Privacy Policies and Competition Law

Andrew J. Heimert*
Asian Competition Forum
Hong Kong SAR
December 11, 2018

The rapid growth of online activity, especially, but not exclusively, social media has led to an equally rapid growth in attention to how various online platforms and other online services providers treat the privacy of customer information. Many of the issues that arise are addressed through consumer protection laws or data privacy laws, and sensibly so. In the United States, the FTC's approach to privacy regulation has focused on enforcing certain statutory data protection obligations, such as the Children's Online Privacy Protection Act (or COPPA), as well as laws relating to privacy of financial or health information and their accompanying regulations. The FTC has combined this with enforcement of the unfair or deceptive acts or practices provision of the FTC Act.[1] In particular, we have brought a series of cases against companies that have not honored their stated privacy policies in one of two ways: first, companies that simply do not do what they said they would, and use or share information for purposes beyond what they had told consumers they would; second, failing to take reasonable precautions to protect collected data, such as preventing cyberintrusions. This is sensible, straight-forward, and, I believe, non-controversial.

Yet with these approaches available, or at least potentially available through adoption of new laws or regulations, there is an enthusiasm in some quarters for addressing issues involving privacy policies through the lens of antitrust laws. In my view these approaches are misguided for at least three reasons, which I'll explain during my remarks. I will begin, however, with a

* My remarks do not necessarily represent the views of the Commission or any individual Commissioner. An abbreviated version of these remarks was presented at the conference.

[1] 15 U.S.C. § 45(a)(1).

discussion of when privacy policies may be relevant to antitrust enforcement, and properly considered in antitrust analysis of mergers or conduct. Then I will explain why in my view, outside those circumstances, antitrust enforcement tools should not be used to address privacy policies and penalize failures to adhere to them.

When Privacy Issues are Competition Issues

Online services, whether e-commerce, social media, or otherwise, continue to grow in importance to consumers. Some of these services collect information about consumers in order to improve their services to individual consumers, for example, shopping sites that may suggest similar products that you might "also like." Others, particularly social media, rely on the collection of consumer information and online activity to sell to advertisers or to third parties that assist advertisers. And, of course, businesses may blend these two models, using information both to provide better service to an individual consumer and also to provide information about those consumers for use by advertisers.

The collection of consumer information by many of these online services is their *raison d'être*. In exchange for the collection of information, the operator provides a service of some value to its consumers or users, while, in many cases, providing the service at no financial cost to the user. Examples are abundant, but include free search and email provided by, for example, Google or Baidu, or a place to exchange personal updates and opinions, such as Weibo or Twitter. As a result, competition among these services may not focus on price, as occurs in markets for many goods and services, be it food, airline tickets, or appliances. Instead the competition focuses on non-price attributes, including the nature of the service offering and,

potentially, the privacy, or lack thereof, afforded by the service.[2] Indeed, Assistant Attorney General Makan Delrahim suggested privacy considerations will become ever more prominent for consumers in selecting the online services they use.[3]

The value consumers place on privacy protections is unclear. A survey-based study in 2013 by Scott Savage and Donald Waldman concluded that customers in the United States were willing to pay somewhat more for putative comparable mobile apps that required the sharing of less information (*e.g.*, browser history, contacts, location, text message content).[4] This study, however, found variation across several user characteristics. For example, more "experienced" users of mobile apps (longer and broader use of apps) were willing to pay more for sharing less information, as were people with higher levels of education and income.[5] Other studies, in contrast, suggest greater ambiguity in how much consumers are willing to pay for privacy, as well as whether they are more willing to pay to avoid sharing information than they are to stop sharing information they already are providing.[6] While there are numerous other product attributes that may contribute to pricing differences, consider, for example, the differing business models between Apple's iOS, for which Apple shares limited information with advertisers, and Google's Android operating system, through which Google monetizes services through

---

[2] *See, e.g.*, Note by the United States, *Quality Considerations in the Zero-Price Economy*, Submission to the Competition Committee, Organization for Economic Co-operation and Development, at 6-7 (Nov. 28, 2018) ("[T]o the extent that firms compete with one another to offer effective protection of consumer data—a non-price dimension of competition—conduct that restrains competition on that basis . . . could give rise to an antitrust violation."), https://one.oecd.org/document/DAF/COMP/WD(2018)139/en/pdf.

[3] *See* Makan Delrahim, *Don't Stop Believin': Antitrust Enforcement in the Digital Era*, Remarks at University of Chicago Antitrust and Competition Conference, at 6-7 (Apr. 19, 2018), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-keynote-address-university-chicagos.

[4] Scott J. Savage & Donald M. Waldman, *The Value of Online Privacy* (Oct. 2013), https://ssrn.com/abstract=2341311.

[5] *Id.* at 25-26.

[6] *See* Joseph L. Cordes and Daniel R. Pérez, Working Paper, *Measuring Costs and Benefits of Privacy Controls* (Nov. 2017), https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs1866/f/downloads/Cordes-Perez_Measuring%20Costs%2BBenefits%20of%20Privacy.pdf.

collection of search and other user data. Further, the importance of privacy may vary across countries or societies. As an example, Europe's emphasis on these issues through various policy tools suggests a particularly high value there; elsewhere it may be different.

What this means, however, is that competition for privacy as a dimension of quality may be even more difficult to assess than competition via more readily measureable metrics such as price, where lower is virtually always better.[7] Indeed, the answer in any given case may be ambiguous. For example, how should a competition enforcer assess a merger between two firms with radically different approaches to privacy? If the companies are to adopt the approach of only the high-privacy party, are consumers better off as a result? Is that the case if the high-privacy party also charges higher prices? For some consumers, the increased privacy protections may be well worth the additional costs (which perhaps they already were paying); for others, the increased price may be something they would prefer to "pay" for through continued sharing of data about themselves.[8] I should mention the limitation we identified in connection with our clearance of the Facebook/WhatsApp merger, where, separate from the Commission's decision not to intervene in the merger, the FTC's Bureau of Consumer Protection cautioned Facebook to ensure that it did not apply its relatively less robust privacy policies to information obtained by WhatsApp from its customers, absent further disclosures and acceptance by users.[9]

Overall, there is a lot of room for development in the evaluation of the competition between different approaches to privacy. This reflects some of the challenges we already face in

[7] Notable exceptions include Veblen goods, which are luxuries, and predatory prices that harm competition.

[8] *See* D. Bruce Hoffman, *Competition Policy and the Tech Industry – What's at Stake?*, Remarks at the Computer and Communications Industry Association, at 8 (Apr. 12, 2018) ("We cannot presently determine that consumers should value data in certain ways, or should not want to provide that data to firms in the same way that we can generally assume that consumers would not want to pay higher prices or accept lower quality."), https://www.ftc.gov/system/files/documents/public_statements/1375444/ccia_speech_final_april30.pdf.

[9] *See* Letter from Jessica Rich, Bureau of Consumer Protection, Federal Trade Commission, to Erin Egan, Facebook, Inc., and Anne Hoge, WhatsApp Inc. (April 10, 2014), https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer.

assessing non-price factors of competition. Regardless, applying the same fundamental principles to non-price competition on privacy-related attributes of a product or service falls within the proper scope of competition law.

When is Privacy not a Focus of Competition Law

Having spoken a bit about how and when privacy may be an element of competition that should be considered in antitrust analysis, I would like to turn now to explain ways in which antitrust law should not, in my view, be applied to privacy issues. As companies increase their ability to compile, analyze, and use or sell more and more information collected about consumers, consumers' attention to privacy issues has increased. For many observers, enhancing privacy is an important policy goal, some of whom have made calls in the United States for investigations of companies such as Facebook for disclosures of consumer data[10] and proposals for a general privacy law.[11] And of course Europe already has adopted the General Data Protection Regulation.[12]

I would like to identify three possible ways antitrust law could apply to privacy-related issues, and why I believe its use in these ways would rarely if ever be appropriate.

[10] The FTC announced that it was undertaking an investigation of Facebook's adherence to its FTC consent decree in light of its disclosure of information to Cambridge Analytica this past Spring. *See* https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[11] *See* Cecilia Kang, "Tech Industry Pursues a Federal Privacy Law, on Its Own Terms", *New York Times* (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html.

[12] Regulation (EU) 2016/679, Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (Data Protection Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Privacy Policies as Non-Competition Considerations

First, although some may view increased privacy protections as desirable, but that does not necessarily mean insufficient privacy protection properly falls within the scope of antitrust enforcement. U.S. antitrust law has, for at least the past 40 years, had a singular focus on consumer welfare and promoting competition. Thus the U.S. antitrust agencies do not consider non-competition factors in their antitrust analysis.[13] Of course, the FTC recognizes that there are many worthwhile policy goals, but we have encouraged supporters to pursue them through more appropriate channels, whether it be legislation or regulatory intervention by a competent agency. To this end, the FTC itself enforces the FTC Act with respect to privacy issues, as I've described, and has testified in support of Congressional consideration of general privacy legislation.[14] In prepared testimony before Congress last month, the Commission noted that "This process understandably will involve difficult value judgments and tradeoffs that are appropriately left to Congress."[15]

The FTC's approach was highlighted by the Commission's decision in the Google-DoubleClick merger, which involved two companies that engaged in online advertising services. The FTC's antitrust analysis focused on potential horizontal and vertical theories of harm that could result from the merger, with the Commission ultimately concluding that the evidence did not show the transaction was likely to substantially lessen competition.

---

[13] Note by the United States, *Public Interest Considerations in Merger Control*, Submission to Working Party No. 3 on Co-operation and Enforcement, Organization for Economic Co-operation and Development, at 2 (June 2016), https://www.ftc.gov/system/files/attachments/us-submissions-oecd-other-international-competition-fora/1606public_interest_merger-us.pdf.

[14] *See* Prepared Statement of the Federal Trade Commission: Oversight of the Federal Trade Commission Before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, Washington, D.C., at 9 (Nov. 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1423835/p180101_commission_testimony_re_oversight_senate_11272018_0.pdf.

[15] *Id.*

Commissioner Pamela Jones Harbour, however, identified privacy concerns as a basis for seeking conditions on the clearance of the merger. The combination of the two companies would combine their extensive datasets about consumer behavior and preferences, which she believed they could use in further developed behavioral advertising to the detriment of consumers and their expectations of privacy.[16]

The 4-1 majority of the Commission rejected Commissioner Harbour's suggestion that these privacy concerns were a basis to intervene in a merger that otherwise could not be shown to harm competition and consumer welfare. It explained that, as when the Commission has been asked in the past to "intervene in transactions for reasons unrelated to antitrust concerns . . . the sole purpose of federal antitrust review . . . is to identify and remedy transactions that harm competition."[17] The Commission majority went on to explain that, not only did it lack the authority to intervene on the basis of privacy concerns, "regulating the privacy requirements of just one company could itself pose a serious detriment to competition."[18]

Antitrust as a Catch-All

A second way in which antitrust law might apply is if violations of other laws can provide a foundation for a violation of the antitrust laws. The paradigmatic example of this is the dominant firm that burns down its competitors', or potential competitors', factories. Unlike building a better product, or otherwise having superior skill, foresight, and industry, destruction

[16] In the Matter of Google/DoubleClick, F.T.C. File No. 071-0170, Dissenting Statement of Commissioner Pamela Jones Harbour (Dec. 20, 2007), https://www.ftc.gov/public-statements/2007/12/dissenting-statement-commissioner-harbour-matter-googledoubleclick.

[17] In the Matter of Google/DoubleClick, F.T.C. File No. 071-0170, Statement of the Commission, at 2 (Dec. 20, 2007), https://www.ftc.gov/public-statements/2007/12/statement-federal-trade-commission-concerning-googledoubleclick; *see also Quality Considerations in the Zero-Price Economy*, *supra* note 2, at 6-7 ("[I]n the absence of actual or likely harm to competition, the misuse or abuse of consumer data does not present a mandate for intervention under the U.S. antitrust laws . . . .").

[18] In the Matter of Google/DoubleClick, Statement of the Commission, *supra* note 17, at 2

of a competitor's assets seems as far away from competition on the merits as possible. Of course, burning a competitor's factory also likely qualifies as arson or some similar crime in many jurisdictions, and can be prosecuted that way.

A case not altogether different from such a scenario was addressed by a U.S. court of appeals at the beginning of this century. In *Conwood Co. v. United States Tobacco Co.*,[19] U.S. Tobacco stood accused before a civil jury of using its position as category captain or manager for moist snuff, a type of smokeless tobacco, to destroy its competitor's products and advertising in retail stores. A category manager works with a retail store to help optimize displays, advertising, and product location to enhance sales. U.S. Tobacco, acknowledged to be the dominant firm in smokeless tobacco, held this position at a number of retail outlets selling smokeless tobacco. While providing these services, however, it also discarded or destroyed its competitor's racks and advertising. Although U.S. Tobacco acknowledged the destruction of its competitor's racks and materials was tortious under law, it denied that it was anticompetitive. The court of appeals rejected this argument, holding that the conduct was sufficiently widespread to support a claim for monopolization.

Smokeless tobacco shelving and advertising is a far cry from privacy, you are likely thinking. And it is. Yet there is a broader point that is worth considering, and that is whether conduct that might otherwise be unlawful, or that creates civil liability, could be deemed something other than competition on the merits. *Conwood* seems to suggest yes—indeed, destruction of a competitor's products seems the antithesis of legitimate competition. Thus, could a violation of a privacy policy—whether wrongful as a contractual matter or as a violation of an

[19] 290 F.3d 768 (6th Cir. 2002), *cert. denied*, 537 U.S. 1148 (2003).

applicable consumer protection or privacy protection law—form the basis for an antitrust violation?

While a privacy violation might constitute wrongful conduct, other important elements remain necessary to establish a monopolization case under U.S. antitrust law. First, the firm must be dominant in a relevant product market. That alone would eliminate many of the privacy breaches we have seen from the ambit of antitrust law. Second, the conduct must be an effort to strengthen or maintain a monopoly. That too will limit the number of cases, and, indeed, may reduce them to zero.

On this latter point, a company's breach of its *own* privacy policy does not tend to prevent competitors from competing on the merits. On the contrary, it is typically harmful to the reputation and business of the company committing the violation. Rather than undermining or inhibiting a competitor's ability to compete, a dominant firm's failure to adhere to its privacy policies, or even have privacy policies that are unattractive to consumers, is likely to drive business to its competitors, not to itself. It simply is not a rational competitive strategy.[20]

Alternatively, a company's misleading characterizations of its adherence to a privacy policy might give rise to a basis for an antitrust claim.[21] We may be getting a bit closer on such a theory, although consider what likely would need to be shown. First, the privacy policy would have to be an important element of a substantial number of consumers' decisions to choose the company's product over a competitor's. That is, but for the false representations about the

[20] If detection (by the public or relevant regulator) of the breach is imperfect, and the costs of ensuring compliance are high, relatively low reputational costs may make underinvestment in preventing breaches economically rational.

[21] The FTC has pursued such cases under its consumer protection mandate. *See, e.g.*, Federal Trade Comm'n v. Ruby Corp. et al., No. 1:16-cv-02438 (D.D.C. filed Dec. 14, 2016) (settlement of charges that Ashley Madison.com failed to protect users' personal information despite claims it would), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting; *see also* In the Matter of Uber Technologies, Inc., FTC No. C-4662 (Aug. 15, 2017) (resolving allegations that Uber made misleading claims about employees' access to user information), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.

privacy policy the company would not have obtained or maintained its dominant position.[22] Second, substantial barriers to entry would need to remain that would prevent consumers from switching relatively costlessly and quickly to the competing providers of the putative service. If switching is easy, the dominant position would quickly evaporate. While I do not rule out the possibility that such a scenario could transpire, it strikes me that these two elements are likely to limit the number of such cases to an extremely small number.

Privacy Policies as Exploitation

A final way in which privacy issues might implicate antitrust concerns is if "unfair" privacy policies might be deemed an exploitative abuse. Most antitrust laws, although not those in the United States, contain provisions regarding excessive pricing or unfair high pricing undertaken by a firm with a dominant position. As I discussed earlier, privacy policies could be considered a dimension of non-price quality on which businesses compete. Thus, under a statute where excessive pricing also includes (or separately includes) non-price excessiveness (or unfairness), a case might be made for abuse of dominance through exploitation. In fact, I understand this to be the basis for the Bundeskartellamt's investigation into Facebook.

U.S. antitrust law would not allow such a case because of it does not prohibit exploitative abuses, in particular excessive pricing. U.S. antitrust law does not prohibit excessive pricing for three basic reasons, all deriving from the fundamental presumption that a lawful monopolist should be free to charge whatever price it wishes and the market will bear.[23] The reasons the

[22] *See* Rambus Inc. v. Federal Trade Comm'n, 522 F.3d 456, 466-67 (D.C. Cir. 2008) (FTC failed to show that but for Rambus's misleading conduct before standard-setting organization a different standard would have been adopted).

[23] *See, e.g.*, Berkey Photo, Inc. v. Eastman Kodak Co., 603 F.2d 263, 297 (2d Cir. 1979).

United States does not pursue exploitative abuses with respect to pricing apply more strongly, perhaps much more strongly, with respect to non-price attributes of quality.[24]

First, placing restrictions on unilateral price setting diminishes incentives to compete. This derives from the principle stated in *Alcoa* by Judge Learned Hand that a "successful competitor, having been urged to compete, must not be turned upon when he wins."[25] Limiting the flexibility of a winner to charge a monopoly price reduces the incentive to seek the monopoly in the first place.

Second, prices are a signaling mechanism from the market that encourages increased production, or reduced consumption. Interfering with that mechanism by penalizing prices that are deemed too high runs the risk of discouraging the production of goods and services that the market is demanding more of.[26]

Third, there is an institutional challenge in determining what constitutes a reasonable, or at least not excessive, price.[27] This derives primarily from institutional competence—antitrust agencies are not generally price regulators, and are not in the business of setting prices for all players in an industry, which most typically is done by regulators based on extensive data about capital and variable costs on an industry-wide basis. In a related vein, remedying an excessive

---

[24] *See generally* Note by the United States, *Excessive Prices*, Submission to Working Party No. 2 on Competition and Regulation, Organization for Economic Co-operation and Development (Oct. 2011), https://www.ftc.gov/sites/default/files/attachments/us-submissions-oecd-and-other-international-competition-fora/1110excessivepricesus.pdf.

[25] United States v. Aluminum Co. of America, 148 F.2d 416, 430 (2d Cir. 1945); *see also* Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 407-08 (2004) (permitting monopoly pricing maintains incentives for investment).

[26] *See OECD Excessive Prices*, *supra* note 24, at 4.

[27] *Id.* at 2-3.

price would take a similar amount of effort to determine what the price *should* be, which would need to account not only for costs but also for demand and value to consumers.[28]

These principles, particularly the third, are instructive with respect to non-price features. A company that has achieved success with a given privacy policy may have done so *because of* that business approach, striking whatever balance it determined would be accepted by the market and also make its business plan profitable. Determining afterwards that the company's approach is impermissible risks punishing the company for its success.

Even more difficult is determining what an appropriate policy *should* be if the existing one is exploitative. A competition agency would need to determine not only that the policy disfavored consumers, it would also have to determine what the policy should be instead. This seems even more complex than pricing decisions, as any quality related decision a company is likely to make inherently hinges on a number of factors that it must balance using its business judgment.

Conclusion

The attention paid to privacy issues has led supporters of enhanced privacy protections to suggest antitrust law as a new basis to promote increased privacy. While privacy may be a dimension on which firms compete, making mergers with impacts on privacy competition potentially worthy of antitrust scrutiny, broader antitrust theories that would seek to implement non-competition policies or views on fairness seem misguided.

Thank you for your attention.

[28] *Id.* at 3.