

**Before the &
Federal Trade Commission &
Washington, D.C. &**

In the Matter of)	
)	
Competition and Consumer)	Docket No. FTC-2018-0098
Protection in the 21st Century)	
Hearings)	

**Topic 5: Competition and consumer protection issues in communication,
information, and media technology networks**

Comments of Mark A. Jamison

Following are the comments of Mark A. Jamison, Ph.D., on the topic of privacy in communication, information, and media technology networks. I am a Visiting Scholar with the American Enterprise Institute and Director and Gunter Professor at the Public Utility Research Center, Warrington College of Business, University of Florida. While I am honored to have these affiliations, my comments are my own and may not reflect the views of the American Enterprise Institute, the Public Utility Research Center, or the University of Florida.

Disclosure statement: I provided consulting for Google in 2012 regarding whether Google's search should be considered a public utility.

Introduction

Privacy has become an increasingly controversial topic. The growing use of unprecedentedly large and constantly updated databases – called big data – to study individual behavior has led to concerns that the lowering of computing and data storage costs will result in consumer harms. The revelation that Cambridge Analytica had used information collected about Facebook users in violation of Facebook’s policies and to the surprise of Facebook users, startled people worldwide. So did revelations that Google had scanned content of emails of Gmail users. More recently The New York Times (2018) reported that while Facebook is technically correct that it doesn’t sale user data, it does share the information and that the scope of this sharing and other data uses is beyond what typical users understand.

A typical reaction to these revelations is to think that users’ rights have been violated. An implicit premise in such reactions is that an individual has an inherent right to control what others learn or know about that individual. This belief underlies the European Union’s (EU) General Data Protection Regulation (GDPR), for example.

In my comments below, I provide an economic view of the privacy issue. I explain that there are diverse markets for information and that the varying characteristics of the market participants imply that one-size-fits-all regulations, such as the GDPR, harm both producers and consumers.

Economics Literature on Privacy

The economics literature shows that the diversity that exists across digital markets makes one-size-fits-all regulations harmful. Acquisti, Taylor, and Wagman (2016) provide an excellent summary of the economic research on privacy, focusing on “the economic value and consequences of protecting and disclosing personal information, and on consumers’ understanding and decisions regarding the trade-offs associated with the privacy and the sharing of personal data.” They explain that both empirical and theoretical research has shown that regulations controlling privacy can both help and harm individual and societal welfare. They also explain that research finds that, in digital economies, it is costly for consumers to make informed decisions about their personal information because of the number of decisions that would be required to make on a regular basis, the cost of their obtaining full understanding of how information about them is collected, for what purposes, and with what consequences.

The literature shows the particular danger of one-size-fits-all regulations for digital markets. Acquisti, Taylor, and Wagman (2016) identify this as the third wave of research. They explain:

Because so many transactions and activities, once private, are now conducted online, firms, governments, data aggregators, and other interested parties can observe, record, structure, and analyze data about consumer behavior at unprecedented levels of detail and computational speed (Varian 2010). As a result, the digital economy is, to a degree, financed by the organization of large

amounts of unstructured data to facilitate the targeting of product offerings by firms to individual consumers. For instance, search engines rely on data from repeat and past searches to improve search results, sellers rely on past purchases and browsing activities to make product recommendations, and social networks rely on giving marketers access to their vast user bases in order to generate revenues.

Taylor (2004) finds that, in the presence of tracking technologies that allow merchants to infer consumers' preferences and engage in price discrimination, the usefulness of privacy regulatory protection depends on consumers' level of sophistication. Naïve consumers do not anticipate a seller's ability to use any and every detail about their past interactions for price discrimination; consequently, in equilibrium, their surplus is captured by firms—unless privacy protection is enforced through regulation. Regulation, however, is not necessary if consumers are aware of how merchants may use their data and buyers can adapt their purchasing decisions accordingly, because it is in a company's best interest to protect customers' data (even if there is no specific regulation that forces it to do so).

Acquisti and Varian (2005) demonstrate that consumer tracking will raise a merchant's profits only if the tracking is also used to provide consumers with enhanced personalized services.

Information disclosure is therefore not always harmful to the individual and may contribute to improving the welfare of all parties involved. Moreover, in line with Taylor (2004), companies may be inclined to develop their own privacy protection policies for profit-maximizing purposes, even without the intervention of a regulatory body. Conitzer, Taylor, and Wagman (2012) confirm these findings.

More recently, Baye and Sappington (2018) confirm that the impacts of regulations can vary greatly with context. Focusing on online shopping platforms, such as Amazon or eBay, they compare the performance of *laissez faire* policies (the firm chooses its preferred strategy), opt-in mandates (that require consumers to give their explicit consent) and opt-out mandates (that require platforms to allow consumers to not participate in default sharing of transactions data). They find “that sophisticated consumers and the platform generally benefit when the platform shares all transactions data with third parties (i.e., other merchants on the platform). The data sharing provides a channel through which sophisticated consumers can” receive price concessions. “In contrast, unsophisticated consumers benefit when the platform never shares transactions data with third parties... Thus, the privacy policy that best serves unsophisticated consumers harms sophisticated consumers. Consequently, the formulation of privacy regulations for online platforms can be challenging even when the sole objective of the regulations is to maximize consumer welfare.”

Much of the economics literature finds that markets compensate customers for the information they divulge when engaging in online activities. I explained this in a blog I wrote earlier this year (Jamison 2018b). In it I explained:

Suppose that customers think it is creepy that Amazon gathers information on them when they buy books. (I'll call this the creepiness factor, but it could be any reason for disliking Amazon watching and learning about the customer.) Then, for these customers to be willing to buy from Amazon, the company has to provide a price that compensates them for the creepy feeling. Otherwise, the customers either would not buy or might go to Barnes & Noble, for example, and pay cash. If, on the other hand customers think it is great that Amazon gathers information and uses it to make product recommendations, for example, then Amazon can reflect that premium feeling in the prices it charges. Either way, Amazon's prices reflect how customers feel about Amazon and what they know about Amazon's data practices.

But what about companies such as Facebook that don't charge consumers? A similar thing happens. Once Facebook users learn the company's data practices, they consider the creepiness factor in deciding whether to be on the platform, how often to use it, and for what purposes. If the creepiness factor is high, Facebook has to make sure that using Facebook is sufficiently valuable to consumers so that they feel compensated for the creepiness. Otherwise, their use of Facebook would be limited, and perhaps non-existent.

What if users actually value Facebook's data collection and use? They can enjoy the benefits of Facebook's services that rely on the company's big data and the benefits of the company's efforts to take care of customers who experience creepiness.

In summary, the economics literature points to the importance of not imposing broad privacy regulations. Indeed while the literature finds that some types of consumers can benefit from protective regulations in some circumstances, it appears that the more beneficial approach would be oversight that addressed specific harms when they occur and failures of companies to be candid and complete in their disclosures.

What's Missing from the Economic Literature on Privacy

Three important issues are missing from the economic literature: consumer adaptation, technology evolution, and an explicit market for information. These issues, once analyzed, are likely to further the case for policies that emphasize addressing harms and dishonesty when they arise.

The first missing analysis is the important issue of how consumers evolve. Consider, for example, the introduction of Caller ID in the late 1980s and early 1990s in the US.¹ The New York Times (1990) explained that "some civil libertarians argue that the company [New Jersey Bell] is invading the privacy of callers, especially those with unlisted numbers that are disclosed when they call a customer whose telephone is equipped with Caller ID." (parenthetical added) The paper quoted Marc Rotenberg,

¹ I would like to thank FTC Commissioner Noah Joshua Phillips for this insight.

director of the Washington office of Computer Professionals for Social Responsibility, as saying, “ “This is a case of a company that has a great deal of personal information making money exploiting the sale of that information without the consent of the phone subscriber.’ ” The article also cited Deborah Ellis, legal director for the American Civil Liberties Union of New Jersey, as saying that Caller ID would allow banks and other lenders to use the calling number information to discriminate against callers from poor areas. Ferguson (2001) wrote in the *Journal of Business Ethics* that, at its outset, Caller ID was “widely assailed as an invasion of the caller's right to anonymity, a right which allegedly subsists as an important component of the caller's right to privacy.”

What a difference time makes. Consumers have fully adapted to Caller ID, no longer feeling that the technology violates inherent rights to privacy. In fact many consumers find the service quite important for screening unwanted callers. (Ferguson 2001)

The Caller ID experience makes clear that consumers adapt their norms and expectations. This implies that policy makers should resist feelings of urgency to create new regulations in light of new circumstances because people’s initial feelings of loss may be replaced by newfound value. This topic is an under researched, so we cannot say when such evolution will occur or how long it will take. But we do know that stopping Caller ID because it seemed to violate norms would have denied customers services that they now value greatly.

Regarding technology evolution, privacy regulations can hinder important technology developments. In a recent blog (Jamison 2018a), I explain two conflicts between GDPR – which gives Europeans the right to require certain data gatherers to destroy data in their possession – and the use of blockchain.

One is that there may be no one to regulate. Often no one is in charge of the data on a blockchain, and no one owns it. For example, no one owns the bitcoin blockchain. So if a European wanted his or her transaction information pulled off the bitcoin blockchain, to whom would he or she go? If bitcoin is found in violation of GDPR rules, whom does the EU fine? Whom does the European citizen or nongovernmental organization (NGO) sue? (The GDPR allows NGOs to sue on behalf of citizens.)

The other conflict is with the immutability of blockchain. Suppose that data about a European are on a blockchain, and that the European wants the data removed. Even if there were a responsible party that could be held accountable for removing the data, how could it be done? Remember that one of the strengths of blockchain is its immutability. This means that if someone tries to alter historical data by, for example, removing the European’s data, all the subsequent data are corrupted.

People are trying to figure out workarounds.... But none that I have seen resolve the basic conflict of visions — centralized versus decentralized computing — with the heavy hand of government coming down on the side of centralization.

Lastly, we have yet to develop a coherent economic theory of privacy. There are two reasons for that. One is that “privacy” in practice is actually a hodgepodge of ideas, many of which are poorly developed, and many of which have little relationship to each other except for the label “privacy”. (Posner 1981) The other is that economic analyses almost uniformly treat privacy or a lack thereof as a consequence of a transaction rather than a transaction in and of itself.

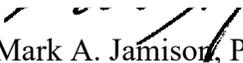
More specifically, in the economic models I have reviewed the consumer is on the demand side of the market seeking to purchase a product or participate in an activity, and the business is on the supply side. The research question becomes something like, “What are the consequences of information flowing and being gathered by the business in the transaction for a good or service?” A more appropriate formulation might be to view the ‘consumer’ on the supply side in an information market and the business on the demand side. This formulation might not significantly change the analytical model, but it could lend new insights. For example, such a formulation makes it easy from an economic perspective to explain privacy restrictions for children since we already have rationale for laws restricting minor children from being parties to contracts. Likewise, regarding medical privacy, a medical patient supplying health information to a physician has a clear interest in restricting the physician’s reuse of that information, just as many businesses supplying software products place restrictions on the use and resale of their products. As a supplier of information, either by directly divulging information or by allowing others to observe information-revealing activities such as shopping, the consumer as supplier could be viewed as placing explicit restrictions on how the information supplied can be used and passed along.

Viewing the consumer as a supplier could also clarify property rights to information. One of the problems with GDPR-like approaches to privacy, which simply endow people with rights to information related to them, is that they misalign disutility, value exchange, and rights. Normally we think of markets for property as including a supplier, who incurs costs in the form of exerted effort or forgone opportunities, and a buyer who receives something of value in exchange giving something up that the supplier values. The consumer-as-supplier privacy framework follows this normal market model in that the information supplier is exerting effort to be involved in an activity (such as online shopping) or divulging information that could be reserved for another use, in exchange for something of value that the buyer of the information provides (such as a product or service in lieu of money). Certain rights to the information that the supplier previously controlled are transferred to the buyer. In contrast, in some circumstances a GDPR-like approach grants rights to persons who never gave up opportunities or engaged in any effort to supply. Indeed the business holding the data may have been the only party to have incurred any costs in developing the information, yet someone else is granted property rights. This distorts economic incentives. Even when this isn’t the case, a GDPR-like approach fixes a specific form of contract between information suppliers and buyers that would be optimal in only a few circumstances, if ever.

Conclusion

In these comments, I examine some economics of privacy. I show that the scholarly literature shows the importance of not imposing broad privacy regulations. Indeed while the literature finds that some types of consumers can benefit from protective regulations in some circumstances, it appears that the more beneficial approach would be oversight that addressed specific harms when they occur and failures of companies to be candid and complete in their disclosures. I also describe issues not yet fully explored in the literature, but that also point to the importance of a light handed approach to regulating privacy.

Respectfully submitted this 21st day of December, 2018.


Mark A. Jamison, Ph.D.

Gainesville, FL
Telephone:

References &

Acquisti, Alessandro, Curtis R. Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* (2016), 52(2), pp. 442-92.

Acquisti, Alessandro and Hal R. Varian, "Conditioning Prices on Purchase History," *Marketing Science* (2005), 24(3), pp. 367-381.

Baye, Michael R. and David E. M. Sappington, "Revealing Transactions Data to Third Parties: Implications of Privacy Regimes for Welfare in Online Markets," Working paper, Department of Economics, University of Florida (2018).

Conitzer, Vincent, Curtis R. Taylor, and Liad Wagman, "Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases," *Marketing Science* (2012), 31(2), pp. 277-292.

Ferguson, Kenneth G., "Caller ID – Whose Privacy Is It, Anyway?" *Journal of Business Ethics* (2001), 29(3), pp. 227-237.

Jamison, Mark A., "Will the EU's privacy rules doom blockchain in Europe?" *AEIdeas*, October 24, 2018 <https://www.aei.org/publication/will-the-eus-privacy-rules-doom-blockchain-in-europe/>.

Jamison, Mark A., "Would new privacy laws help consumers?" *AEIdeas*, November 7, 2018 <https://www.aei.org/publication/would-new-privacy-laws-help-consumers/>.

Posner, Richard A., "The Economics of Privacy," *The American Economic Review* (1981), 71(2), pp. 405-409.

Taylor, Curtis R., "Consumer Privacy and the Market for Customer Information," *RAND Journal of Economics* (2004), pp. 631-650.

The New York Times, "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants," December 18, 2018 https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html?emc=edit_tu_20181221&nl=bits&nlid=8742491620181221&te=1.

The New York Times, "'Caller ID' Stirs Debate on Phone Privacy," February 11, 1990 <https://www.nytimes.com/1990/02/11/nyregion/caller-id-stirs-debate-on-phone-privacy.html>.

Varian, Hal R. 2010. "Computer Mediated Transactions." *American Economic Review* (2010), 100 (2), pp. 1-10.