# What's Up with WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets

BY LISA KIMMEL AND JANIS KESTENBAUM

DATA CAN BE VIEWED AS THE raw material of the information economy, and firms in markets for consumer-facing digital goods and services have built business models that depend on the collection and use of consumer information. When firms in this sector merge, it can lead to a substantial increase in the scope and magnitude of consumer data under the control of a single firm. Some regulators and privacy advocates have expressed concern that the aggregated data of the combined entity, when subjected to increasingly powerful "big data" analytic tools, will yield especially revealing pictures of consumers, making data breaches more consequential, and raising the risk that data will be used in ways that will disadvantage consumers.

Privacy law provides the first line of defense in protecting consumers from risks that may be associated with combining large stores of data. Both the United States and the European Union have robust privacy regimes that seek to promote transparency and consumer control over personal data. At the same time, as the collection and use of consumer data become more prevalent and predictive analytic tools more potent, some privacy regulators and advocates on both sides of the Atlantic have called for antitrust scrutiny of the privacy ramifications of digital market mergers, an argument first heard in connection with Google's acquisition of DoubleClick nearly a decade ago. Most recently, Facebook's agreement to acquire the mobile messaging application WhatsApp has re-energized calls to find antitrust solutions for the privacy risks that may flow from digital market mergers.

In this article, we describe how privacy and antitrust law operate in distinct ways to protect consumers from privacy risks that may be associated with digital market mergers. Our analysis shows that the privacy regimes in the United States and European Union share common objectives of promoting transparency and consumer control despite their differing statutory frameworks. With respect to antitrust, both jurisdictions have evaluated mergers that may implicate consumer privacy exclusively through the lens of competitive effects. This lens, while wide enough to capture privacy risks that flow from digital market mergers that may create or enhance market power, is not designed to capture risks that are not the result of a likely lessening of competition. Privacy risks not tied to diminished competition are best addressed through strong enforcement of the privacy laws and building any additional protections necessary to protect consumers into such regimes.

*The authors are advisors to Federal Trade Commission Chairwoman Edith Ramirez. Lisa Kimmel focuses on antitrust law and competition policy and Janis Kestenbaum focuses on privacy and other consumer protection issues. The views expressed here are those of the authors and do not reflect the views of the Federal Trade Commission or any individual Commissioner.*

## Privacy Law in the United States

***Federal Framework.*** Privacy regulators in the United States and European Union express shared objectives of transparent data practices, meaningful consumer choice, and "privacy by design," notwithstanding differing regulatory frameworks to protect privacy in the commercial sphere.[1]

The United States has a "sectoral" privacy regime under which companies must adhere to an array of focused privacy laws covering categories of information that Congress has determined warrant special protection, such as children's online data under the Children's Online Privacy Protection Act,[2] health information in the hands of medical providers, hospitals, pharmacies, and insurance companies under the Health Insurance Portability and Accountability Act (HIPAA),[3] non-public personally identifiable information held by financial institutions under the Gramm-Leach-Bliley Act,[4] certain information for decisions about a consumer's eligibility for credit, employment, insurance, or housing under the Fair Credit Reporting Act (FCRA),[5] and video rental records under the Video Privacy Protection Act.[6]

These targeted laws are grounded in the Fair Information Practice Principles, a set of privacy norms that has served as the foundation for privacy regimes worldwide.[7] As a consequence, U.S. privacy laws generally mandate some or all of the fair information practice principles, such as notice and an opportunity to object to the collection and use of personal data, reasonable data security, and limits on the purposes for

which data may be used, such as those found in the FCRA.

For the large body of data that falls outside these discrete areas, the main federal safeguards are found in the FTC Act's general prohibitions on "deceptive" or "unfair" commercial acts and practices.[8] Since the spread of the Internet in the 1990s, the FTC has applied this authority to online and offline commercial data practices.

A major component of this enforcement activity concerns data security. Enforcing the prohibitions on both deceptive and unfair practices, the FTC has brought a steady stream of cases against companies charged with failing to take reasonable steps to safeguard consumer data. For example, following what was at the time the largest breach of payment card data, in 2008 the FTC alleged that The TJX Companies engaged in unreasonable—and hence unfair—practices by storing and transmitting personal information in its network in unencrypted text, not requiring network administrators to use strong passwords, and failing to use firewalls to limit access among its users.[9]

Outside the data security context, the FTC has relied on the prohibition on deception to allege that companies breached express or implied representations as to what consumer data they would collect or how data would be used or shared. For example, in *Snapchat*, the FTC alleged that a mobile app deceptively promised users that their videos and photo messages would permanently disappear after a brief time set by the user when, in fact, recipients had readily available means to preserve the videos and photos.[10]

The FTC has used the prohibition on unfair acts or practices to challenge retroactive changes to data practices made without affirmative express consent. For example, the FTC alleged that Facebook, in revamping its platform in December 2009, unfairly overrode users' privacy settings that had restricted access to certain information, such as a profile picture and Friends List, without its users' informed consent.[11] In addition, in complaints filed against the Aaron's rent-to-own franchisor, a number of its franchisees, and a software designer, the FTC alleged that the deceptive collection of highly private data through the surreptitious installation of spyware and key loggers on laptop computers was an unfair practice.[12] And the complaint in *FTC v. Frostwire, LLC* charged that a software company's failure to notify users that many preexisting files on computers and mobile would be designated for public sharing constituted an unfair practice.[13]

Changes in technology and business practices have resulted in growing gaps in the U.S. consumer privacy legal regime. For example, new technologies and business models, such as wearable fitness bands and mobile health apps, mean that health data are now often in the hands of entities that are not covered by HIPAA. Similarly, emerging products, beyond traditional credit scores, that purport to predict or "score" everything from the chances that a transaction will result in fraud to the efficacy of sending consumers catalogs and the best prices to offer consumers, generally fall outside the FCRA.[14] To fill such gaps, the FTC has supported "baseline" privacy legislation as well as legislation governing data brokers.[15] Likewise, the Obama administration has urged Congress to adopt legislation implementing a Consumer Privacy Bill of Rights, which the administration is also seeking to implement through multi-stakeholder meetings to create voluntary codes of conduct in areas like mobile privacy disclosures and facial recognition.[16]

***State Framework and Private Litigation.*** State privacy law mirrors federal law in its structure. Nearly all states have statutes governing specific privacy issues. Notably, 48 states have laws that require businesses to notify individuals of security breaches of their personally identifiable information.[17] California has the broadest assortment of targeted privacy statutes, including one that requires online service providers to post privacy policies and, as of January 1, 2014, to disclose how certain providers respond to "do not track" signals.[18] Likewise, 28 states have general prohibitions on deceptive or unfair practices,[19] often referred to as "mini FTC Acts," many of which have been used in the privacy arena.[20] There is also a growing body of class actions alleging federal and state privacy violations and some of these cases have led to significant settlements and decisions.[21]

## Privacy Law in the European Union

Whereas in the United States the Constitution exclusively protects individual privacy vis-à-vis governmental conduct, in the EU, since 2000, the "protection of personal data" has been enshrined in the EU Charter of Fundamental Rights.[22] In addition, in contrast to the complex mixture of federal sectoral laws, the FTC Act, state laws, and private rights of action that characterize the U.S. privacy regime, a general EU data protection directive adopted in 1995 (General Directive) establishes comprehensive principles to limit the "processing"—a broadly defined term—of all "personal data," meaning "any information relating to an identified or identifiable natural person."[23] Each member state implements the General Directive through its own law, which is enforced by one or more independent data protection authorities in each member state.[24]

Under the General Directive, personal data may only be processed for specified, explicit, and legitimate purposes and may not subsequently be processed for an incompatible reason.[25] One lawful basis for processing personal data is the consent of the consumer—the "data subject" in EU parlance—at the initial collection of the information.[26] In addition, the collection and use of personal data must be proportional to the purpose of its initial collection.[27] The General Directive also specifies that data processing must be transparent, meaning, for example, that individuals should be given information about the purpose of the processing and the recipients or categories of recipients to which data are disclosed.[28] Likewise, data controllers must take appropriate measures to safeguard the security of the data.[29] The General Directive also provides that individuals have the right to access data collected about them.[30]

In applying the General Directive, the European Court of Justice in *Google Spain, SL v. González* recently held that search engines are "data controllers" and must, on request, remove links to personal information that is inaccurate, inadequate, irrelevant, or excessive in relation to the purpose for which the data were originally processed. The court explained that the scope of this "right to be forgotten," as it is commonly known, would be decided on a case-by-case basis and must be balanced against rights of Internet users to get access to information.[31]

To update its data protection regime, the EU is in the process of replacing the General Directive and the implementing laws of member states with a uniform, binding data protection regulation across the EU. The European Parliament approved a version of the proposed regulation on March 12, 2014.[32] Among the major features of the Parliament-approved regulation is the creation of a "one-stop shop," under which each data protection authority would coordinate all EU enforcement activities for those organizations with EU headquarters located in its jurisdiction. The Parliament-approved regulation also would establish a right to data portability to enable an individual to transfer data from one digital platform to another. An organization found to have violated the proposed regulation could be subject to fines of up to 5 percent of its annual turnover or 100 million euros, whichever is greater—a dramatic increase from the maximum fines most individual data protection authorities may currently impose.[33] To become law, the final text of the regulation must be negotiated and jointly approved by the EU Parliament and the EU Council of Ministers.

**Changes in technology and business practices have resulted in growing gaps in the U.S. consumer privacy legal regime. For example, new technologies and business models, such as wearable fitness bands and mobile health apps, mean that health data are now often in the hands of entities that are not covered by HIPAA.**

## Privacy and Digital Market Mergers

***Calls to Recognize the Interplay Between Privacy and Antitrust.*** Despite more active efforts by regulators on both sides of the Atlantic to protect consumer privacy, privacy regulators and advocates have looked to antitrust law to protect consumers from the privacy risks that may be associated with digital market mergers.

Advocates and regulators argue that the combinations of large data sets that can come with mergers in this sector raise two primary privacy risks. First, when individual organizations amass more comprehensive and revealing profiles of consumers, a single data breach can lead a larger trove of data to fall into the hands of criminals, potentially putting consumers at greater risk of malicious conduct. Second, richer data sets, when subject to predictive analytic tools, may enable firms to draw more revealing inferences about consumers and make more fine-grained distinctions among them, increasing the prospect of differential treatment with regard to what products and services are marketed to them, the prices they are charged,[34] and the level of customer service they receive, potentially outside the reach of existing laws.[35]

The European Data Protection Supervisor (EDPS), an EU privacy regulator, has urged attention to the competitive implications of data in antitrust investigations, particularly the relationship between data, entry barriers, and market power. In a preliminary opinion on the interplay between data protection and competition law, the EDPS suggested that merger enforcement in digital markets should be based on a broader definition of consumer harm that goes beyond looking solely at competitive effects, and accounts for risks to consumer privacy from the combination of large datasets that are not necessarily linked to a lessening of competition.[36] The EDPS called for greater dialogue among regulators in the areas of data protection, consumer protection, and competition at the intersection of these areas. A follow-on workshop and report explored many of these same themes.[37]

The EDPS raised some of the issues that then-FTC Commissioner Pamela Jones Harbour introduced in her dissent from the FTC's decision to close its investigation of Google's acquisition of DoubleClick in 2007.[38] Since leaving the agency, Harbour has continued to press enforcers to develop a more sophisticated analytical framework for evaluating the antitrust implications of privacy and big data.[39] Then-FTC Bureau of Economics Director Howard Shelanski, writing in his individual capacity, has also recommended that antitrust enforcers focus on the potential exclusionary effects of acquiring customer data, which "can reveal horizontal dimensions of facially vertical conduct and transactions," and recognize privacy protection as an important nonprice dimension of competition in digital markets.[40]

***Google/DoubleClick Revisited.*** The FTC first publicly grappled with the intersection of privacy and antitrust in 2007 in reviewing Google's acquisition of DoubleClick. Google was the dominant provider of search advertising in both the United States and Europe, and both companies were large players in markets for online display advertising, the graphic ads that appear on websites and feature images like company logos to build brand recognition.[41] Websites often sell their premium display space, usually located at the top half of a page, directly through in-house staff and use third-party "ad servers" solely to manage the timing and

placement of such ads. Websites tend to monetize their less valuable territory with the help of "ad intermediaries," who purchase, aggregate, and sell that space to advertisers. Google, with its AdSense product, was a large online advertising intermediary, while DoubleClick was a leading online ad server.

Google and DoubleClick held vast amounts of data on consumer online search and browsing behavior, and the potential consolidation of the data raised red flags for privacy advocates.[42] The Electronic Privacy Information Center (EPIC), the Center for Digital Democracy (CDD), and the U.S. Public Interest Research Group (U.S. PIRG) filed a complaint with the FTC objecting to the merger on privacy grounds.[43] They also claimed that the combination of data would give Google a competitive advantage over both search and display advertising rivals, allowing it to "control the process of monetizing web content."[44]

In clearing the merger unconditionally, the FTC and the EC each released a detailed analysis of the competitive effects of the transaction.[45] Both agencies decided that Google and DoubleClick were not close actual or potential competitors in any markets for online advertising or services. They further found that because DoubleClick did not have market power, it could not exclude advertising intermediation rivals by bundling AdSense with DoubleClick's ad server for publishers. Neither jurisdiction was persuaded that the combination of data would give AdSense an anticompetitive advantage over rivals because DoubleClick's contracts would not permit Google to use the information to target advertisements, and Google committed that it would not combine the data post-merger. More importantly, both jurisdictions determined that even if Google changed or breached these agreements, DoubleClick's data were not unique and similar data of similar scope and quantity were available to competing ad intermediaries from other sources.

While expressing a strong commitment to privacy and noting that FTC staff had just proposed a set of privacy principles for online behavioral advertising, the FTC concluded that the antitrust laws did not provide a basis to seek to block or impose conditions on a merger purely to safeguard privacy. The FTC explicitly recognized that privacy can be a nonprice dimension of competition, and that it therefore has the authority to act where a transaction is likely to reduce competition on that basis. But it concluded that in this particular transaction, harm to competition on privacy was no more likely than harm to competition on price or other nonprice dimensions. Consequently, it determined that "privacy considerations, as such, do not provide a basis to challenge this transaction."[46] The EC also evaluated the transaction solely by analyzing competitive effects, while emphasizing that its decision was without prejudice to the parties' separate obligations under European data protection law.[47]

***Facebook/WhatsApp Provides Recent Guidance.*** The FTC confronted similar complaints in its recent review of Facebook's proposed acquisition of WhatsApp. Facebook, a social network with over a billion active monthly users worldwide, also offers communication services that allow users to share text messages, photos, and other digital content through its "Messenger" smartphone application, as well as through the messaging function within its social network. On February 19, 2014, Facebook announced that it had agreed to acquire mobile messaging company WhatsApp for $16 billion.[48] Like Facebook Messenger, WhatsApp offers a mobile application that allows subscribers to send text messages and other digital content to users over the Internet, without incurring short message service charges. When the acquisition was announced, WhatsApp was reported to have 450 million users worldwide, the majority outside the United States. Facebook indicated that Messenger had 200 million regular users.[49]

At least in part, WhatsApp has marketed itself on the fact that it does not mine consumers' personal data to sell advertising. According to WhatsApp, "Your data isn't even in the picture. We are simply not interested in any of it."[50] The day the acquisition was announced, WhatsApp told users that the transaction would change "nothing" for them in this regard.[51] A few days later, Facebook Chief Executive Mark Zuckerberg was reported to have said that Facebook was not going to "change plans around WhatsApp and the way it uses user data."[52]

Despite these assurances, privacy advocates articulated concerns about the transaction. EPIC and CDD filed complaints with the FTC objecting to the proposed acquisition and echoing many of the arguments made against Google/DoubleClick.[53] In particular, they claimed that Facebook's business model was at odds with the representations WhatsApp had made to users about how their smartphone data would be collected and used, and that WhatsApp did not adequately disclose that its privacy commitments were subject to reversal, or that subscriber data could be transferred in the event of an acquisition. They urged the FTC to investigate WhatsApp's conduct and to use its "authority to review mergers to halt Facebook's proposed acquisition of WhatsApp" until the issues described in the complaint had been adequately resolved. In the event the FTC cleared the transaction, the groups asked the agency to "order Facebook to insulate WhatsApp users' information from access to Facebook's data collection practices."[54]

On April 10, 2014, Facebook announced that the FTC had cleared the transaction.[55] When the FTC closes a merger investigation without taking action, it does not typically issue a statement explaining the details of its review, and it did not do so here. However, the day Facebook announced clearance, the Director of the FTC Bureau of Consumer Protection, Jessica Rich, sent a letter to Facebook and WhatsApp explaining that Facebook's purchase of WhatsApp would not nullify the promises made by Facebook and WhatsApp in WhatsApp's privacy policies as well as the public statements about privacy made by both companies when the transaction was announced. Rich explained that, as a consequence, the companies should not make any material changes

to how they use data already collected from WhatsApp subscribers without affirmative express consent or misrepresent how they maintain WhatsApp user data. She advised that failure to take these steps could constitute deceptive or unfair acts and practices in violation of the FTC Act as well as a 2012 FTC consent order against Facebook.[56] While Rich's letter was issued at the time the investigation was closed, it did not impose conditions on the merger, something the FTC does through the consent decree process when it finds reason to believe a transaction is likely to harm competition. Instead, the letter articulates the obligations that apply to all companies with respect to the collection, storage, and use of consumer information, both before and after a merger.

The EC opened an investigation of the Facebook/WhatsApp merger on August 29, 2014. In announcing it had cleared the merger without conditions on October 3, 2014, the EC explained that the merger was unlikely to harm competition in three areas of potential concern: consumer communication services, social networking services, and online advertising services.[57] With regard to communication services, the EC determined that while both Facebook Messenger and WhatsApp perform similar functions, the firms were not close rivals, in part because Messenger connects users through their Facebook profiles, while WhatsApp relies on mobile phone numbers. The EC found that consumers tend to use the services in different ways, with many using both applications on the same device. In addition, the EC determined that the market for digital communication services was growing rapidly and barriers to launching new applications were relatively low. While recognizing that network effects can sometimes limit entry in communications markets, the EC concluded that the merger was not likely to raise barriers here because "consumers can and do use multiple apps at the same time and can easily switch from one to another." The EC concluded similarly that in the area of social networking, the firms are at most "distant competitors" in a dynamic market with no precise boundaries and many potential players.[58]

Finally, the EC discounted the likelihood of competitive harm in online advertising. Echoing its analysis in Google/DoubleClick, the EC determined that even if Facebook were to use WhatsApp to expand the store of data it uses to target advertising, it would continue to face meaningful competition in this market, in part because data on consumers' online behavior are available to rivals from alternative sources. In clearing the merger, the EC did not evaluate privacy risks associated with the "potential data concentration" that were not relevant to analyzing competitive effects. Instead, it concluded, as it had in Google/DoubleClick, that "[a]ny privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of EU Competition law."[59]

***Privacy Risks that Flow from Enhanced Market Power.*** The available guidance from the FTC and the EC indicates that merger enforcement can play a role in safeguarding consumer privacy in both jurisdictions only where there is a factual basis to tie any privacy risks to enhanced market power or a lessening of competition.

Several broad factual patterns might potentially support that nexus and come into play in future mergers. For example, a combination of data associated with a merger can enhance market power and raise privacy concerns. In its analysis of Google/DoubleClick, both the FTC and the EC examined whether the combination of Google's customer search data with DoubleClick's browsing data would give AdSense an advantage that rivals could not match, restricting competition in online advertising intermediation services. Though both jurisdictions decided that the merger would not give Google exclusive control of an asset needed to compete effectively, both recognized a valid theory of competitive harm if the facts had shown otherwise, something Joaquín Almunia, the EC Commissioner for Competition, later affirmed.[60] Similarly, in Facebook/WhatsApp, the EC also asked whether the combination of data could strengthen Facebook's position in online advertising and harm competition, though ultimately rejecting that theory for reasons that mirrored its analysis in Google/DoubleClick.[61] However, given the prevalence of network effects in many digital markets, if the information necessary to compete on equal footing is not readily available from alternative sources, the potential competitive harm from data-driven entry barriers raises a cognizable theory of competitive harm under the antitrust laws. It is worth noting that, to date, both the FTC and the EC have examined whether anticompetitive foreclosure is likely in big data mergers *even if* the merged entity were to violate pre-existing commitments regarding the use of the data.[62]

The foreclosure issues that could be associated with the aggregation of data do not raise particularly novel questions from the perspective of merger enforcement. Data can be treated as an asset, and both jurisdictions commonly evaluate whether a transaction will restrict competition by combining assets that otherwise would be in the hands of competing entities. Last year, for example, the FTC challenged Nielsen Holdings N.V.'s acquisition of Arbitron Inc. because it believed the transaction was likely to harm competition in the market for national syndicated cross-platform audience measurement services (capable of tracking viewers across television and Internet platforms). That decision was grounded largely in the fact that Nielsen and Arbitron were the only two companies that maintained the broad audience measurement panels necessary to compete in the downstream cross-platform market. Similarly, where the merging parties are competing sellers of data, the combination could raise privacy concerns and, depending on the particular facts, also harm competition in a market for the overlapping product. Both agencies have seen numerous mergers that implicate a market for data, and both have analyzed the competitive effects under standard unilateral and coordinated effects frameworks. For example, in a recent merger the FTC

defined a market for national assessor and recorder bulk data, and found that the merger was likely to harm competition in that market.[63]

But parallel goals between privacy and competition associated with big data mergers that enhance market power may diverge at the remedy stage. Since data usually can be copied at a reasonable cost, the agencies might resolve any likely competitive harm associated with a merger by requiring the merging parties to divest a copy of the data to an entrant.[64] This was the approach the FTC took in Nielsen/Arbitron, where it required the merging parties to license Arbitron's demographic data to a new entrant capable of restoring competition in the cross-platform measurement market.[65] Similarly, the EC cleared a merger between Thomson and Reuters that raised concerns in markets for financial data only after accepting binding commitments that required the parties to divest copies of the competing data products as well as other related assets.[66] Consequently, merger enforcement may not always address privacy concerns associated with aggregating data because even where there is potential antitrust liability, a divestiture that remedies the competitive harm may leave the combined data with the merged entity. However, in fashioning a divestiture remedy, antitrust enforcement agencies would be likely to take into account a company's prior commitments concerning the transfer and use of data, as well as other privacy-related legal obligations or concerns.

Other fact patterns may also create a link between privacy and competitive harm. Customers may choose products and services at least in part on the basis of privacy or other nonprice product attributes, such as quality and customer service.[67] Both jurisdictions acknowledge the role of nonprice competition in their merger guidelines, and the FTC recognized privacy as a nonprice dimension of competition in Google/DoubleClick even before adopting new horizontal merger guidelines expressly recognizing nonprice competition in 2010.[68] Whether a likely reduction in competition on privacy will drive the outcome in any particular transaction depends on the facts. Key questions the agencies are likely to ask are whether privacy is an important competitive dimension in the market and whether the merger is likely to reduce that competition through either unilateral or even, potentially, coordinated effects. To date, neither jurisdiction has challenged a merger based solely on the loss of any form of nonprice competition, but it could be an important theory for evaluating competitive harm in digital markets where nonprice dimensions of competition, like innovation and privacy, may play a more important role in marketplace dynamics.

## Conclusion

Despite the potential nexus between privacy risks and big data mergers, guidance from both the United States and the EU strongly suggests that neither jurisdiction will use antitrust enforcement to challenge a merger that raises privacy concerns that are not tied to a lessening of competition. Both the FTC and the EC declined that opportunity in Google/DoubleClick and Facebook/WhatsApp, and a contrary result would be inconsistent with the merger enforcement guidelines in both jurisdictions, which evaluate transactions solely through the lens of competitive effects. Consequently, merger enforcement has the potential to complement privacy law only in those circumstances where protecting competition has the added benefit of protecting consumer privacy. Antitrust regulators in the United States and the EU have yet to take action in a case where that relationship was apparent. But as new technologies and business models make data collection and analysis a nearly ubiquitous feature of everyday life, we can expect questions about the role of antitrust enforcement in protecting consumers from privacy risks that may be associated with digital market mergers will continue to surface in merger reviews on both sides of the Atlantic.

---

1 *See, e.g.*, Art. 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things (Sept. 16, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf; Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012) [hereinafter FTC Privacy Report], *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

2 15 U.S.C. §§ 6501–6506.

3 Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

4 15 U.S.C. §§ 6801–6809.

5 15 U.S.C. §§ 1681–1681x.

6 18 U.S.C. § 2710.

7 *See, e.g.*, Asia-Pacific Economic Cooperation, Privacy Framework (2005); Organization for Economic Co-Operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (rev. ed. 2013).

8 15 U.S.C. § 45(a). *See also id.* § 45(n) ("[An unfair] act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition").

9 Complaint at 2–3, The TJX Cos., FTC Docket No. C-4227 (Aug. 1, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.

10 Complaint at 2–4, Snapchat, Inc., FTC File No. 132 3078 (May 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf.

11 Complaint at 7–9, Facebook, Inc., FTC Docket No. C-4635 (July 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf.

12 *See, e.g.*, Complaint at 1–5, Aaron's, Inc., FTC Docket No. C-4442 (Mar. 10, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140311aaronscmpt.pdf; Complaint 6–7, DesignerWare, LLC, FTC Docket No. C-4390 (Apr. 11, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf; Complaint 4–5, Aspen Way Enters., Inc., FTC Docket No. C-4392 (Apr. 11, 2013),

*available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt.pdf.

[13] Complaint at 18–20, FTC v. Frostwire LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011).

[14] *See generally* Pam Dixon & Robert Gellman, The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future 9–11 (2014), *available at* http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf; Press Release, Fed. Trade Comm'n, FTC Announces Agenda, Panelists for Alternative Scoring Seminar (Mar. 14, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/ftc-announces-agenda-panelists-alternative-scoring-seminar.

[15] FTC Privacy Report, *supra* note 1, at 12–13; Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 49–54 (2014) [hereinafter FTC Data Broker Report].

[16] *See* The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 35–39 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[17] *See, e.g.*, Cal. Civ. Code §§ 1798.29, 1798.80–84 (West 2014); Mass. Gen. Laws ch. 93H, §§ 1–6 (2014); N.C. Gen. Stat. §§ 75–61, 75–65 (2014).

[18] Cal. Bus. & Prof. Code §§ 22575–22579 (West 2014).

[19] *See, e.g.*, 815 Ill. Comp. Stat. 505/2 (2014); Iowa Code § 714.16(2)(a) (2014); Mass. Gen. Laws ch. 93A, § 2(a) (2014).

[20] *See, e.g.*, Press Release, Office of the Conn. Att'y Gen., Connecticut, 36 Other States Reach $17M Settlement with Google (Nov. 18, 2013), *available at* http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=535258 (settling allegations Google deceptively circumvented default block on third-party cookies).

[21] *See, e.g.*, Joffe v. Google, Inc., 746 F.3d 920 (9th Cir. 2013), *cert. denied*, 134 S. Ct. 2877 (mem.) (2014); Order Granting Motion for Preliminary Approval of Class Action Settlement, *In re* Google Referrer Header Privacy Litig., No. 5:10-cv-04089 (N.D. Cal. July 25, 2014); Order Granting Final Approval of Settlement Agreement, Fraley v. Facebook, Inc., No. 3:11-cv-01726-RS (N.D. Cal. Aug. 26, 2013), *appeal filed*, No. 13-16918 (9th Cir. 2013); *see also* Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (Feb. 17, 2014, 10:19 AM), http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=84&pageNumber=1 (listing private lawsuits yielding ten highest payments).

[22] Charter of Fundamental Rights of the European Union art. 8, 2000 O.J. (C 364) 1, art. VIII.

[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 1995 O.J. (L 281) 31.

[24] *Id.* art. 1(1); *id.* art. 28.

[25] *Id.* art. 6(1)(a)–(b).

[26] *Id.* art. 7(a).

[27] *Id.* art. 6(1)(c).

[28] *Id.* art. 10–11.

[29] *Id.* art. 17.

[30] *Id.* art. 12.

[31] Case C-131/12, Google Spain, SL v. Agencia Española de Protección de Datos ¶¶ 33, 81, Celex No. 612CJ0131 (Eur. Ct. Justice May 13, 2014), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=63817.

[32] European Parliament Legislative Resolution of 12 March 2014 on the General Data Protection Regulation, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN; Press Release, Eur. Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014), *available at* http://europa.eu/rapid/press-release_MEMO-14-186_en.pdf.

[33] *See, e.g.*, *France Slaps Google with Maximum Fine, Citing Privacy Concerns*, France24 (Jan. 9, 2014), http://www.france24.com/en/20140109-france-fines-google-maximum-penalty-privacy-row/ (noting maximum privacy fines of 150,000 euros under French law, 1 million euros under Spanish law, and 300,000 euros under German law).

[34] *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (Sept. 15, 2014) [hereinafter Ramirez comments] (noting concern that enhanced ability to differentiate among consumers may reinforce existing socio-economic disparities), *available at* http://www.ftc.gov/system/files/documents/public_statements/582421/big_data_workshop_opening_remarks_ftc_chairwoman_edith_ramirez_9-15-14.pdf Well-established microeconomic theory indicates that price discrimination will often expand output, though the consumer welfare implications vary depending on how prices are structured. *See, e.g.*, F.M. Scherer & David Ross, Industrial Market Structure and Economic Performance 494–508 (3d ed. 1990).

[35] *See, e.g.*, Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values 51–53 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf; Ramirez Comments, supra note 34; FTC Data Broker Report at 55–57.

[36] European Data Prot. Supervisor, Preliminary Opinion, Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy 30 (2014), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf.

[37] European Data Prot. Supervisor, Report of Workshop on Privacy, Consumers, Competition And Big Data (2014), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdf. While the workshop report echoes many of the themes from the Preliminary Opinion, it adopted a more cautious approach to expanding the concept of consumer welfare in antitrust investigations, noting that "Arguing that data protection should be 'an additional factor' in competition enforcement is unlikely to gain much support," and asking regulators instead to consider "how can we apply the 'parameters of competition'—especially price, quality and choice—in explaining impact on privacy and data protection?" *Id.* at 6.

[38] Dissenting Statement of Commissioner Pamela Jones Harbour, Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf.

[39] *See* Pamela Jones Harbour, *The Transatlantic Perspective: Data Protection and Competition Law*, *in* Data Protection Anno 2014: How to Restore Trust? 225 (Hielke Hijmans & Herke Kranenborg eds., 2014); *see also* Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 Antitrust L.J. 769 (2010).

[40] *See* Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. Pa. L. Rev. 1663, 1688 (2013).

[41] Statement of Federal Trade Commission, Google/DoubleClick, FTC File No. 071-0170, at 3 (Dec. 20, 2007) [hereinafter FTC Google/DoubleClick Statement], *available at* http://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf; Decision of the Eur. Comm'n, Google/DoubleClick, Case No. COMP/M.4731 (Nov. 3, 2008) [hereinafter EC Google/DoubleClick Statement], *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf.

[42] *See* Ellen Nakashima, *Privacy Group Objects to DoubleClick Deal*, Wash. Post (Apr. 20, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/04/19/AR2007041902647_pf.html.

[43] Complaint and Request for Injunction, Request for Investigation and for Other Relief at 10, Elec. Privacy Info. Ctr., In re Google, Inc. and DoubleClick,

Inc. (Apr. 20, 2007), *available at* http://www.epic.org/privacy/ftc/google/epic_complaint.pdf.

[44] Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief at 15, Elec. Privacy Info. Ctr., In re Google, Inc. and DoubleClick, Inc. (June 6, 2007), *available at* http://www.epic.org/privacy/ftc/google/supp_060607.pdf.

[45] Press Release, Fed. Trade Comm'n, Federal Trade Commission Closes Google/DoubleClick Investigation (Dec. 20, 2007), *available at* http://www.ftc.gov/news-events/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation; Press Release, Eur. Comm'n, Mergers: Commission Clears Proposed Acquisition of DoubleClick by Google (Mar. 11, 2008), http://europa.eu/rapid/press-release_IP-08-426_en.pdf.

[46] FTC Google/DoubleClick Statement, *supra* note 41, at 2–3.

[47] EC Google/DoubleClick Statement, *supra* note 41, at 97–98.

[48] Press Release, Facebook, Inc., Facebook to Acquire WhatsApp (Feb. 19, 2014) http://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp.

[49] *Id.*; Robert McMillan, *You May Not Use WhatsApp But the Rest of the World Sure Does*, WIRED (Feb. 20, 2014, 8:17 PM), http://www.wired.com/2014/02/whatsapp-rules-rest-world/; Mike Isaac, *Zuckerberg: More Than 200 Million People Use Facebook Messenger*, RE/CODE (Apr. 23, 2014, 3:04 PM), http://recode.net/2014/04/23/zuckerberg-more-than-200-million-people-use-facebook-messenger.

[50] *Why We Don't Sell Ads*, WHATSAPP BLOG (June 18, 2012), http://blog.whatsapp.com/245/Why-we-dont-sell-ads.

[51] *Facebook*, WHATSAPP BLOG (Feb. 19, 2014), http://blog.whatsapp.com/499/Facebook.

[52] *See* Jessica Guynn, *Mark Zuckerberg: WhatsApp Worth Even More Than $19 Billion*, L.A. TIMES (Feb. 24, 2014), http://articles.latimes.com/2014/feb/24/business/la-fi-tn-mark-zuckerberg-whatsapp-worth-even-more-than-19-billion-20140224.

[53] Complaint, Request for Investigation, Injunction, and Other Relief, Elec. Privacy Info. Ctr. & Ctr. for Digital Democracy, In re WhatsApp, Inc. (Mar. 6, 2014) [hereinafter EPIC-CDD WhatsApp Complaint], *available at* http://www.centerfordigitaldemocracy.org/sites/default/files/WhatsApp%20Complaint.pdf; Supplemental Materials in Support of Pending Complaint, Request for Investigation and Injunction, and Other Relief; Related Commentary Concerning Commission's Surprising Expedition of Google-Nest Review, Elec. Privacy Info. Ctr. & Ctr. for Digital Democracy, In re WhatsApp, Inc. (Mar. 21, 2014) [hereinafter EPIC-CDD WhatsApp Supplemental Materials], *available at* http://epic.org/privacy/internet/ftc/whatsapp/WhatsApp-Nest-Supp.pdf.

[54] EPIC-CDD WhatsApp Complaint, *supra* note 53, at 13–14. In their Supplemental Materials, EPIC and CDD claimed that the merger itself constituted an unfair or deceptive act or practice. EPID-CDD WhatsApp Supplemental Materials, *supra* note 53, ¶ 5.

[55] Alexei Oreskovic, *Facebook Says WhatsApp Deal Cleared by FTC*, REUTERS (Apr. 10, 2014, 4:12 PM), http://www.reuters.com/article/2014/04/10/us-facebook-whatsapp-idUSBREA391VA20140410.

[56] Letter from Jessica Rich, Dir., Bureau of Consumer Protection, Fed. Trade Comm'n, to Erin Egan, Chief Privacy Officer, Facebook, Inc., and Anne Hoge, Gen. Counsel, WhatsApp Inc. (Apr. 20, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

[57] Press Release, Eur. Comm'n, Mergers: Commission Approves Acquisition of WhatsApp by Facebook (Oct. 3, 2014) [hereinafter EC Facebook/WhatsApp Release], http://europa.eu/rapid/press-release_IP-14-1088_en.pdf; Tom Fairless, *EU Looks Poised to Approve Facebook's Purchase of WhatsApp*, WALL ST. J. (Sept. 25, 2014, 4:28 PM), http://online.wsj.com/articles/eu-looks-poised-to-approve-facebooks-purchase-of-whatsapp-1411666891.

[58] EC Facebook/WhatsApp Release, *supra* note 57, at 1.

[59] *Id.* at 2.

[60] Joaquín Almunia, Vice-President for Competition Policy, European Comm'n, Remarks at Privacy Platform Event: Competition and Privacy in Markets of Data, Competition and Personal Data Protection (Nov. 26, 2012), *available at* http://europa.eu/rapid/press-release_SPEECH-12-860_en.pdf. Almunia's term expired on October 31, 2014, and Margrethe Vestager assumed responsibility as the Commissioner for Competition for the EC on November 3, 2014.

[61] EC Facebook/WhatsApp Release, *supra* note 57, at 2.

[62] *See* FTC Google/DoubleClick Statement, *supra* note 41, at 12; EC Google/DoubleClick Statement, *supra* note 41, at 96; EC Facebook/WhatsApp Release, *supra* note 58, at 2 (evaluating competitive effects if, despite the commitments the parties made at the time the merger was announced, Facebook were to introduce advertising on WhatsApp or use WhatsApp data to improve targeted advertising on Facebook).

[63] Analysis of Agreement Containing Consent Order to Aid Public Comment, CoreLogic, Inc., FTC File No. 131-0199 (Mar. 24, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140324corelogicanalysis.pdf. While many of the mergers that the agencies have analyzed involving markets for data have not involved the same consumer-facing data at issue in the Google/DoubleClick and Facebook/WhatsApp transactions, the FTC and EC statements in Google/DoubleClick, as well as the EC's press release in Facebook/WhatsApp, suggest the antitrust principles are the same.

[64] For the same reason, any claimed efficiencies associated with the combination of data may not be credited as merger specific since they may be available through arrangements short of a merger. *See* U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines 30 n.15 (2010) [hereinafter U.S. Horizontal Merger Guidelines], *available at* http://www.ftc.gov/os/2010/08/100819hmg.pdf.

[65] Statement of the Federal Trade Commission, Nielson Holdings N.V. and Arbitron Inc., FTC File No. 131-0058 (Sept. 20, 2013), *available at* http://www.ftc.gov/system/files/documents/cases/140228nielsenholdingstatement.pdf. *See also* Analysis of Agreement Containing Consent Order to Aid Public Comment, Fidelity National Financial, Inc./Lender Processing Services, Inc., FTC File No. 1310159 (Dec. 24, 2014) (requiring divestiture of the acquired firm's title plants to an approved buyer in each geographic market adversely affected by the merger), *available at* http://www.ftc.gov/sites/default/files/documents/cases/131224fidelityanal.pdf.

[66] Press Release, Eur. Comm'n, Mergers: Commission Clears Acquisition of Reuters by Thomson Subject to Conditions (Feb. 19, 2008), http://europa.eu/rapid/press-release_IP-08-260_en.pdf. The DOJ accepted a similar remedy to settle its challenge to the transaction. *See* Press Release, U.S. Dep't of Justice, Justice Department Requires Thomson to Sell Financial Data and Related Assets in Order to Acquire Reuters (Feb. 19, 2008), http://www.justice.gov/atr/public/press_releases/2008/230250.pdf.

[67] The economic literature on the relationship between competition and privacy is not well developed. While competition may under some circumstances promote privacy, market imperfections—such as information asymmetries—may in some cases impede effective competition on this aspect of the quality of a product or service. *See, e.g.*, Joseph E. Stiglitz, *Imperfect Information in the Product Market*, *in* 1 HANDBOOK OF INDUSTRIAL ORGANIZATION 769–848 (Richard Schmalensee & Robert D. Willig eds., 5th ed. 1998). It is therefore not possible to know with any certainty whether merger enforcement has played a role in protecting consumer privacy, such as by encouraging enhanced data security or stronger privacy practices. For a recent effort to explore empirically the relationship between competition and data security, see Martin Gaynor et al., *Is Patient Data Better Protected in Competitive Healthcare Markets?* Research Paper, Presented at the Workshop on the Economics of Information Security 2012, *available at* http://weis2012.econinfosec.org/papers/Gaynor_WEIS2012.pdf (finding a greater incidence of hospital data breaches in less concentrated markets and positing that hospitals in more competitive markets may be inclined to shift resources to more consumer visible activities from the less visible activity of safeguarding consumer data).

[68] U.S. Horizontal Merger Guidelines, *supra* note 64, at 2; Guidelines on the Assessment of Horizontal Mergers Under the Council Regulation on the Control of Concentrations Between Undertakings 2004 O.J. (C 31) 5, ¶ 8, *available at* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52004XC0205(02).