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 essage 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 Copition Comittee, Organizatio fo Economic Coperation and Development, at 6-7 (Nov28208) ("[T]o the extent that firms compete with one another to offer effective potectioof coumer data—a nopice dimension f competition—conduct that restrains competition 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 Univ Chicago Antitrust and Competition Conference, at 6-7 (Apr, 2018), https://www.justice.gov/opa/speech/assistant-attorney-geneal-makan-delrahim-delivddress-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*

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

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.

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

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.

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 ted vein, remedying an excessive

[24] See generally OECD 2011 Policy Roundtable, *Excessive Prices*, 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 accer/BBoD1 (y have nc)]TJd, ared wo