Position Statement of the International Center for Law & Economics

Case Id: 12501e56-7148-485e-8f63-ae32c3c1a240

In the Matter of:

The Public Consultation on the Evaluation and Review of the E-Privacy Directive

International Center for Law and Economics
Geoffrey A. Manne, Executive Director
Kristian Stout, Associate Director for Innovation Policy[1]

July 5, 2016

Introduction

The Commission's interest in protecting the privacy of its citizens is commendable. This concern, however, should be well tempered by humility, and the Commission's ultimate decision should be guided by the understanding that contemporary technology and market innovations have afforded consumers a degree of choice unparallelled in the history of the European Union. While some firms may build their products with the requirement that consumers allow them to use personal information, others will not. And when consumers defect from products that do not meet their individual mix of privacy, price, and other preferences, firms will take notice and change their behavior accordingly.

This leads to another related point: innovation moves so quickly today that uniform prescriptive regulation intended to govern the behavior of many thousands of firms and millions of consumers is doomed to frustration if not

---

[1] Geoffrey A. Manne is the founder and Executive Director of the nonprofit, nonpartisan International Center for Law and Economics (ICLE), based in Portland, Oregon. He can be reached at gmanne@laweconcenter.org. Kristian Stout can be reached at kstout@laweconcenter.org.

outright failure. Moreover, broad regulations meant to bring industry to heel frequently work to the benefit of incumbents, driving out smaller competitors or making entry nearly impossible, only further narrowing consumer choices and guaranteeing less than optimal results for all of society.

With that said, there are certainly actions for the Commission to take that ensure a competitive environment in which consumer interests are adequately protected. Chief among these areas would be to enact regulations that control the damaging effects of costly data localization rules. Overall, however, the Commission would do best to leave much of the implementation of privacy regulations to the individual EU members who are most in touch with the challenges and desires of their own constituents.

Specific EU-level Rules Tailored For Electronic Communications Are Not Necessary to Ensure the Free Movement of Information or Full Consumer Protection

A tremendous value offered by modern business models, fueled by the incredible connectivity afforded by digital technologies, is that consumer choice is empowered by an unexpected and largely unforeseeable wave of competition among firms. Product cycles quickly relegate dominant firms to also-ran status as consumer preferences shift like quicksilver between product offerings. It is this dynamic process that has provided the greatest historical level of both innovation as well as consumer protection. Thus, the Commission should tread with care and humility as it considers privacy rules, as many of the proposals for the current Consultation could very well undermine the gale of creative destruction that has hitherto guaranteed to consumers the products and services they desire.

Concerns relating to online privacy have been extensively studied by regulators and others over the past two decades. By and large, regulators around the world have responded to these concerns with recommendations that combine a general case-by-case approach alongside tailored rules derived from the relevant information involved in particular areas of privacy concern. Creating blanket proscriptions without regard to actual particularized facts at a multinational level is nothing short of a recipe to ensure that innovation is chilled and consumer demand goes unmet, while also guaranteeing that large dominant firms capable of handling extensive regulation further dominate the economy.

Highly prescriptive rules that bind not only the various nations comprising the EU but also the untold number of firms operating within those nations, creates a privacy regulatory regime that is essentially disconnected from the collective wisdom of the scholars and policy makers that have been operating in this space

for decades. The overwhelming conclusion of this intense scrutiny is that there is no clear consensus about the proper way to deal with the intersection of innovative business models, online activity, and consumer privacy.[2] Ideal privacy regulations would evidence more restraint and assess trade-offs, recognizing that the authorized collection and use of consumer information by data companies confers enormous benefits, even as it entails some risks.

Although there may be virtue in trying to create a unified set of rules governing consumer privacy, there are simply too many important differences between the EU members and their populaces. Any attempt to impose a uniform set of privacy rules across the EU is bound to fail to properly assess the particularized costs and benefits facing members and their citizens.

There is a world of difference between a regulatory regime based on suggested best practices, industry codes of conduct and overarching consumer protection standards in which businesses are free to experiment and compete within the general limits of transparency, choice, data security, and consumer privacy, and a prescriptive regime that imposes aggressive constraints that fundamentally limit competition and choice across 27 different countries.

A key problem with the Commission's approach to privacy is that it allows the concerns of some highly privacy sensitive individuals to dictate the market realities for all consumers and firms. Such an approach harms consumers who do not view privacy protections through the same maximalist lens as the Commission. The net result of these rules is that, on the margin, consumers will be presented with a narrower range of options, in terms of both price as well as features, meaning that fewer consumers – who have a wide range of heterogeneous preferences – will be offered their preferred options. Consumer welfare will consequently decrease.

It is possible that the privacy-sensitive among us might be willing to pay for ad-free, non-tracking, or similarly restrictive versions of today's apps and other online services, just as it is possible that they would be willing to bear the cost of finding and using ad- and cookie-blockers. But the data show most people prefer to access apps, content, and services for free,[3] and don't care as much about

---

[2] *See, e.g.*, Peter Swire & Kenesa Ahmad, Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws, and Practices (2012).

[3] *See, e.g.*, Mary Ellen Gordon, The History of App Pricing, and Why Most Apps are Free, The Flurry Blog (Jul. 18, 2013), http://blog.flurry.com/bid/99013/The-History-of-App-Pricing-And-Why-Most-Apps-Are-Free; Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks (The Facebook Case)* (ACM Workshop on Privacy in the Electronic Society 2005), *available at* http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

privacy as they do about lower prices[4] except with respect to the most sensitive information (e.g., healthcare data, children's educational records) so long as the personal data they provide is secure and they get something of value in return.

In a world without transaction costs, it wouldn't matter how we chose to regulate online privacy and data security. The bargain struck between advertisers, content providers and users would result in the "right" level of sharing and use of behavioral data. But, in reality, there *are* transaction costs, and those transaction costs will directly bear both upon the choices that firms make in developing new services as well as the choices that consumers make in selecting those services

Further, the mere fact that a consumer's information may be used in ways that the user doesn't expect or understand does not mean that such use is harmful to consumers individually or in the aggregate. Whether such uses are desirable, or on net are beneficial or harmful to consumers, is an empirical question – one that has been extensively researched. For instance, when comparing opt-in and opt-out regimes, the evidence is decidedly stacked in favor or more permissive use of customer information:

> "Opt-in" is frequently portrayed as giving consumers greater privacy protection than "opt-out," and In fact, the opposite is true. "**Opt-in" provides no greater privacy protection than "opt-out" but imposes significantly higher costs with dramatically different legal and economic implications**.[5]
>
> **[T]he opt-out regime produces better welfare results than the anonymity regime, which in its turn is better than the opt-in regime.** Therefore, from a social welfare point of view, it matters whether opt out or opt in is adopted as the privacy standard.[6]

And the effects on competition of overly prescriptive privacy rules inevitably serves the interests of large incumbent firms. The seemingly marginal costs

---

[4] *See, e.g.*, Alastair R. Beresford, Dorothea Kübler, Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* (SFB 649 Discussion Paper 2011-010, 2011), *available at* http://ftp.iza.org/dp5017.pdf; Jens Grossklags & Alessandro Acquisti, *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, *in* Proceedings of Sixth Workshop on the Economics of Information Security (2007), *available at* http://weis2007.econinfosec.org/papers/66.pdf.

[5] *See* Fred H. Cate & Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In"* 1 (2003), *available at* http://home.uchicago.edu/~mferzige/fallacyofoptin.pdf.

[6] Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis Of Privacy Policies* 5 (CESifo working paper, No. 1831, 2006), *available at* https://www.econstor.eu/bitstream/10419/25876/1/521168813.PDF (emphasis added).

imposed on consumers by requiring particular privacy rules can have a significant cumulative effect on competition:

> [P]rivacy regulation imposes transaction costs whose effects… will fall disproportionately on smaller firms. **Consequently, rather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive**.… Under regulation, the extra costs required to obtain consent mean that in some cases where entry had been profitable without regulation, [some firms] will choose not to enter.[7]

Thus, on net overly prescriptive privacy regimes may tend to favor the status quo, and to maintain or grow the position of a few dominant firms. These broad regimes impose additional costs on consumers and hurt competition. In the absence of any meaningful evidence or rigorous economic analysis to the contrary, the Commission should eschew imposing a potentially harmful, EU-wide regime on firms operating within the Eurozone.

Further, it is not at all clear that consumers approve or disapprove of companies that rely upon the collection and use of consumer data. The Net Promoter Scores ("NPS") – a common metric that measures consumers satisfaction – indicates that, while some online companies that use consumers data have a below average NPS, others are above average.[8]

The Commission Should Carefully Consider the Costs Involved in Mandating EU-Wide Privacy Regulations

In the modern, global economy data is fast becoming the lifeblood of firms that have even modest amounts of technological connection with their customers and users. The increasing regulatory constraints imposed by governments around the world force a series of difficult decisions upon firms, the results of which are typically unforeseen and unintended by the regulators themselves – results that include a range of items from limitations on the scope of firm operations to choices regarding corporate structure. And these rules especially affect most profoundly platforms that by their nature cross national boundaries – a category that includes a diverse array of firms from search engines to payment services, to e-commerce sites.

---

[7] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. Econ. & Mgmt Strategy 47, 48-49 (2015) (emphasis added).
[8] Brian Iverson, *Maverick Research: The Unbearable Cost of Privacy*, Gartner Research (Oct. 1, 2015) at 43 *available at* https://www.gartner.com/doc/3140821/maverick-research-unbearable-cost-privacy

"[R]egulation often influences behavior in ways that differ from the initially stated rationale."[9] When regulations like the ePrivacy Directive increase the compliance and other costs associated with data collection and use, some firms will, at least marginally, alter their behavior to avoid the costs. This means that the choice of how to structure internal affairs is not solely dictated by consumer or competitive concerns, but necessarily includes strategies to reduce or avoid regulatory costs. Thus, to the extent that privacy regulation imposes a greater level of privacy restriction on firms than consumers would otherwise demand on their own, the costs become deadweight loss as firms adopt strategies that lower regulatory risks, costs, or provide greater predictability in the administration of their businesses.

When faced with these costs, firms will engage in a form of regulatory arbitrage as they face a choice between reducing regulatory costs on one side of the ledger, and increasing transaction costs on the other. When the costs of compliance become great enough, firms will rationally choose to engage in activity that otherwise would have been uneconomic:

> Deal lawyers routinely depart from the optimal transaction-cost-minimizing structure even though restructuring the deal reduces its (nonregulatory) efficiency. A corporation that needs cash might minimize transaction costs by entering into a secured loan, but instead, in order to improve the cosmetics of the balance sheet, enters into an economically similar transaction to securitize the assets. A company that would minimize agency costs by incorporating in Delaware decides that, to save on taxes, it will instead incorporate in Bermuda. So long as the regulatory savings outweigh the increase in transaction costs, such planning is perfectly rational.[10]

There are several important elements to consider when examining the costs of compliance for any regulatory regime.

The evidence about the efficacy of imposing a broad privacy and data regulation is at best mixed. On the one hand, the question of whether the "seen" or easily quantifiable costs of compliance justify regulatory intervention is a basic economic question, and one that should be answered by an empirical examination of costs and benefits (and decidedly not by conducting an opinion poll). A 2013 study by the Analysis Group indicates that the costs of compliance for small and medium enterprises in the

[9] Lee Benham, *Licit and Illicit Responses to Regulation*, in Handbook of New Institutional Economics (Menard and Shirley, eds.) (2005) at 591.
[10] Victor Fleischer, *Regulatory Arbitrage*, 89 TEXAS L. REV. 227 (2010).

eurozone would consume up to 40% of the organizations' IT budgets.[11] And in 2011, the Ponemon Institute estimated that multinational firms have on average $3.5M in compliance costs as a result of privacy regulations.[12]

On the other hand, the European Centre for International Political Economy estimated in 2014 that there existed negative impacts on GDP as a result of data localization legislation in seven different countries, and, within the EU, welfare losses to citizens amounted $193B.[13]

Worse yet, the harms that arise as a result of extensive privacy regimes are, rather predictably, not born by those who could most afford to bear them. Instead, as with many other regulatory interventions, it is the least well off who suffer disproportionately through reductions in wages and job losses.[14]

> The benefits and burdens of privacy protection are not distributed equally over rich and poor. Privacy protection is a superior (or luxury) good, which implies that the demand for it is not only a negative function of price but also a positive function of income and wealth. The rich want more privacy protection than the poor. Consequently, privacy law has a regressive income effect and hurts the poor who are required to cross-subsidize the needs of a rich privacy elite. The poor suffer disproportionately also where they already have less choice and pay higher prices than the rich. Take, for instance, consumer credit and lending. Due to privacy law's adverse effects on the free circulation of consumer credit information, loans or credit may no longer be available to the poor or only at substantially higher interest rates; the rich, on the other hand, may not be significantly affected by the restricted flow of their credit data. Privacy protection thus indirectly causes economic and social exclusion. Similarly, a move

---

[11] Laurits R. Christensen and Federico Etro, *European data protection: Impact of the EU data-protection regulation*, VOX: CEPR's Policy Portal (Mar. 24, 2013) *available at* http://www.voxeu.org/article/european-data-protection-impact-eu-data-protection-regulation.

[12] *The True Cost of Compliance: A Benchmark Study of Multinational Organizations*, Ponemon Institute (Jan. 2011) at 5 *available at* http://www.tripwire.com/tripwire/assets/File/ponemon/True_Cost_of_Compliance_Report.pdf.

[13] Matthias Bauer, et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, *European Centre for International Political Economy*, ECIPE Occasional Paper: No. 3/2014 at 2 *available at* http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf. It of course bears noting that these localization costs are precisely the sort of excess costs that a general EU regulation would possibly avoid, since these represent the costs that multiply when different countries have different rules. Thus, to the extent that the Commission opts to impose a data localization regulation, the net benefits could exceed the costs.

[14] Researchers also found a "substantial negative impact of the introduction of EU data-protection regulation on business and job creation." Christensen and Etro, *supra* note 11.

> from opt-out to opt-in in the catalog apparel sector would increase prices by up to 11% and those increases would disproportionally affect rural customers and those in less affluent city neighbourhoods. Unfortunately, these effects are not recognized, denied or at best downplayed by the various participants in the privacy debate.[15]

At the same time, a perhaps even more critical component, are the "unseen" costs that firms bear as part of an expansive regulatory regime, and which they consequently pass on to consumers in the form of higher prices and narrower options. One major aspect of these unseen costs are the ways that firms will structure their businesses to minimize the impact of legal rules.

Although privacy regulations are by intent, if not always in practice, consumer protection regulations, efforts by firms to structure themselves around regulations are not inherently efforts to "exploit" consumers. More accurately, such efforts are likely aimed at avoiding the practical problems that emerge as a consequence of applying general legislation to a heterogeneous set of markets, and difficulty that creates for firms trying to innovate and experiment.[16]

When firms rationally seek to avoid the costs associated with regulation, they necessarily must substitute prefered practices for alternative, less costly behavior (both in terms of euros, as well as legal implications), a substitution which is, by definition, a second-best (or worse) arrangement of all the factors of production.

This behavior could come in a variety of forms. Some companies will choose to collect and use less data as part of their operations, and others will be encouraged to restructure their operations in a manner that avoids regulatory burdens by, for instance, avoiding vertical integration when it is otherwise economical to integrate, or else creating various local divisions that are better able to comply with data regulations but that consume much more in overhead than would otherwise be the case. These firms may also opt to alter the geographic scope of the data they use, or else further allow legal jurisdiction to dictate the choice of where incorporation and principal business takes place.

Although opting for second-best choices is perfectly rational conduct for regulated firms, these second-best choices impose costs on society, both in

---

[15] Lucas Bergkamp, *The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 Computer Law & Security Report 31, 38 (2002).
[16] Campbell, Goldfarb, and Tucker, Privacy Regulation and Market Structure, 24 J. Econ. & Mgmt. Strategy 47, 48-49 (2015).

the narrow sense of the firm itself being necessarily less efficient, as well as in the broader sense that consumer welfare is diminished by creating a greater drag on the enterprises that serve society.

More specifically, it has also been found that privacy and data regulations can deter the entry of new competitors into markets,[17] a reality that further diminishes overall welfare in society by removing the competitive pressures that drive firms to innovate, economize and otherwise compete for consumer business.

The Free Movement of Data in the EU is Best Facilitated by Directives that Allow Member Countries to Act on Local Knowledge

"[P]rivacy is not reducible to a set of neutral conditions that apply to all matters we deem private"[18] and, consequently, privacy interests do not have a single value that translates easily across all contexts. The relative weight and contours of privacy interests are bound up in the relationship between firms and consumers. This necessarily implicates different countries (or even smaller geographic units) that have different cultures, consumer expectations, degrees of wealth, and the like. It is therefore, if not impossible, then a highly fraught exercise to conceive of a single privacy regime for all of Europe.

Although the EU has generally moved in the direction of opting for regulation of consumer data in the form of the General Data Protection Regulation, the Commission would be wise to withhold the application of a similarly monolithic privacy regulation to the fast-moving online world.

> Any sensible approach to regulating the collection and use of data will take into account the risk of abuses that will harm consumers. But those risks must be weighed with as much precision as possible, as is the case with potential consumer benefits, in order to guide sensible policy for data collection and use. The appropriate calibration, of course, turns on our best estimates of how policy changes will actually impact consumers on the margin, not whether we can identify

[17] See, e.g., *Id.* ("We show that such privacy regulation can preclude profitable entry by the specialist firm. Under regulation, the extra costs required to obtain consent mean that in some cases where entry had been profitable without regulation, the specialist firm will choose not to enter.... Overall, our model suggests that privacy regulation can alter the competitive market structure of data-intensive industries.").

[18] Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087, 1092 (2002).

> plausible narratives about how particular business practices might result in consumer harm.[19]

Each of the members of the EU presents an opportunity to "get it right" with respect to privacy regulation. The calibrations necessary in five years or even a year can be entirely unforeseen from the Commission's current vantage. As new uses of consumer data emerge, member legislatures are in a better position to evaluate the local knowledge of their constituents and more quickly amend their laws to both conform with an EU privacy directive, and also to answer to the concerns of their constituents.

Any efforts of the Commission to remove data localization rules are the right approach in that they open up competition among members along this dimension. An EU-wide regulation that creates proscriptive rules, however, would necessarily be far more general than what a member country is capable of creating, and, consequently, far less fitted to the reality on the ground.

Mandating Business Models Tilts the Playing Field in Favor of Incumbents and Ultimately Harms Consumers

There are any number of possible business that could both support the development of Internet services, and that use consumer data to lesser or greater extents, with correspondingly different levels of privacy protection offered. All of these models currently operate to greater or lesser success, however perhaps the most dominant to emerge is the zero-price model – at least for the time being. Surely there are paid services among these providers – for instance HushMail[20] provides a premium email services for those concerned with privacy – but the overwhelming majority are zero price.

And basic economic reasoning fairly explains this phenomenon, as well as the rise of subsidization through tracking and advertising sales:

> Due to the nature of information goods – high fixed costs for production, near-zero marginal costs and widely different values placed on the information by people – differential pricing is required to allow pricing based on consumer value. Having a free version of a service allows a service to attract even those customers for whom the marginal value of the network is almost zero. These are people who turn out to be more important to the network than the network is for

[19] Remarks of Joshua D. Wright, *How to Regulate the Internet of Things Without Harming its Future: Some Do's and Don'ts*, Federal Trade Commission (May 21, 2015) at 10 *available at* https://www.ftc.gov/system/files/documents/public_statements/644381/150521iotchamber.pdf

[20] *Enhanced email security to keep your data safe*, Hushmail *available at* https://www.hushmail.com

> them, because the larger network mass attracts other customers, some paying (such as advertisers), that can help to subsidize the cost of the network for those who derive the most value from it.[21]

The key insight here is that consumers prefer zero (or near-zero) price and on-demand, highly-flexible services. But the core of this is not that zero-price is the only model that work, but that firms are free to experiment with differential pricing, even where some models rely upon advertising and user-tracking. There is no single business method that will drive all platforms or that will remain dominant forever – even the ubiquitous zero-price models that are so popular today. In the same vein, there is no single method by which firms use data to deliver targeted marketing, or enhance consumer experiences.

And the market is the best disciplining force for correcting firms that stray from consumer preferences. Firms are driven by the profit motive, which is to say that if the non-tracking, privacy-oriented products that already exist were actually offering a service that consumers desired at a price they were willing to bear, those services would thrive, and the less privacy-sensitive options would be forced to shift their practices. No barriers to entry, regulatory impediments or the like prevent such services from operating or succeeding, other than, it seems, lack of consumer demand.

Competition is the single best mechanism of both discovering actual consumer preferences – for services as well as business and payment models – as well as guaranteeing that firms emerge to serve those preferences. Under a relatively free market where firms can experiment with business models, consumers will naturally gravitate to those options that best satisfy their particular price sensitivity and desire for service.

An *ex ante* requirement of a particular payment model, however, will in fact do much to discourage competition. As noted above, developing successful online platforms entails significant fixed costs; no magic switch exists to suddenly bring into existence a particular version of a software platform. Developments of successful platforms entails hundreds or thousands of hours of engineering time – and mandating a platform that consumers don't seem to prefer means devoting that time to developing what the market has demonstrated to be an inferior product. Thus, the returns to such development will necessarily be less than the returns to development of the primary, ad-supported product, and, consequently,

[21] Iverson, *supra*, note 8 at 44.

the ad-supported product will be forced to itself subsidize the legally-mandated paid version of the product.

For large, established platforms this cost can be (more or less) easily absorbed (depending, of course, on the underlying technology of the platform). But for startups such a regulatory obligation would amount to a significant entry barrier. In particular, the ability to gain critical mass for its service would be approximately significantly reduced as its upfront fixed costs will explode, and its users will be spread across multiple services. The net result will be less entry, and less-effective competition.

Imposing broad, general regulations regarding business models and privacy practices is a surefire way to curtail innovation and reduce overall competition. This inevitably will lead to a handful of large firms that are able to dominate a space as network effects will reinforce their success, and a lack of differentiation along privacy and advertising dimensions will discourage or outright forbid experimentation with novel business models.

The Commission Should Allow Consumer Demand to Guide Privacy Standards, and Rely Upon Mature Legal Regimes for Handling Instances of Consumer Abuse

Do Not Track

Do Not Track, an ostensibly benign technology, often works in a way that distorts competition without providing much in the way of the sought-after privacy protection goals.

As we have noted variously above, when regulatory standards are imposed they frequently redound to the benefit of the largest players in an industry, and work to retard the growth of (or outright exclude) smaller rivals. Do Not Track regulatory requirements are no exception. Do Not Track standards can be great for large organizations as the costs imposed upon smaller rivals are high enough to effectively inhibit competition.[22]

Do Not Track proposals, as they are popularly presented, are intended to prevent the use of third-party identifiers in behavioral advertising.[23] But, as in many other

[22] Alan Chapell, 'Do Not Track': Great For Internet Giants Like Google And Facebook, AdExchanger (May 29, 2014) available at http://adexchanger.com/data-driven-thinking/track-great-internet-giants-like-google-facebook/

[23] *See, e.g.*, Ceren Budak, at al., *Do-Not-Track and the Economics of Third-Party Advertising*, Boston U. School of Management Research Paper No. 2505643 (2016) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505643

area, prescribing the use of Do Not Track says nothing about how to architect such a system, nor do its proponents admit that such systems necessarily truncate user choices: who gets to determine the default settings for Do Not Track, who gets to define what counts as "tracking," and who gets to broker the exchange between users and sites when users actually do want tracking? Making these decisions in a regulation deprives consumers from arranging their options according to their own preferences.

And, crucially, if this standard were uniformly imposed upon the entire EU, the whole cost calculation for sites that currently have some mix of user tracking changes, which possibly destroys the justification for developing free services, or else creates a free-rider problem whereby users who opt-out of Do Not Track subsidize the use of consumers who do not do so.

Nicklas Lundblad and Betsy Masiello have aptly described the "opt-in dystopia" that occurs under a mandated Do Not Track regime.[24] An opt-in regime reverses the normal course of interaction between users and firms: they are forced to opt-in to a services before they can obtain adequate familiarity with it.[25] Opt-in regimes also incentivize services to maximize the amount of data they request under a given opt-in, in order to avoid making multiple requests to a given user.[26] This diminishes the user's overall understanding of exactly what is requested and for what purposes on any given instance. And, a harm that many otherwise pro-privacy advocates are sensitive to, opt-in regimes increase switching costs, which in turn increases the likelihood that service providers will become walled gardens.[27]

And the sort of proposal envisioned by the Commission's does nothing to prevent first-party tracking within services (nor should it), and serves largely to prevent new companies from intruding upon established firms' behavioral advertising territory.

Meanwhile, the market has developed a number of self-help mechanisms for those users who are particularly concerned with tracking and privacy. AdBlock Plus,[28] Ghostery[29] and related browser plugins are so effective at preventing third party (and first-party) tracking that many sites have begun to beg users to disable them when visiting their sites – and short of that are offering reduced fee versions

---

[24] Niklas Lundblad and Betsy Masiello,*Opt-in Dystopias*, (2010) 7:1 SCRIPTed 155 *available at* http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Surf the web without annoying ads!*, Adblock Plus *available at* https://adblockplus.org
[29] Ghostery *available at* https://www.ghostery.com

without the ad content.[30] Wired and other sites have actually moved to quasi-gated regimes in which visitors arriving at sites with ad blocking enabled are required (or requested) to pay for content.[31]

Allow well developed consumer protections laws to handle consumer abuses

At times, it is appropriate for regulators to examine particular companies, or even industries, when there is evident harm to consumers. Such scrutiny, however, is proper only when alleged consumers harms can be actually demonstrated, and when those harms are not adequately handled by the market, existing laws or regulations. Before proposing new regulatory mandates for handling perceived privacy and other abuses, the Commission should first make a thorough examination of existing antitrust and consumer protection law in order to discover the empirically observable legal gaps into which particularized harms actually fall.

The manner in which firms use data, and the extent to which such uses actually harm or help consumers, the efficacy of constraining data use, and, most importantly, the extent to which new regulations actually create a barrier to entry for new competitors are important questions that must be answered empirically.[32] This is particularly so as the real effects of privacy and data regulations vary considerably and in important ways across industries, and even between firms within particular industries.

Further, harms to consumers and competition are best addressed on a case-by-case basis, at least until it becomes clear that there is a consistent, observable negative effect arising from well-identified behavior, and that behavior can be effectively dealt with by ex ante regulation. Absent this approach, the error costs associated with over-enforcement arising from vaguely suspected and anecdotally supported "harms" threaten to do more harm than good, and reliance upon a mature consumer protection and antitrust regime provides a far better approach.[33]

If the Commission does in fact intend to proceed with an enhanced ex ante proscriptive regime, it is crucial that it first clearly define the actual harms it

---

[30] Jeremy Barr, *The New York Times Begins Testing Ad Blocking Approaches*, AdAge (Mar. 17, 2016) *available at* http://adage.com/article/media/york-times-a-message-ad-blockers/302995/

[31] *How WIRED Is Going to Handle Ad Blocking*, Wired (Feb. 8, 2016) *available at* http://www.wired.com/how-wired-is-going-to-handle-ad-blocking/

[32] On the other hand, one of the ways in which the firms use of data *is* consistent has to do with the widely distributed nature of the use. Thus, one of the rules of general applicability that would be well-applied here would remove data localization rules to the extent that they inhibit the ability of firms to operate efficiently throughout Europe.

[33] *See, e.g.*, Geoffrey A. Manne & Joshua D. Wright, *Innovation and the Limits of Antitrust*, 6 J. Competition L. & Econ. 153, 158-63 (2010).

observes or anticipates, and elaborate the manner in which existing legal regimes are insufficient to correct them.

The EU already affords its citizens an enhanced level of privacy and data security protection relative to much of the rest of the world.. Connected with these protections are robust antitrust laws and a well-developed commercial and contract law. Before imposing stringent new regulatory demands, the Commission should identify the exact failure points of its existing laws. Short of this, it is nearly impossible to recommend that additional privacy regulations be imposed upon firms in the EU.