Competition, Consumer Protection, and The Right**[Approach]** to Privacy

Remarks of Maureen K. Ohlhausen[1]
Commissioner, Federal Trade Commission

Premier Cercle
Competition Summit 2013
Brussels, Belgium

December 6, 2013

I. Introduction

It is an honor to give the morning address at Premier Cercle's 2013 Brussels Competition Summit. I will speak with you today about online privacy, an issue on everyone's mind lately. Since the emergence of e-commerce in the mid-1990s, the online marketplace has grown with accelerating speed. Low barriers to entry and the technical advantages of Internet protocol communications have allowed unprecedented experime85 4(r)-.Tan ssi

privacy recognizes that competition law and consumer protection law are complements, not substitutes, and thus applies them in accord with their different underlying purposes.

II. The Proper Relationship between Competition Laws and Consumer Protection Laws: They Are Complements by Design.

I just spent my Thanksgiving holiday in South Carolina, and we have a saying in the southern United States: if it ain't broke, don't fix it. The same can be said of our current enforcement regime. For nearly 100 years, the FTC has successfully discharged its Congressional duty under Section 5 of the FTC Act to prevent unfair methods of competition and unfair or deceptive acts or practices.[2] The first clause is the source of our competition law authority; the second our consumer protection authority.[3] This dual mandate is no mistake: the competition and consumer protection laws are complements, two different but equally important tools to help ensure fairness in our markets and thereby promote consumer welfare. Each protects consumers in different ways, and each has its limitations. Let me explain this interrelationship more fully.

Henry Ford once said: "It is not the employer who pays the wages. Employers only handle the money. It is the customer who pays the wages." And it is through this mechanism that healthy competition operates as the first line of defense to protect consumers. Sellers facing competition are forced to offer the best prices and quality to consumers able to spend their money elsewhere. Providing quality service includes being honest and forthright about products and giving customers the benefit of their bargain, including about the data they may share. An unhappy customer that feels tricked by a dishonest seller is unlikely to transact further business

[2] The FTC Act was signed into law in 1914 and included Section 5, which prohibited "unfair methods of competition." In 1938, the Wheeler-Lea Act amended Section 5 to empower the agency to directly enforce against "unfair or deceptive acts or practices." Before this amendment, the FTC had been required to show harm to competitors when pursuing claims for consumer harms like deceptive advertising.

[3] *See* 15 U.S.C. § 45(a)(1).

with that seller and will be vocal about his dissatisfaction to other consumers. By providing a platform for consumers, particularly unhappy ones, to voice their opinions about their treatment by sellers the Internet has actually magnified this effect. Bad consumer experiences and critical reviews hurt the business's reputation and its fortunes as customers turn to better, more reputable, alternatives. Or it could force the seller to change its ways. As Bill Gates has said, "Your most unhappy customers are your greatest source of learning." A competitive market thus disciplines potential bad actors and should be considered an important ingredient in protecting privacy online.

I do not mean to suggest, however, that competition alone can fully discipline the market. Former FTC Chairman Tim Muris put it well when he said, "the commercial thief loses no sleep over its standing in the community."[4] For a variety of reasons some companies engage in fraud, dishonesty, unilateral breach of contract, or other conduct that hurts consumers, with little regard for their reputations or the possibility of being put out of business. Because the rigors of a competitive market are insufficient to discipline these behaviors in some circumstances, we also use our consumer protection authority. The FTC, for example, has broad power to stop unfair or deceptive acts and practices under the FTC Act, and we enforce more than 50 other laws directed more narrowly to consumer protection issues like privacy, the handling of sensitive information, and decisions about personal credit, insurance, and housing, among other things.

This evolution of two distinct but complementary bodies of law reflects a consensus in the United States about the limits of our competition laws. They are not designed to address conduct that may be unjust or immoral, unless it also happens to harm competition. American competition law enforcement objectives are and for a long time have been primarily focused on

[4] Timothy J. Muris, *The Interface of Competition and Consumer Protection*, Fordham Corporate Law Institute's Twenty-Ninth Annual Conference on International Antitrust Law and Policy (Oct. 31, 2002).

economic efficiency, whereas its consumer protection goals are and have always been focused on harm to individuals. Former FTC Chairman Robert Pitofsky captured this view about the FTC's competition mandate from Congress when he said: "Oppressive, coercive, bad faith, fraud, and even contrary to good morals. I think that's the kind of roving mandate that will get the Commission in trouble with the Courts and with Congress."[5]

Even if privacy advocates are correct that privacy concerns should trump economic efficiency ones, disrupting Congress's bifurcated design of these laws is a legislative matter. Short of such legislative action, however, an enforcer's job is to apply the lawD.00058ladhe lawD.00058lae..3 T

searches per day.[10] It is a runaway success and is compared by many observers to an early Google. Another example is the wide range of privacy and security protection add-ons available for all of the major Internet browsers. One such add-on, Ghostery, helps users easily detect tools that behavioral advertisers often use to track individuals across sites.[11] This type of innovation gives me faith in the market's ability to meet consumer demand for product attributes, including privacy.

IV. The Competition Laws Are Not Intended to and Should Not Promote Non-economic Goals.

Having addressed whether the U.S. competition laws currently permit the consideration of privacy issues unrelated to competition, I will now address the normative question of whether they should evaluate non-competition factors, such as privacy. Welcoming non-competition factors like privacy into competition analysis would necessarily erode the focus on calculable economic efficiencies and evidentiary demonstration of harm. Instead, this would allow competition enforcers to embark on consideration of social mores and political issues without any meaningful limiting principles. Our rigorous standards of proof would be called into question as we sought to quantify an "economically optimal" amount of privacy to balance against diversion ratios, efficiencies, and the like. Because a society's understanding of privacy varies from one geographic area to another and even shifts over time it makes it nearly impossible to transform privacy into a meaningful, reliable, and objective metric that can fit within our competition framework. This conjures the disturbing notion of one nation's antitrust agency, which may have no privacy expertise, making decisions to block a deal based on a

[10] *50 Websites That Make the Web Great*, TIME, *available at* http://content.time.com/time/specials/packages/article/0,28804,2087815_2088176_2088178,00.html (last visited Dec. 6, 2013); https://duck.co/help/company/history (last visited Dec. 6, 2013); https://duckduckgo.com/traffic.html (last visited Dec. 6, 2013).

[11] http://www.ghostery.com/.

subjective sense that the deal would harm privacy too much while another nation's antitrust enforcer allowed the transaction because of either a different privacy preference or a lack of substantive knowledge about it. This obviously cuts against the trend toward global convergence on standards in antitrust reviews, which has been such an important focus for the FTC and other sophisticated antitrust regimes.[12]

As an example of how far notions of privacy can change, consider the different perception of privacy in Warren and Brandeis's 1890 work, which many people view as the starting point for the consumer privacy laws in the United States. Warren and Brandeis wrote their article, *The Right to Privacy*, because they were alarmed that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[13]

These concerns are so far removed from our world of ubiquitous television, Internet, and social media that they seem almost quaint by comparison. Our expectations of privacy have changed significantly. Mark Zuckerberg recently claimed privacy is disappearing as a social norm, although it is open to debate whether he will be proven right. As I will discuss later in my remarks, the FTC's consumer protection authority, which considers the reasonable consumer and evaluates substantial harms, is well suited to adjust to evolving consumer expectations and preferences about privacy. Although varied and changing expectations of privacy may be an appropriate issue for our consumer protection analysis, it simply cannot influence our empirical competition analysis. We cannot discard the scientific consistency we have worked so long to

[12] *See* Taking Notes: Observations on the First Five Years of the Chinese Anti-Monopoly Law, Remarks of Commissioner Maureen K. Ohlhausen, Competition Committee Meeting United States Council for International Business, Washington, D.C. (May 9, 2013), *available at* http://www.ftc.gov/speeches/ohlhausen/130509uscib.pdf.

[13] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 5 HARVARD L. REV. 193, 195 (Winter 1890).

develop and that has allowed for a common language of competition policy among us that extends across national boundaries. And, worse still, without meaningful limiting principles, once we open the door to non-competition factors, we are opening it to other policy issues like indigenous innovation, domestic

Third, does the consumer harm that the regulation seeks to prevent exceed the loss in consumer

provide consumers the benefits that a competitive market offers while addressing any identified privacy harms.

VI. The FTC Is Already Protecting Privacy Online.

Finally, not only is policing privacy through competition law a challenging idea – it is unnecessary. Section 5 of the FTC Act empowers the FTC to protect against unfair or deceptive acts or practices in or affecting commerce.[15] The FTC has been very active in enforcing the prohibition against unfair and deceptive trade practices in the areas of privacy and data security and has brought over 100 spam and spyware cases[16] and over 40 data security cases.[17] The Commission uses its deception authority in cases where a company makes a representation to consumers about the collection and/or use of their personal data but it fails to keep that promise. By contrast, the Commission's unfairness authority does not require a representation to consumers but instead focuses on the consumer harm that an act or practice may cause.

Our Unfairness Statement requires that for the Commission to find an act or practice unfair, the harm it causes must be substantial, it must not be outweighed by any offsetting consumer or competitive benefits, and the consumer could not have reasonably avoided the harm.[18] The Statement specifically identifies financial, health, and safety harms as varieties of harm that the Commission should consider substantial and further states that emotional impact and more subjective types of harm are not intended to make an injury unfair. The Commission's deception and unfairness standards are effective and flexible and are well suited to adapt to

[15] 15 U.S.C. § 45.

[16] Press Release, Fed. Trade Comm'n, *FTC Testifies on Protecting Consumers' Privacy* (July 14, 2011), *available at* http://www.ftc.gov/opa/2011/07/privacy.shtm.

[17] *See, e.g.*, Fed. Trade Comm'n, Bureau of Consumer Protection,

while minimizing the inappropriate use or insecure maintenance of data that could cause significant harm. The Commission will carefully analyze the submissions from the companies and use the information to supplement its knowledge of the industry and help decide how to proceed in this area.

As you can tell, the FTC is using all its tools to protect consumer privacy online. I know many in Europe are concerned about that and in particular have struggled with whether the Safe Harbor agreement remains viable in light of concerns about enforcement in the United States. I am happy that the agreement, which has been a useful framework for both government and business, will continue. I want to emphasize that the FTC has been and will continue to be a good partner and an aggressive enforcer of Safe Harbor certifications.

VII. Conclusion

Let me close by noting that, unlike in the days of Warren and Brandeis, billions of people use the Internet and at some

whether consumers even know how their information is being collected and used. These are important questions, and I believe the best way for the FTC to continue answering them is to focus its energy and resources on maintaining competitive online markets through antitrust oversight, enforcing the consumer protection laws currently in place, and continuing to invest in education and research regarding online privacy issues.