provide warnings for expired security certificates or sites that claim and fail to offer security – providing simple icons that communicate the browsers' view (including script and cookie functions) can provide privacy information even for sites that have no motivation to comply with the FTC's regulations on their own.

[3] Id at 61.

Julia Horwitz, Privacy Icons[†]

I. From the Report

The Report takes on the problem of consumer choice by segregating out data that falls under the category of "commonly accepted practices." By this, the Report means that certain kinds of data are essential to the functionality of the Internet, or "obvious from the context of the transaction."[1] Therefore, "the consumer's consent" to transmitting that data to the first-party developer "is inferred."[2] These data fall into roughly two categories – legal rules and regulations (fraud prevention and legal compliance), and customer service (first-party marketing, internal operations, and product and service fulfillment).

The Report recommends that consumers should have the choice as to whether or not to transmit all other kinds of data.[3] It encourages online businesses and social media websites to provide consumers with a "clear and concise" explanation of their data practices,[4] which should take place after the consumer has visited the site, but before she has entered any data (other than, presumably, the subdirectories the user has visited; the number of navigation decisions she's made within the site, etc.). The roundtable panelists suggest that an "opt-in" or "opt-out" procedure would be effective, although they are not certain which would be most effective.

II. The World Wide Web Consortium's Workshop

In July of 2010, W3C[5] hosted its Workshop on Privacy for Advanced Web APIs, at which they reviewed papers and proposals for developing new and better web privacy models. Two of these reports – one by Aza Raskin on behalf of Mozilla[6]; and one by Alissa Cooper, the Chief Computer Scientist at the Center for Democracy and Technology[7] – seem to converge on some real possibilities for obtaining meaningful consumer consent. They drew on the work of Creative Commons, which allowed a user to choose her copyright license for anything she might publish on the internet, and to express it through a set of simple, intuitive icons[8]. Why shouldn't this work for privacy, as well?

If every site were tagged with a privacy icon, a user could tell immediately the extent to which her data was being stored and utilized. Under the Report's proposed data classification

---

[†] B.A 2008, Brown University, JD Candidate 2012, The University of Chicago Law School.

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, 54 (2010).

[2] Ibid.

[3] Id at 57.

[4] Id at 58.

[5] http://www.w3.org/.

[6] http://www.w3.org/2010/api-privacy-ws/slides/raskin.pdf.

[7] http://www.w3.org/2010/api-privacy-ws/slides/cooper.pdf.

[8] http://creativecommons.org/licenses.

system, a user would consent to "commonly accepted practices" (CAP) by default, and then would be faced with a choice as to the distribution of the rest of her data. This system still leaves some gray area, though. Should a user assume that every site is necessarily keeping track of her CAP data? The Report also notes that some websites will have different standards for CAP data than others, depending on the service they provide. Should a user be able to infer from the nature of the site how much of her CAP data is being stored? Together, the Raskin and Cooper reports present a two-step approach to meaningful consumer consent and choice, which provide one possible resolution to these questions.

A. Step One: The Privacy Icon

One might imagine a privacy icon on every webpage (not just every site, but every page). This can't be a popular suggestion—so much of the internet's appeal lies in its non-uniformity. When the alternative, however, is invisible data mining of user information, the idea of a basic, easily-understandable icon on every page might actually be reassuring. The privacy icons would work like a more sophisticated MPAA rating system – an icon would stand for a small, well-defined set of data. CAP data, for example, might have an icon indicating that some combination of "rules and regulations" data and "customer service data" is used. Each website could then display its default privacy settings on every page. That way, simply by opening a website, a user could tell instantly how much data the site is collecting, and whether she needs to proceed to step two.

B. Step Two: The Drop-Down Bar

In step two, the user could have the opportunity to exert some control over how much of her data is actually used. The default privacy setting would let her know generally what kinds of data are at stake in her web browsing, but (like the MPAA rating) would encompass a number of possible combinations of data. In the Privacy Page (modeled on Cooper's drop-down bar idea), a user could adjust her privacy settings within the parameters of the site's "rating." This allows for much more control on the part of the user, who could choose, for example, how much of her data can be distributed to "affiliates" (as the Report points out, there could be "hundreds of affiliates"[9]), or how long the first-party developer could store her data.

III. The Economic Effects

I imagine this privacy system would have pro-competitive economic consequences, as many users would put a high premium on high levels of privacy. Online businesses would have to choose their privacy default with an efficiency formula in mind. If a business offered the highest privacy default, it would certainly lose money due to its inability to sell user data on the sly. However, it would also stand to gain a better reputation among users for being a "safe" business (as the Report mentions), and could attract more consumers, who would otherwise be afraid to submit their financial information online. Furthermore, a business could price the value of its privacy icon into its products. That is to say, a site might find it more profitable to show a low

[9] FTC Report at 26.

privacy setting and sell cheaper products, since it would not have to sacrifice the "invisible" business of data sales.

Vineeth Narayanan, Negative Externalities of Enhanced Choice[†]

I. Introduction

Like most people, I value my privacy including my private information on the web, but, like most people, I'm not sure *how* much I value it. I know that I care whether my social security number or financial information is disclosed to those who may use it to cause me economic or physical harms. In addition, I know that I care if that information is disclosed to people I know or will know with the effect of causing reputational harms. It seems clear to me that the vendors of goods and services online are the least cost avoiders in these transactions, so the burden of regulation should fall on them. The only challenge, then, is to find the optimal level of regulation.

The FTC's proposed framework for consumer privacy regulations tackles the lofty goal of guarding against these harms by adopting a structure of rules that promote better notice regulations and, importantly, more consumer choice. The first of these proposals I consider a welcome change. Existing rules have resulted in long, complicated disclosures that few consumers actually read. The new approach envisions lower requirements for "commonly accepted" practices and more streamlined requirements for the more unusual uses of private information. It will allow consumers to focus on uncommon privacy policies when they arise instead of being buried in language they may see from many other vendors. I also agree with the commission's conclusions concerning the harm-based approach, which essentially depend on the deterrence effect from targeting specific instances of privacy violations that result in physical and economic harm. Though bad publicity from an information disclosure can be devastating, given how attenuated the privacy violations usually are from the vendors who solicit the information, it's hard to believe that the harm-based approach alone can minimize privacy-related harms.

II. Identifying Negative Externalities

The second component as put forth by the proposed framework, more consumer choice, is where I take issue with the Commission. The enhanced provisions are two-fold. First, the framework calls for greater context and simplicity at the point of decision-making for the consumer. Second, the framework proposes a do not track list for those who wish to opt-out of the online behavioral advertising scheme, which creates consumer profiles to create a more targeted advertising experience. The report seems to justify the need for additional consumer control by pointing out that "when given the opportunity, [consumers] will take active steps to protect [their privacy]."[1] They cite the many consumers who choose to change privacy settings on social networking sites or delete cookies from their browsers. However, the report goes on to concede that whether consumers take the necessary step to protect privacy depends on the ease of

[†] B.A., Physics, University of California Berkeley, 2006; JD Candidate 2011, The University of Chicago Law School.

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, 29 (2010).

the process. "For example, someone who takes the time to change his settings on a social networking site, or check that his online shopping is secure, may not be willing to devote comparable time and effort to figure out how to protect his online browsing activity[.]"[2] This observation seems to drive the report forward toward the enhanced standards put forth in the framework but what strikes me immediately is that there is another conclusion to be drawn: individuals may not value privacy enough to take those extra steps to protect it. It may be argued that when it's easy to enhance privacy protections, individuals are not driven by a rational desire to defend against harms but perhaps motivated instead by notions of protecting ones name without understanding the actual likelihood of the reputational, physical or economic harms.

Moreover, what is missing from the individual's calculus is the negative externality that the decision to opt-out of consumer data collection schemes may cause. As the FTC itself notes, "The growth in mobile and social networking services in particular is striking, and is funded, in part, by the growth of targeted advertising that relies on use of consumer data."[3] The data that is collected from individual searches goes toward identifying patterns, thereby making the advertising model more lucrative. Without such a model, these vendors, which essentially allow consumers to purchase their goods at marginal cost, will have to rely on other, less optimal, pricing models. In this way, every consumer that decides to withhold their data decreases the value the vendor may retrieve from advertising and creates a negative externality for the rest of the users. For individuals at the point of the decision to either allow or prohibit the use personal information, the benefit they see from more targeted advertising is far removed and the evils of using personal data are exaggerated. The result is that every user will likely choose to opt-out and not allow the vendor to use personal information.

Thus, making decisions more contextualized and simpler or offering a simple mechanism to opt out of behavioral advertising (Do not track) is somewhat dangerous because it allows people to make the easy choice for them to opt-out of the regime, without heeding the negative externalities caused by that decision. And though I agree with the FTC that existing notice regimes are unwieldy they may provide a kind of natural barrier around these advertising schemes that, in the aggregate, deliver positive results to consumers. The solution then might be to keep things the way they are with the understanding that "reasonable security for customer and employee data is well-settled."[4] Thus consumers may rely on consumer watchdogs to point out vendors who abuse data but otherwise need to take additional steps to protect private information when the choice is not easy.

III. A Proposal: More Consequential Choice

But even if the FTC moves forward with the proposed framework, I suggest making the consumer choices more meaningful. As it is now, if consumers are able to opt-out of privacy policies, the report suggests that they should still be permitted to use the service. ("Regardless of

[2] Ibid.

[3] Id at 21.

[4] Id at 45.

the specific context, where the consumer elects not to have her information collected, used, or shared, that decision should be durable and not subject to repeated additional requests from the particular merchant."[5] I propose that instead, just as a shop is not required to turn off their security cameras for some, the choice to opt-out of the consumer data collection scheme should result in the consumer not being able to use the service. This way the people who do submit their data are not cross-subsidizing those who choose not to and they see more downside consequences to deciding to opt-out of the regime. Furthermore, I suspect, people don't value privacy enough to not use the services and for those that do, companies can truly compete on privacy policies by tying their product to those policies. If consumers are able to opt-out while still using the services, paid for by consumer data advertising dollars, they are not really allowing the vendors to compete on privacy policies because, in effect, they can choose their own.

IV. Conclusion

My proposal mainly serves to emphasize two main points that I urge the Commission to address: (1) there are negative externalities that result from enhanced consumer choice; and (2) consumer choice as contemplated by the proposed regulations may not adequately account for these externalities. Understanding the tradeoff between low cost online content and privacy is essential for creating an optimal framework for consumer privacy. For me, until we get to this point, I'm okay with a little less privacy policy and a little more free content.

[5] Id at 59.

Joseph Parish, Should We Really Care that Much about Online Privacy?[†]

Please suspend your disbelief and disregard any facts you might be aware of concerning the actual history of evolution, and imagine the early human race before it had eyes. One day, a prehistoric human invents eye-sight. It isn't long before it catches on and soon everyone is spending countless hours just watching stuff. There are even support groups for eyesight addiction. The most pervasive problem, though, is that now everyone can see what everyone else is doing. We all know who went where, and who is flirting with whom, and what kind of leaves they use to clean up. This is all very private information that people are embarrassed to suddenly have out in the open. Naturally, there is a clamor for rules and regulations that control what people are allowed to look at, and who they are allowed to tell about it. Given the lack of any system of government outside of natural law, nothing happens. However, people soon become accustomed to certain activities being public (anyone can find out, but nobody cares how much Nutella I eat in a month) and figure out ways to hide other information (build an outhouse).

This is similar to the situation we are in with internet privacy. The biggest problem I see with the FTC's privacy report is that it assumes that information should be kept private just because people want it to be private. They state that privacy technologies "should be proportionate to the ... sensitivity of the data at issue." This creates an infinite number of gradations of privacy because everyone places a different value on the privacy of certain information. The FTC also wants businesses to have "greater transparency" with privacy notices that are "clearer, shorter, and more standardized," and stakeholders who "educate consumers about commercial data privacy practices." You just can't account for the varying sensitivity of data, and have privacy notices that are clearer, and shorter. Making privacy technologies proportionate to the sensitivity of the data is in opposition to shorter, clearer privacy notices. But even if you could do both, you simply can't force people to know and understand how their private data is used.

The reality is that there is certain information that is naturally public. Information generated through online activity is that kind of information. Our real world walking-about and shopping behavior is open to be witnessed by any number of people. For the most part, people have no problem with this. People need to get used the fact that certain behavior online can be witnessed by any number of people. Most information generated online is free to be used by whoever is there to see it. I'm comfortable with this because most people just don't care what I'm doing online enough to collect and use that information. But Amazon.com does, and they can use that information to my advantage.

Now, there is certain information that can cause direct harm to people in the wrong hands: social security numbers, credit card numbers, bank account numbers, and to a lesser extent, phone numbers and email addresses. This should most definitely be kept private, but none of this information is generated by online activity. And the sensitivity of this information is

[†] B.A 2008, Brown University, JD Candidate 2012, The University of Chicago Law School.

so clear that we already have mechanisms in place to keep it secure. They aren't perfect, but will surely get better.

In conclusion, the FTC would be extremely unpopular if they excluded all but the most private information from protection. But I don't think they should preempt the development of potentially valuable information industries by granting privacy rights to information that is naturally public. We stand at the dawn of a world economy where information will be the most highly-traded good. People will become accustomed to certain information being used for advertising or other revenue generating purposes. And if they want to keep that information private, technology can, and probably will provide a way for them to do so on an individual basis. We don't yet know all the ways information will be used either for good or bad. So it doesn't make sense to cut off access to this information before we know the trade-off.

Jaime I. Puyol Crespo, The FTC's Role on the Development of Privacy Terms[†]

I. Balance Between privacy and the Evolving Needs of Commerce

The FTC report assumes as a principle that the privacy of consumers has to be balanced with the needs of the data collection business.[1] The idea is that data collection justifies sacrificing privacy because it benefits consumers through "free" services such as online search, behavioral advertising and social networking. The conveyance of data implies a trade-off between privacy and free content/services.

The contract that is celebrated each time a consumer agrees to share info with a data collector has to adequately reflect the above-mentioned balance between consumer's privacy and business development. As in any contractual relation, a balance will exist only if both parties can reasonably regard the values exchanged as equal. In contracts that involve the collection and commercial use of data, the consumer makes several concessions such as differences in the amount of data collected; allowed uses of data; and conveyance of data to third parties. In order to arrive to contractual equilibrium or balance, these concessions should be proportional to the benefits that the consumer obtains.

II. A Need to Develop Standardized and Balanced Terms

In theory each party will try to maximize its benefits from a contract, being this true only for freely bargained agreements. This maximizing behavior ensures the conciliation of both sides of the bargain allowing a balanced outcome. Therefore, there is not only a need for standardized and easy to understand terms as the report notes, but also of developing a balance over the requirements of each party, as would occur in a free bargain.

All the agreements that allow the use of personal data are contracts of adhesion, on which no real negotiation takes place. In the absence of consumer's bargaining force, the law should act in behalf of consumer to ascertain the prevalence of the stated balance. However it is impossible for the law to figure out how much of the consumer's privacy is sacrificed in each one of these contracts. Thus, a catalog of standardized terms of privacy and data conveyance could be a solution to keep the balance, but only if these terms are designed keeping proportionality in mind.

III. The Role of the Data Collectors

How much of my privacy should Consumers give away in order to reach a fair balance between privacy sacrificed and what it is obtained in exchange?

Consumers are giving away personal data in exchange for something. This something could be a free service, a free program or the desire to be targeted by personalized advertising. Online advertising funds many of the free information and services available on the web, and this

---

[†] L.C.J.S. 2007, Universidad de Chile; LL.M Candidate 2011, The University of Chicago Law School.

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, 3 (2010).

kind of advertising relies on data collection. In order to get free benefits, consumer pays off with their personal data. From this perspective alone, resigning to all these benefits may be too high a price to pay for privacy.

Data collectors are an intermediary between consumers and advertising companies. Intermediaries act as hubs that centralize the collection and management of data away from consumer's control. As the report acknowledges consumers don't know and cannot control the use of data by third parties.[2] However, the fact is that at the present stage of the web development, third parties are needed, as intermediaries between Consumers and Providers. Consumers don't have other direct means to manage their profiles and make them available exclusively for the purposes that they want.

IV. Conclusion

The above-mentioned balance will not forcefully derive from the market's response. The Commission has a key role in the developing of a catalog of standardized and balanced terms. The Data Collectors would have the option to choose between them. Fairness in the terms would be guaranteed by the approval of the Commission.

Also, the Commission should encourage the development of alternative business models such as identi.ca[3] or diaspora*[4] that could still offer similar services to the current "free" ones without risking Consumer's privacy. These models aim to develop decentralized social networking services, taking privacy as a main concern. They allow consumers to limit the information they want to share, keeping their data in their own hard drives and managing their own profiles. At the same time, these services will potentially offer comparable benefits, such as information sharing, social services and so on.

[2] Id at 73.

[3] http://identi.ca/.

[4] https://joindiaspora.com/.

Julian Russo, Exploring the Ill-Defined Anxieties over Online Privacy

Reading the FTC Privacy Report brings to mind an argument I had with a friend nearly a decade ago. My friend was praising her father for at once demanding the discounts that membership in his grocery store's "value club" made available while adamantly refusing to be taken advantage of by giving over personal information like his address and phone number. I tried to make the point that the grocery store might be trading the discounts for that very information (or more likely, to track her father's purchases), but that approach had no purchase with this particular friend and the conversation devolved pretty quickly.

This anecdote suggests that neither the trade of consumer information for consumer benefit nor the consumer misunderstanding or lack of awareness of that trade are novel phenomena. What is novel is the context of the Internet. In the grocery store context, we might have expected that in an efficient market a strong enough consumer demand for a particular balance of "privacy cost" and downstream benefit would have resulted in stores providing that particular balance point as either a sole option or one among several (so, perhaps the ideal trade for my interlocutor's father was to divulge his general neighborhood location for fewer benefits but not his particular address for more benefits). To the extent that stores never did this (and, indeed, I think they have not), it seems this must be either because there is not enough competition to force them to meet consumer demand, the consumer demand is not actually very high, or consumers are uneducated and do not realize the implications (whether deemed positive or negative) of their participation in the value club.

As[*] we switch from stores tracking purchase behavior and matching it up with an address to the Internet context, what exactly changes? Why is this of such interest now, but it wasn't when CVS did it ten years ago?

Ideally, the market would provide a solution for the privacy questions that the FTC is trying to solve with its proposed framework. On the one hand, the Internet seems like it would enhance competition among businesses so that to the extent privacy is something consumers care about, competition might drive policies toward some optimal level in a way that competition among drugstores or grocery stores might not (it takes a lot more for me to go to a store farther away from my house than to simply abandon one website for another). That, at least, would suggest that privacy considerations should need less government protection online than offline. Indeed, the FTC report notes that "consumer outcry caused companies such as Google and Facebook to change the privacy practices related to their social networking tools after launching new products and features."[1] This also suggests that consumers online seem to care more about their privacy than they did when they were just joining the value club at a physical store location.

So, we have online consumers caring more about their privacy and online businesses possibly being forced to be more responsive to those privacy concerns than businesses for which

[*] BA 2005, Cornell University, JD Candidate 2011, The University of Chicago Law School.

[1] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policy Makers*, 51 (2010).

geography is an important factor. However, strongly weighing against this, and in favor of more serious consideration of privacy policy today than ever before, is the incredible volume, as the FTC summarizes, of private information flowing around on the Internet and the fact that the (hopefully) value-creating use of this information funds much of the free or subsidized online services consumers enjoy. Simply put, the stakes of the privacy game are higher today on both sides of the counter. This is not just about tracking produce purchases and receiving a few cents saved on the dollar, this is about tracking *everything* and receiving services for *free*!

What has remained constant, and where I think the FTC is very appropriately attempting to play a role, is the dearth of consumer awareness and understanding. It would be hard to imagine my friend's father getting enraged if someone outside the grocery store had explicitly offered him money in exchange for information. If my friend and her father understood "value club membership" this way, they would have been less angry (usually a good thing) and better equipped to shop around for competing service if that's what they desired. To the extent that the FTC policies such as those guiding simplified norms for notice will promote a commercial atmosphere of better educated consumers, mandating specific and potentially troubling options such as the "Do Not Track" proposal may not be necessary. My hope is that ensuring maximal transparency while enhancing consumer education and awareness will allow the online market to reach some acceptable equilibrium where consumers get a range of privacy options with proportionately subsidized service.

However, there are a few things to consider before gleaning prospective guidance from my value club analogy. First, value club membership is usually not a requirement of buying something at CVS while the online analog of such membership may very well be a requirement of using an online service. Secondly, today, refusal to participate in the online marketplace of services that use private information is becoming increasingly similar to refusing to use airlines because you disagree with the invasiveness of TSA security screening. It is literally true that "one does not have to fly," but this is not practically true. And if it is not now the case, then it likely will be in the future that it is similarly *not practically true* that one can thrive in our society without relying on Internet services that deal in private consumer information. What this means is that we should be weary of blind faith in a market filled even with educated consumers (or faith in the results from multiplex decisions by consumers and businesses) to deliver a satisfactory balance of privacy for subsidy since consumers are increasingly strapped in for the ride without meaningful alternatives. If it were up to "the market," there might very well be a few discount airlines/airports that specialized in low cost, low-security, fast-lane air travel. But, collectively, we think that would be a bad idea (even without factoring in the externalities resulting from plane crashes this would seems foolish), so we try to set what we think are reasonable security policies. If privacy is completely left up to "the market," we might get results that are similarly unsatisfactory even though it results from what consumers apparently demand by enthusiastically consuming the least expensive services.

The first step to an ideal regime of privacy protection will be informing consumers and Internet users of the trade-off they are necessarily making. The second will be empowering them in making that trade-off. In essence, this brings us to the notice and consent problem: no one

reads privacy policies and they probably won't read changes to one either. Therefore, those regulating in the interest of the public must ask themselves the following question: what are the purposes for which private data are used that citizen consumers are so anxious about? As I try to answer this question I come up with four categories:

1. Spam/annoyances in one form or another
2. Identity Theft/Economic Harm
3. "Creepy people" finding out user habits and embarrassing, blackmailing, or otherwise threatening/harming user
4. Government curtailing counter-majoritarian or unpopular political movements, speech, and activism (the "Big Brother" anxiety)

For me, the first category is simply not a big deal. It seems the second category could (and should) be dealt with by criminal law and enhanced technical protections like encryption. If setting new privacy norms will help mitigate identity theft, that's great, but I do not believe that the threat of identity theft is what lurks behind the public's amorphous and ill-defined fears of burgeoning access to private information.

The third and fourth categories listed above seem, to me, to get closer to what irks people about use of their personal information because they are characterized by *the unknown* — also known as *the spooky creepy unknown.* Why wouldn't I or anyone else want Amazon tracking all the books I buy, movies I watch, and mailing and billing addresses I've had? Am I *really* scared that Amazon is going to get *too good* at selling things to me? Or that they'll sell the information to a third party advertiser who will be *too good* at targeting me with promotions that might tempt me? Plainly, this is not what I worry about. I have a hard time believing anyone fears this.

When Amazon deleted copies of *1984* and *Animal Farm* from its Kindle, people jumped at the opportunity to delight in the poetic creepiness of the event. But, significantly, *1984* is about *the government* trying to *control* the behavior of its *citizens* to some extent by destroying their privacy. Today's debate over online privacy seems to be predominantly about allowing *businesses* to *respond* to *consumer* behavior by… to some extent destroying their privacy. Most people don't seem to care that Google searches through their emails because (at least right now) most of us believe Google is truly just trying to make money by getting revenue from people trying to sell things to the user. Once/if businesses like Google start making deals with one government or another, or one political group or another, or one creepy blackmailer or another, to *share* user information, people like me will get strongly chilled from using their services to the extent we can find substitutes. Note that I say this as a person with basically mainstream tastes and majoritarian political values. The threat would be much more alarming if I actually had unpopular tastes and beliefs. Nonetheless, I have been taught to get anxious when the government or a particular political group starts tracking what books a person reads, and perhaps asking why they read them. It is not insane to think, and may be myopic to categorically deny, that in a different political climate Amazon or Google Books might one day sell or turn over the

history of books I am reading or web searches I have made to someone who would then use that information to discredit me or an organization I belong to in a political campaign of some kind.

I do not see an adequate exploration of the concern that a business will have an unforeseen incentive, be it financial or legal, to hand over information it collected about its users to the government or powerful political actors that desire the information for reasons not linked to business development or more efficient marketing. I think the failure to discuss this issue is likely due to the unfortunate truth that it is difficult to discuss concerns like this without sounding far afield from the mainstream — that is to say, without sounding like the kind of person who might get labeled colloquially as a "nut". But if such *nutty* concerns are what are bothering consumers though they might not fully articulate it (consumers, it should be remembered, who are *also* citizens, that is, political beings), then we should be talking about those concerns clearly and taking those concerns seriously as we engage in this public discussion.

James Shliferstein, Increase Consumer Choice by Channeling Online Currencies[†]

I. The Challenge at Hand

Online data privacy poses a qualitatively different challenge than does traditional privacy. The archetypal *traditional* privacy concern is that someone is looking in your window or digging through your trash; the best lens through which to understand this activity is as a simplex tort or crime, since the spied-upon victim has in no sense assented to, nor profited from, the invasion. But the archetypal *online* privacy concern more closely resembles marketplace fraud or an unconscionable contract: the victim may indeed have been bamboozled in ways we find objectionable, but he (at least nominally) agreed to the transaction and got (at least something) out of it.

The latter category of regulation poses a more complex challenge. Our society is happy to ban more or less *all* trash-picking and window-leering—but in regulating online privacy violations, we distinctly want to *avoid* banning those transactions (however few) that have genuinely benefited both parties.

II. The Status Quo: Three Intermingled Currencies

Consumers demand content and functionality, and owners of websites can supply content and functionality. How, then, is the owner of a website to monetize the fact that she has something consumers want? Broadly speaking, the world has discovered three solutions to that problem.

The website-owner delivers her content or functionality in exchange for one (or more) of three currencies:

- At some websites, such as www.Lexis-Nexis.com, the consumer pays in **the currency of dollars**.
- At some websites, such as www.About.com, the consumer pays in **the currency of ad-impressions**. (That is to say, the consumer tolerates ads, in return for which the advertiser (who may or may not be internal to the website) pays the consumer's content bill.)
- At some websites, such as www.e-Rewards.com, the consumer pays in **the currency of private information** about himself. (Here, the consumer tolerates some loss of privacy, in return for which a marketing researcher (who likewise may or may not be affiliated with the website) pays the consumer's content bill.)

[†] BA Economics and Government, Cornell University, JD Candidate 2011, The University of Chicago Law School.

So long as all the parties to these exchanges are fully informed adults, none of these exchanges should be troubling. The problem that the Commission has correctly identified is that many consumers are especially unlikely to be well informed about the third currency of exchange. After all, the average consumer surely understands what it means to part with **dollars** in exchange for something he wants; doing so is a mundane and familiar part of offline as well as online life. And we are only slightly less comfortable with the practice of enduring **ad-impressions** in exchange for enjoyable experiences; nearly every American alive today has bought television in this manner for his entire adulthood. But the concept of paying for your purchases with **private information** remains somewhat alien to the American consumer, and remains mostly the province of online commerce (CVS ExtraCare Cards notwithstanding).

III. The Problem with the Status Quo: Ignorant Overpayment and Ignorant Free-Riding

The opacity of this new currency to most consumers takes two pernicious tolls. First, consumers may pay more than they realize—because they do not pay attention to what information *will* be mined from their browsers, or because they do not understand what information *can* be mined from their browsers, or because they do not realize how much the release of that information will cost them. Second—as Commissioner Kovacic discusses in his concurrence to the Commission's December 2010 staff report—they are susceptible to free-riding by savvier consumers. Those few consumers savvy enough to be aware of software that *prevents* data collection (such as by installing Firefox extensions, by blocking cookies, or by implementing a browser's "Do-Not-Track" feature), can obtain content effectively for free—knowing that the content they are skimming will probably nonetheless remain available, since website-owners will foist accordingly higher privacy costs on their unsavvy counterparts (and perhaps also knowing that at least a few of their unsavvy counterparts will be repelled by the resultant higher prices, meaning that their free-riding will reduce total consumption and inflict a deadweight loss).

Note that neither of these dangers is specific to the currency of **private information**. It is (unfortunately) commonplace (both online and offline) to wind up paying more **dollars** for an object, or viewing more **ads** while enjoying an experience, than you had quite realized you were signing up for. And it is possible for the savvy to free-ride on the unsavvy in these currencies, too. (Consider the credit card or travel club that supplies "bonus reward dollars" to attentive consumers, funding that subsidy by subjecting their irresponsible counterparts to higher interest rates or to large fees. Consider the effects of ad-blocking software or Tivo, both of which can offload one consumer's share of the ad burden onto other viewers.)

IV. A Solution: Three Segregated Currencies

How might we minimize the dangers of privacy overpayment and privacy free-riding, without also squelching those private-data-for-desired-service transactions that would genuinely be mutually beneficial? Rather than categorically blocking *all* expenditures in the currency of private information, and rather than setting absolute limits on the sensitivity of the information that may be collected (effectively a price cap)—the Commission might consider restricting only the *marketplace locations* where private information could be expended.

Imagine that instead of logging in to www.youtube.com, consumers learned to log into their choice of www.youtube-pay.com, or www.youtube-ads.com, or www.youtube-data.com.

- At www.youtube-pay.com, the consumer may view Youtube videos for $2.99 per month. It would be illegal for Youtube to collect consumer data or display ads at this version of their website, and naturally it would be illegal for the consumer to shirk payment.
- At www.youtube-ads.com, the consumer may view identical Youtube videos, flanked by a few ads. It would be illegal for Youtube to charge for this service or collect consumer data at this website, and it would be illegal for the consumer (or for third-party software acting on behalf of the consumer) to block the ads. (Since this most closely resembles the original service, perhaps Youtube might choose to redirect its old URL, www.youtube.com, to this sub-site.)
- At www.youtube-data.com, the consumer may view identical Youtube videos in exchange for the automated collection of some of his private demographic information. It would be illegal for Youtube to charge for this service or to display ads, and it would be illegal for the consumer to prevent information tracking at this sub-site.

Present regime:

	Credit card charge	Advertisements	Data collection
www.youtube.com	None	Yes, but some free-riding consumers block them, while others wind up watching more than their share.	Possibly? The average consumer is uncertain. If there is, then free-riders once again offload some of it onto the unsavvy.

FTC's Proposed regime:

	Credit card charge	Advertisements	Data collection
www.youtube.com	None	Yes, but some free-riding consumers block them, while others wind up watching more than their share.	Limited by law. Free-riding problem remains.

My proposed regime:

	Credit card charge	Advertisements	Data collection
www.youtube-pay.com	YES; consumer may not underpay.	Forbidden	Forbidden
www.youtube-ads.com	Forbidden	YES; consumer may not block.	Forbidden
www.youtube-data.com	Forbidden	Forbidden	YES; consumer may not block.

Certainly this regime would remain imperfect. We can conceive of some consumers for whom the optimal form of payment would have been some combination of multiple currencies, and some of these consumers might lose that option (although the market was already unlikely to offer the precise payment plan such consumers may have had in mind—and some such idiosyncratic consumers would still be able to cobble together their favorite mixed payment plan simply by alternating which sub-sites they visited).

But the simplicity and benefits of the regime would be substantial:

1. Consumers who didn't want to sacrifice any privacy...
    a. would be able to surf the Internet in full confidence that the law protected them against all incursions upon their privacy.
    b. would never need to read any complex privacy policies.
2. Consumers who *were* willing to spend some privacy...
    a. would be permitted to do so, to whatever extent they preferred.
    b. would be forewarned that they were giving something up, by the fact that they had to actively enter the special "-data" suffix before reaching the site.
    c. could become relative specialists in interpreting privacy policies (which could still be regulated for clarity).
3. Free-riding would effectively become illegal: savvy consumers would no longer be able to offload the price of their enjoyment of content onto unsavvy counterparts, inflicting at least some deadweight loss by doing so.

V. Conclusion

The solution I have laid out would expand, rather than restrict, consumer choice. As in the offline world, each individual consumer would choose how he most prefers to pay for his consumption. What the Commission would be introducing to the Internet would be another valuable feature that is natural to the offline world: as in the offline world, each individual consumer would have confidence that he was paying in his chosen currency and in no other.

Matthew Stoker, Exploring the Android Market as a Privacy Notice Model[†]

I thought one very interesting aspect of the FTC report was the proposal for reforming general privacy notice policy. The report highlighted that privacy notices have become so long and complex that they are virtually incomprehensible for the average consumer. As a partial solution to this problem, the report focused on a "notice-and-choice" strategy for ensuring consumer privacy protection and listed several aspirational ideals for privacy notices that would ensure they provide meaningful notice to consumers. These included standardizing notices and terminology, using widely comprehensible phrasing and focusing on user accessibility in aesthetic design.

In thinking about these aspirational goals, I decided to explore their fit with the Google Android Marketplace, a web application market widely used in several portable communication devices. The Android system runs applications independently of the underlying system, allowing the platform to use an individualized "permissions" mechanic to restrict which functions each application is allowed to access on a device. For example, if an application wished to send a phone's location to a cloud server for storage and processing, the application would need specific permissions to access the phones GPS receiver and access to the internet to send the coordinates to the cloud server. When downloading an application from the Android marketplace, a consumer is presented with a concise list of permissions which they must approve before the download is completed.

The permissions approval interface created by Google matches the FTC ideals in many ways. Because the Android software limits developers to approved permissions, many of the device and data uses sought by developers are standardized within specific software permissions. This system also allows Android to sort uses into categories which are intuitively easy for users to understand, such as "Your location" or "Services that cost you money." The use of predefined permissions and categories also allows the information to be provided in a concise and aestheticly accessible way even on small devices like mobile phones.

While the Android marketplace model demonstrates some ways in which the FTC privacy notice ideals could be implemented, it is far from a perfect model of effective privacy notices. Several news reports and academic papers have recently come out castigating Android applications for potentially improper uses of private data.1 These uses have included sending contact lists and location data to advertising companies through applications that do not intuitively relate to those services.

[†] BA Political Science 2008, The University of Michigan - Ann Arbor, JD Candidate 2011, The University of Chicago Law School.

[1] Scott Thrum & Yukari Iwatani Kane, *Your Apps are Watching You*, Wall St. J., Dec. 17, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html?mod=WSJ_hp_LEFTTopStories2010; Google Android Apps Found to be Sharing, BBC News, Sept. 30, 2010, http://www.bbc.co.uk/news/technology-11443111; William Enck Et Al., TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphone, *available at* http://appanalysis.org/tdroid10.pdf.

Part of this problem stems from the limits of using only concise privacy notices. Brief notices using broad terminology can cover both inoffensive and opprobrious uses without alerting users that they should be concerned. For example, programs that offer to send location data to local business to find specials may look acceptable, but could also cover sending all location data over long periods of time so those business could track users personal and spending habits. The model FTC privacy notices could address these problems by incorporating optional consumer access to longer specified descriptions of acceptable uses prior to registering user acceptance. Alternatively, the FTC could explicitly cabin the allowed uses for standardized terms to a very narrow set of defined uses and then employ enforcement actions to ensure meanings are not stretched to cover unexpected uses.

Another possible problem with the Android marketplace can be ascribed to the limits of notices that only cover direct uses. The Android marketplace is limited to informing users only of potential direct interactions from their device. This notification doesn't cover any further uses of consumer information once it has been sent from the device, such as reselling information to data compilers or combining information with personal data acquired from other sources. Creating a comprehensive table of secondary uses likely would be costly and rife with enforcement difficulties in the Android marketplace since it is managed solely by a single private company. However, FTC involvement could help ensure that developers accurately report secondary uses in the face of the additional deterrence of punitive regulatory actions.