COMPETITION, CONSUMER PROTECTION, AND *THE RIGHT* [APPROACH] *TO PRIVACY*

MAUREEN K. OHLHAUSEN
ALEXANDER P. OKULIAR*

Many people view Samuel Warren and Louis Brandeis's 1890 work, *The Right to Privacy*,[1] as the starting point for the consumer privacy laws in the United States. 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,'" they argued for the right to prevent invasions of privacy by the press, particularly by photographers, and "to be let alone."[2] Noting the protections for private letters and for works of art and literature, which they characterize as "a general right to privacy for thoughts, emotions, and sensations," Warren and Brandeis asserted "these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression."[3]

Warren and Brandeis's concerns about the ability of technology to invade the private sphere continue to resonate today, 125 years later. The technology encroaching on privacy now is, of course, the Internet—or, to be more precise, the technologies that permit the tracking and aggregation of individual consumers' online behavior and that support the many services that financially sustain the broader Internet ecosystem. These technologies also facilitate the advent of "big data"—a term used to describe the collection, storage, and analysis of datasets that have large volume, significant variety, and high velocity, sometimes fed by the melding of online and offline data.

---

* The authors are, respectively, Commissioner and Attorney Advisor to Commissioner Ohlhausen, Federal Trade Commission. The views expressed herein are those of the authors alone and do not represent the views of the FTC or any other Commissioner.

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[2] *Id.* at 195.

[3] *Id.* at 206.

Nearly everyone agrees the Internet has transformed how we live and interact, largely for the better. Similar optimism exists about the benefits of big data.[4] But not everyone agrees on how much this transformation has, or should, cost in terms of privacy losses. Ardent advocates of an "Internet of Things" believe that people are consciously choosing to trade at least some privacy for otherwise free and improved content and services. For instance, Facebook CEO Mark Zuckerberg famously claimed privacy is disappearing as a social norm.[5] Many consumers, however, are worried about the privacy losses associated with extensive collection and manipulation of consumer information online.[6]

As was the case in Warren and Brandeis's day, numerous proposals have surfaced for how to defend expectations of personal privacy while still realizing the benefits of commercialized technology. Those defending free market principles argue that the best solution is little-to-no government intervention—consumer demand for privacy will create a market for privacy protections.[7] Other commentators propose increased governmental scrutiny of the collection and use of consumer data online, and some even advocate unifying the competition and consumer protection laws to examine privacy through a competition lens.[8]

Evaluating this last proposal—using competition law to address privacy concerns—is the focus of this paper. To do so, we first look to history. To-

---

[4] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 34 (May 2014) [hereinafter BIG DATA REPORT], *available at* www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; *id.* at 5 ("Used well, big data analysis can boost economic productivity, drive improved consumer and government services, thwart terrorists, and save lives.").

[5] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, THE GUARDIAN (Jan. 10, 2010), www.theguardian.com/technology/2010/jan/11/facebook-privacy. Internet pioneer Vint Cerf neatly summed up the personal tension between privacy and interconnectivity at a talk at the Federal Trade Commission, noting: "Technology use today has far outstripped our social intuition[.]" Paul Roberts, *At FTC Forum, Experts Wonder: Is Privacy Passé?*, THE SECURITY LEDGER (Nov. 20, 2013) (quoting Vint Cerf).

[6] *See, e.g.*, TRUSTE, TRUSTE 2014 US CONSUMER CONFIDENCE PRIVACY REPORT (2014) (noting increased concerns about privacy among consumers).

[7] *See, e.g.*, Slade Bond, *Doctor Zuckerberg: Or, How I Learned to Stop Worrying and Love Behavioral Advertising*, 20 KAN. J.L. & PUB. POL'Y 129 (2010); Kent Walker, *The Costs of Privacy,* 25 HARV. J.L. & PUB. POL'Y 87, 87–88 (2001) ("Legislating privacy comes at a cost: more notices and forms, higher prices, fewer free services, less convenience, and, often less security. More broadly, if less tangibly, laws regulating privacy chill the creation of beneficial collective goods and erode social values. Legislated privacy is burdensome for individuals and a dicey proposition for society at large.").

[8] *See, e.g.*, Robert H. Lande, *The Microsoft-Yahoo Merger: Yes, Privacy Is an Antitrust Concern*, FTC: WATCH NO. 714, at 1 (Feb. 25, 2008); Peter P. Swire, Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall 5–6 (Oct. 18, 2007), *available at* www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony_peterswire_en.pdf; Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. ON TELECOMM. & HIGH TECH. L. 251 (2012).

day's debate about privacy is part of a long-running discussion about the meaning and proper legal protection of privacy in the face of commercial technological change. Earlier periods within this discussion reveal important concepts that offer lessons for current analysis. For instance, Warren and Brandeis established the need for personal privacy in the 1890s; the Federal Trade Commission showed the risk of undisciplined enforcement with its early failed attempts to expand its competition mandate to reach consumer protection issues; the debate over credit reporting practices in the 1960s and legislation like the Fair Credit Reporting Act of 1970 (FCRA) created a potentially instructive path for balancing reasonable privacy protections with new commercial technology that uses personal information; and, finally, the review of mergers in data-driven industries by federal antitrust agencies demonstrated how valuable personal data can have competitive significance and is susceptible to antitrust analysis using existing empirical tools.[9]

We explore these events for insights into the best role for the antitrust and consumer protection authorities in the United States in dealing with ongoing concerns about privacy. From this historical analysis we derive three factors to approach privacy concerns under the right analytical framework. First, the character of the harm—whether it is commercial, personal, or otherwise—is paramount to the analysis and helps identify the right legal approach to the conduct. For example, conduct that creates harm by reducing economic efficiency is likely best resolved under the antitrust laws. Second, if the potential harm undermines the terms of the particular bargain between a company and an individual consumer, the solution is less likely to lie in competition law than in consumer protection or another area of law. Third, the remedy available under the law must be able to address the problem effectively and efficiently. The appropriate body of law will be the one that offers remedies best calibrated to address the identified potential harm.[10]

This article proceeds in three main parts. We begin with the historical development of privacy protections in the United States and the tension between

---

[9] *See, e.g.*, Press Release, Statement of the Department of Justice Antitrust Division on Its Decision to Close Its Investigation of the Internet Search and Paid Search Advertising Agreement Between Microsoft Corporation and Yahoo! Inc. (Feb. 18, 2010), *available at* www.justice.gov/atr/public/press_releases/2010/255377.pdf; Press Release, U.S. Dep't of Justice, NASDAQ OMX Group Inc. and IntercontinentalExchange Inc. Abandon Their Proposed Acquisition of NYSE Euronext After Justice Department Threatens Lawsuit (May 16, 2011) [hereinafter DOJ NASDAQ/NYSE Release], *available at* www.justice.gov/opa/pr/2011/May/11-at-622.html; Standfacts Credit Servs. v. Experian Info. Solutions Inc., 294 Fed. App'x 271, 272 (9th Cir. 2008) (noting relevant market consisting of wholesale credit data).

[10] For example, blocking a merger of two companies with large consumer datasets solely to protect privacy under the competition laws may not be the right approach because those companies could still enter a data-sharing arrangement that could subvert the intent of the enforcement action. Rather, it may be more prudent to monitor the merged entity's subsequent treatment of consumer data and ensure it is keeping its promises under its privacy policies.

privacy concerns and the growing value of consumer data in the digital arena. Next, we explore how the agencies and courts have applied the law in this area over the years and the reasoning behind the bifurcation of the FTC Act into separate spheres of competition and consumer protection law. This explains the historical separation of the law's treatment of privacy as a personal consumer expectation from commercialized privacy and data. Third, we synthesize analytical factors from the historical approaches to privacy and offer them as guidance for distinguishing between competition and consumer protection issues at the intersection of the laws pertaining to competition, consumer protection, and privacy.

I. THE HISTORICAL TENSION BETWEEN PRIVACY AND COMMERCE IN THE UNITED STATES

In the United States, much of the conceptual grounding of privacy is in our collective belief in rights to life, liberty, and property.[11] The original national understanding of privacy evolved from concepts associated with English common law trespass and classical liberal thought that emerged with European enlightenment thinkers.[12] The Constitution was the first national embodiment of the American belief in privacy as a personal right, albeit written there as a right to be free from unreasonable governmental intrusions.[13] From its roots as a way to safeguard the individual's liberty vis-à-vis the government, the concept grew to include private actors as early as 1782, when Congress passed a law prohibiting the opening of mail.[14]

The modern norms of individual privacy, however, did not coalesce until nearly a century later, largely in response to the technological change of the Second Industrial Revolution. In this era, advances like the camera and widespread daily printing and distribution of newspapers increased economic de-

---

[11] Privacy scholars often distinguish among the many different philosophical explanations for the individual's need for, and scope of, personal privacy. ADAM D. MOORE, PRIVACY RIGHTS, MORAL AND LEGAL FOUNDATIONS 14–15 (2010) (offering an excellent overview of the development of privacy expectations in the United States). Professor William Parent said that descriptive privacy "is the *condition* of not having undocumented personal knowledge about one possessed by others." W.A. Parent, *Privacy, Morality, and the Law*, 12 PHIL. & PUB. AFF. 269, 269 (1983) (emphasis added). Normative privacy, on the other hand, "makes references to moral obligations or claims." MOORE, *supra*, at 14. Moore discusses the dispute between advocates of the reductionist and nonreductionist (or coherentist) views of privacy. The former view privacy as derived from other rights; the latter view it mainly as a right in and of itself. *Id.* at 14–15. This debate is outside the scope of this article.

[12] *See* United States v. Jones, 132 S. Ct. 945, 949–51 (2012) (explaining the history of the Fourth Amendment).

[13] *Id.* at 949.

[14] Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY § 1:3.1[B] (PLI Treatise 2006). Common law prohibitions on eavesdropping date much earlier. *Id.* § 1.2.

mand for personal information, raising questions about whether and how the law could protect individual political and social freedoms.

Personal privacy laws in the United States have evolved in three phases during the modern era. The first period began with Warren and Brandeis and lasted until about the Second World War. This period exhibited a growing recognition of personal privacy and the attempt to protect privacy by extending existing doctrines of law, like trespass. Next came the post-War era and early computer age, in which federal laws developed to augment state and common laws and help reconcile the growing commercialization of personal data and the need to protect the individual; and finally, the modern era that began with commercial use of the Internet in the 1990s and in which we now find ourselves.

A. THE EARLY YEARS OF PERSONAL PRIVACY LAW IN THE UNITED STATES

In the late 1800s era of technological change, Warren and Brandeis captured the modern American understanding of personal privacy.[15] They wrote their article largely in response to the creation of the portable camera by Kodak in 1888 and the subsequent rise of gossip journalism.[16] Warren and Brandeis identified the tension apparent at this time between enjoying the personal and commercial benefits of new technology and the individual's instinct to shield intimate details from prying eyes.[17] Their work represented an early recognition that unwanted exposure of personal details could create harm, even if the actor divulging or using that information was someone other than the government. They wrote, "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world . . . but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[18] They argued that the rise of commerce and technology was creating an invasion of the person similar to an intrusion by the government on the individual's "right to be let alone":

---

[15] But their work was not the first to express the notion that an individual has some right to be left alone. That honor likely goes to Judge Thomas Cooley and his 1878 treatise on torts. There, he asserted that the "right to one's person may be said to be a right of complete immunity: to be let alone." THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (Chicago, Callaghan & Co. 2d ed. 1888).

[16] LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 49–50 (2012); Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 644 (2007); Leah Burrows, *To Be Let Alone: Brandeis Foresaw Privacy Problems*, BrandeisNOW (July 24, 2013), www.brandeis.edu/now/2013/july/privacy.html.

[17] *See* Warren & Brandeis, *supra* note 1.

[18] *Id.* at 196.

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the particular method of expression adopted.[19]

Their article was timely and influential. Before 1890, very few significant jurisdictions allowed individuals to prevent others from distributing information about them. The shift was almost immediate. The State of New York became one of the first jurisdictions to recognize an explicit right to privacy with a decision in 1890. That year, a state court granted an injunction blocking the publication of a photograph of an actress taken without permission.[20] Within a few decades, most states had recognized some legal right to privacy under the tort laws.[21]

In 1915, legal scholar Roscoe Pound, building on the work of Warren and Brandeis, noted that the law had been slow to recognize the growing consensus on personal privacy as a legal right, but that the tide was shifting. He wrote,

> [I]t would seem . . . the invasions of privacy by reporters in competition for a "story," the activities of photographers, and the temptation to advertisers to sacrifice private feelings to their individual gain call upon the law to do more in the attempt to secure this interest than merely taking incidental account of infringements of it.[22]

He argued that a "man's feelings are as much a part of his personality as his limbs."[23]

Warren, Brandeis, Pound, and others advanced early 20th century social norms about privacy beyond their original base in physical trespass to encompass a wider range of harms. The resulting body of privacy law grew to include prohibitions on using an individual's image for commercial reasons

---

[19] *Id.* at 198–99 (internal citation omitted).

[20] JOHN M. SHARP, CREDIT REPORTING AND PRIVACY 52–53 (1970). However, several years earlier, a Michigan court had granted recovery to a woman alleging that a young man had intruded upon her in childbirth without her consent. *See* De May v. Roberts, 46 Mich. 160 (1881). The court did not offer a basis for its decision, but Dean William Prosser drew the conclusion in his 1960 law review article that, "In retrospect, at least, this was a privacy case." William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[21] SHARP, *supra* note 20, at 53.

[22] Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 343, 363 (1915).

[23] *Id.* at 363–64.

without the individual's consent;[24] harassment by telephone;[25] as well as wiretapping and electronic surveillance.[26] The extent of privacy protections has ebbed and flowed in the decades since *The Right to Privacy*, commensurate with changes in American views and the prevailing level of concern about the encroachment of commerce and technology on personal privacy.

B. THE COMPUTER AGE AND EXPANSION OF LAWS ON PRIVACY

The second wave of growth in privacy law occurred after the Second World War, with development in state common law and significant pieces of federal legislation in the 1960s and early 1970s.[27] The catalyst for this growth was the computer and communications technology developed during and after the War, which accelerated corporations' ability to aggregate and use information about consumers for commercial transactions.[28] Consumer credit reporting developed to allow easier and cheaper provision of credit—a development sought as much by consumers as the business community.[29] The potential costs, though, of exposing such personal information to fraud, abuse, or mistake by credit reporting companies raised fears that state law would be inadequate to address the possible harms. These concerns drew the attention of Congress and led to the passage of the FCRA in 1970.[30]

The legislative history of the FCRA, particularly the 1968 Congressional testimony of Retail Credit Co. (predecessor of Equifax Inc.), offers insights into the atmosphere surrounding these developments. Several congressmen,

---

[24] *See, e.g.*, CAL. CIV. CODE § 3344 (West 1997).

[25] *See, e.g.*, 47 U.S.C. § 223.

[26] *See, e.g.*, 18 U.S.C. § 2511.

[27] Americans in the mid-20th century also worried about abuses of privacy by the government. Congress responded by, for instance, passing the Privacy Act of 1974, 5 U.S.C. § 552a, which sets out fair information principles for the collection, maintenance, use, and dissemination of information about individuals held by the federal government. U.S. Dep't of Justice, Overview of the Privacy Act of 1974 (2012), *available at* www.justice.gov/sites/default/files/opcl/docs/1974privacyact-2012.pdf.

[28] *See, e.g.*, *Retail Credit Co. of Atlanta, Ga: Hearing Before a Subcommittee of the Committee on Government Operations*, 90th Cong. 44–45 (May 16, 1968) [hereinafter 1968 Hearing Testimony].

[29] Andrea Ryan, Gunnar Trumbull & Peter Tufano, *A Brief Postwar History of US Consumer Finance* 3–4 (Harvard Business School, Working Paper No. 11-058, 2010), *available at* www.hbs.edu/faculty/Publication%20Files/11-058.pdf.

[30] The Fair Credit Reporting Act, 15 U.S.C. § 1681, was enacted in 1970 and significantly amended in 1996, 2003, and 2010. The FCRA does not limit what information may be collected by credit reporting agencies, but rather focuses on limiting third party access to credit data for permissible purposes (which do not include marketing), ensuring accuracy of such data, providing consumers notice of adverse actions taken against them based on such data, and ensuring consumer access to and ability to correct data about themselves.

including Cornelius Gallagher of New Jersey,[31] grilled the company's executives in exchanges that easily could have taken place today:

> **Mr. Gallagher.** [This] firm, which I am sure you are familiar with, has 35 million names in it and can give a 90-second credit check. Even if a man decides to go west, even before he has purchased a ticket, [the firm] has a credit-rating reference for him out in California or wherever he is going. He said under the growth record that he has had that it would be possible to computerize the level of his file information within a matter of 5 years on every single American. Every American would have a dossier or a profile of some kind within his computer.
>
> At the rate [such firms] and the Associated Credit Bureaus are growing, I wonder whether all of this adds up to a very large national data bank or national intelligence center in the hand of private industry. This would be quite unregulated, there are no restrictions, no regulations, it is all really within the ethics of your own community and the business community. Do you see any need for regulation? Do you see this as a threat in the future?
>
> **Mr. Burge [Retail Credit Co.].** Not at the present time. We share some of the same visions that you do, that the economy is going to continue to grow and that the information needs of business will continue to grow, and that it should be kept a competitive atmosphere.
>
> **Mr. Gallagher.** I don't worry that it is competitive. I do worry about the corrosion of the rights of privacy.
>
> **Mr. Burge.** I have less apprehension so long as it remains within the realm of the private sector because economics govern a great factor in all of this. In addition to that, as I outlined in my statement, the strict proprieties in our responsibilities to all of the parties involved and the overriding consideration of the American businessman that he wants to sell people, not to deny them sales.

---

[31] Congressman Gallagher, Chairman of the House Special Subcommittee on Invasion of Privacy, had a colorful tenure in Congress and a controversial exit. As noted in a biographical sketch in the University of Oklahoma Congressional Archives:

> Gallagher had a variety of causes and interests while in Congress. He especially made a name for himself on privacy issues and was particularly concerned about government invasion of privacy. In 1963 Gallagher proposed a study of lie detector tests used by federal agencies with hearings on the topic being held the following year. Gallagher's Invasion of Privacy Subcommittee held hearings on a proposed National Data Center in 1966 to ensure "that the Government computers do not provide the means by which federal officials can intrude improperly into our lives." An attempt at creating a Select Committee on Privacy, Human Values, and Democratic Institutions failed in 1971. He advocated a civilian review board in 1972 to "cleanse and purge" FBI files following the death of J. Edgar Hoover.

Congressional Archives, University of Oklahoma, *Cornelius E. Gallagher Collection*, www.ou.edu/special/albertctr/archives/gallaghe.htm. The Congressman left office in 1973 after being connected to the Mafia in a *Life* magazine article and then pleading guilty to tax evasion and perjury. *Id.*

> **Mr. Gallagher.** Perhaps you really are selling people: merchandising reputations, retailing character.
>
> . . . .
>
> **Mr. Burge.** I think in view of the climate in which American business operates that we are on fairly firm terra firma at this stage of the game. I think we have to be alert to the changing needs of business, to the developments in technology, to abuses that might develop that are not apparent at the present time. Certainly it is a changing environment in which we live. To this degree, I think this committee has done a good service, particularly as it pertains to governmental data banks, and on the basis of this atmosphere in which we live, I think we have to constantly examine whether our invasion of privacy is a proper invasion and is beneficial to the people overall or whether it is basically one that is leading toward abuse and a denial of rights and privileges.
>
> **Mr. Gallagher**. Yes; that is a prime concern; the individual rights and what is happening to the individual's rights, and in particular, his right to privacy.[32]

The FCRA, which passed shortly after these hearings, has been enforced by the FTC over the years as a way to safeguard consumers' privacy interests in relation to commercial decisions made about the consumer, including extension of credit and employment.[33] The agency noted in testimony to Congress that, "The principle underlying the FCRA when it was first enacted in 1970 was to ensure that this country's consumer reporting system would function fairly, accurately, and efficiently, without unwarranted intrusion into consumers' privacy."[34] The FCRA represents a balance between privacy and commercialized technology.

In areas outside of credit reporting, the Supreme Court confirmed during this period that "the protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."[35] The

---

[32] 1968 Hearing Testimony, *supra* note 28, at 44–45.

[33] The FTC has brought over 100 FCRA enforcement actions. *See What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing, Before the S. Comm. on Commerce, Sci. & Transp.*, 113th Cong. (Dec. 18, 2013) (statement of Jessica Rich, Dir., Bureau of Consumer Prot., Fed. Trade Comm'n, at 4).

[34] *Prepared Statement of the Federal Trade Commission: Hearing Before the S. Comm. on Banking, Housing & Urban Affairs, Subcommittee on Consumer and Regulatory Affairs* (Oct. 22, 1991) (statement of Kathleen Buffon, Assistant Dir. for Credit Practices, Fed. Trade Comm'n, at 2) [hereinafter *FTC 1991 Prepared Statement*].

[35] Katz v. United States, 389 U.S. 347, 350–51 (1967) (internal citation omitted). The Supreme Court, in 1967, expanded the zone of privacy against the government under the Fourth Amendment beyond its origins in trespass to encompass all "reasonable expectations of privacy." *Id.* at 362.

common law had matured at this point, with enough consensus across the states to allow Dean William Prosser in 1960 to draw up four categories of privacy-based torts: "1. Intrusion upon the [person's] seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the [person.] 3. Publicity which places the [person] in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the [person's] name or likeness."[36] By the late 1970s, these developments in the law, among others, had helped ease public concerns about invasions of personal privacy.

C. The Internet Age, Big Data, and a New Era of Privacy Concerns

Beginning in the 1990s and accelerating more recently, privacy concerns have grown along with a new wave of technology that further facilitates the collection and use of data about consumers.[37] Once again, new technologies, most notably the Internet, have made information about individual consumers more accessible but also more commercially valuable. Consumer data now forms the foundation of a wide variety of services, products, and business models, with enormous benefits to both competition and consumers.

The value and importance of consumer data to e-commerce and the Internet ecosystem is widely understood.[38] As a threshold matter, it is a key input to vigorous online competition. Many of the most prominent digital businesses are platforms,[39] similar to newspapers or credit card networks, whose main function is to intermediate between different groups of customers, often including individual consumers and advertisers.[40] Thus, one side of the digital

---

[36] Prosser, *supra* note 20, at 389.

[37] In 1991 testimony about the need to amend the FCRA to reflect advances in the Internet, the FTC noted: "The challenge today is two-fold: to ensure that our laws are adequate to protect consumers' privacy in the face of an ever-escalating technological revolution and to ensure that the increasing amount of financial information compiled on consumers is accurately reported." *FTC 1991 Prepared Statement*, *supra* note 34, at 2. The FTC recognized that "Consumer groups are rightly concerned that detailed personal information about each of us may have simply become another commodity that is marketed without adequate regard for privacy rights." *Id.*

[38] *See, e.g.*, Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. Pa. L. Rev. 1663, 1677 (2013).

[39] *See id.*

[40] *Id.* Digital platforms operate by attracting consumers to one side of the platform with "free" content and services such as webmail, maps, or travel search. James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 Geo. Mason L. Rev. 1129, 1130 (2013). They monetize this consumer traffic by charging users on the other side of the platform—e.g., advertisers—for access to, or information about, the consumers on the "free" side. *Id.* They exhibit network effects, scale, and scope economies; can realize significant first mover advantages; and, with market power, can act as a bottleneck between users on opposite sides of the platform and extract rents from multiple markets and impose high switching costs on consumers. Shelanski, *supra* note 38, at 1675–79.

platform effectively subsidizes the other side.[41] Examples of digital businesses that rely at least in part on platform models include household names like Google, Microsoft's Bing, Amazon, Facebook, and Priceline. The data collected by electronic platforms can take several forms, including "volunteered data" shared intentionally by consumers, "observed data" obtained by recording consumer actions online, and "inferred data" derived from analyzing volunteered and observed data.[42]

In the online commercial world, consumer data is both an input for other online services and a commodity asset for advertisers. As an input, detailed consumer data can help improve and refine downstream products and services. For example, travel metasearch site Kayak uses data mining technology to analyze more than one billion queries run by consumers on its websites to forecast price trends on flights for specific routes.[43] This service could not work without user search data and allows Kayak to offer its users advice as to whether a ticket purchase would represent a good value for them and assign a degree of confidence to its buy/wait recommendation.[44]

Data is also a commodity. For example, advertisers purchase robust consumer data sets, allowing them to focus promotion of their products or services narrowly to avoid spending money advertising to uninterested consumers.[45] Philadelphia merchant John Wanamaker once observed: "Half the money I spend on advertising is wasted; the trouble is I don't know which half."[46] Modern online behavioral data reduces such waste. As the FTC noted in its report about data brokers, businesses can now "purchase information about their customers' interests in order to market specific products to them, including using consumers' offline activities to determine what advertisements to serve them on the Internet."[47]

---

[41] *See* Allen P. Grunes, *Another Look at Privacy*, 20 GEO. MASON L. REV. 1107, 1109 (2013) (discussing various advertising supported media). For example, Google sells advertising to businesses looking to target consumers based on specific search queries conducted for free by consumers.

[42] WORLD ECONOMIC FORUM, PERSONAL DATA: THE EMERGENCE OF A NEW ASSET CLASS 7 (Jan. 2011).

[43] Sean O'Neill, *Kayak Adds Price Forecasts to US and UK Fare Search, Saying It's Better than Bing Travel*, TNOOZ (Jan. 15, 2013), www.tnooz.com/article/kayak-adds-price-forecasts-to-us-and-uk-fare-search-saying-its-better-than-bing-travel.

[44] *Id.*

[45] Grunes, *supra* note 41, at 1110 (explaining benefits of web advertising over traditional media); J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 111–12 (2008).

[46] John Wanamaker (attributed).

[47] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY ii (May 2014) [hereinafter FTC DATA BROKERS REPORT], *available at* www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Given the intrinsic value of this data, digital platforms can monetize it in several ways, including by using it internally to improve services or by selling it directly to advertisers or data brokers for repackaging. This monetized data in turn supports consumer access to an ever-expanding selection of free, high-quality services and content, such as online search, email, maps, and streaming video, much of which was previously available only for a substantial fee.

The scale and scope of data collection and use will only accelerate as we move into the era of big data fueled with increasing amounts of information from the "Internet of Things."[48] It is clear that big data offers enormous potential commercial, social, and political gains. For example, McKinsey Global Institute has estimated that analytics enabled by big data could yield benefits for health care of up to $190 billion annually.[49] Big data enables business researchers and data scientists to do things "at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more."[50]

Nonetheless, concerns persist over the implications for privacy of the widespread collection and use of consumer information to fuel these new products and businesses. These may arise from the combining of data sets through mergers and acquisitions involving large Internet businesses, which either give control of consumer data to an entity with which the consumer did not choose to interact or where the combination allows the merged firm to gain new insights about individual consumers.

Such data combinations also frequently occur outside the merger area, however, and raise similar concerns. For instance, the FTC recently noted that "data broker practices may raise privacy concerns," largely because data brokers "collect, manipulate, and share information about consumers without interacting directly with them," making consumers unaware of these practices.[51] The privacy concerns implicated by mergers of data-rich firms, as well as by

---

[48] The scale of digital platforms and their ability to collect data, which is already impressive, is set to grow through the creation and collection of information by new Internet connected devices, such as cars, home appliances, and wearable medical devices. This trend, now finally taking shape after years of discussion, is commonly referred to as the "Internet of Things." These Internet connected devices will inevitably increase the volume and detail of collected information, much of which can be done with little to no consumer interfacing. *See* Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, CISCO 3 (White Paper Apr. 2011), www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (Cisco estimates that there will be 25 billion connected devices in 2015).

[49] MCKINSEY GLOBAL INSTITUTE, GAME CHANGERS: FIVE OPPORTUNITIES FOR US GROWTH AND RENEWAL 70 (July 2013).

[50] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 6 (2013).

[51] FTC DATA BROKERS REPORT, *supra* note 47, at 3.

data broker activity, apply equally to big data tools, which may be used to reveal sensitive or personal details about an individual by compiling and analyzing anonymous or non-sensitive data points.[52] As the White House *Big Data Report* observed, "The advent of more powerful analytics, which can discern quite a bit from even small and disconnected pieces of data, raises the possibility that data gathered and held by third parties can be amalgamated and analyzed in ways that reveal even more information about individuals. What protections this material and the information derived from it merit is now a pressing question."[53]

As a result of these concerns, privacy protection has emerged as a small, but rapidly expanding, dimension of competition among digital platforms. Examples include the numerous 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.[54] Another prominent example in the online search engine business, DuckDuckGo, promises users that it does not retain search history or track users based on search habits. Its marketing slogan is "The search engine that doesn't track you."[55]

Dozens of popular new applications and social media platforms are now targeting users seeking more privacy online. Examples of popular social media that offer privacy as a value proposition include Backchat, Whisper, Ask.fm, and SnapChat.[56] Whisper, for instance, allows users to post pictures and comments without personal attribution.[57] Each of these digital platforms is relatively new and, despite the size of social media players like Facebook,

---

[52] Big data is not synonymous with data broker activity, however, and much of the information collected and used for big data purposes does not implicate individual privacy.

[53] BIG DATA REPORT, *supra* note 4, at 34.

[54] GHOSTERY, www.ghostery.com.

[55] DUCKDUCKGO, duckduckgo.com. The company was ranked among the "Top 50 iPhone apps of 2013" by *TIME*, has attracted significant investment, and has seen its volume nearly triple in the last two years, to over 5 million searches per day. *About*, DUCKDUCKGO, duckduckgo.com/about.

[56] Cecilia Kang, *Apps Feed Teens' Yen for Online Anonymity*, WASH. POST, Feb. 17, 2014, at A1. The FTC settled allegations that Snapchat misrepresented that the photos sent by users would disappear forever, that the sender would be notified if the recipient took a screen shot of the photo, that Snapchat would not access location data, that it would only access phone numbers to find user's friends, and that it had reasonable security measures for the find friends feature. *See* Complaint, FTC v. Snapchat, FTC Docket No. C-4501 (Dec. 23, 2014), *available at* www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf; Agreement Containing Consent Order, FTC v. Snapchat, FTC Docket No. C-4501 (Dec. 23, 2014), *available at* www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf.

[57] Kang, *supra* note 56, at A2. Allegations have surfaced that Whisper may have tracked some customers' geo-location information against their wishes. Meena Harris, *Whisper's Privacy Problem: Sen. Rockefeller Pushes for Probe While Editorial Team Is Suspended Pending Review*, NAT'L L. REV. (Oct. 28, 2014), www.natlawreview.com/article/whisper-s-privacy-problem-sen-rockefeller-pushes-probe-while-editorial-team-suspende.

Twitter, and Google, has been able to quickly attract large volumes of consumer traffic by offering greater anonymity as an attribute of otherwise similar social media offerings.

In another sign of the growing commercial prominence of privacy, Tim Cook, the CEO of technology giant Apple recently posted a letter on the company's website explaining that, unlike its competitors, "We don't build a profile based on your email content or web browsing habits to sell to advertisers. We don't 'monetize' the information you store on your iPhone or in iCloud. And we don't read your email or your messages to get information to market to you."[58] Apple is making security and privacy "fundamental to the design of all [its] hardware, software, and services . . . ."[59]

II. PRIVACY AND THE FTC ACT

These modern emerging privacy concerns have prompted a wide range of proposed solutions. One such class of proposals, which we detail below, seeks to use competition law to protect consumer privacy. We also describe how such proposals may be inconsistent with the evolution of the separation between competition law and consumer protection law and with the FTC's application of competition law and consumer protection law to handle privacy concerns.

A. PROPOSALS TO USE COMPETITION LAW TO PROTECT PRIVACY

Some policymakers and advocates have proposed that the federal antitrust and competition laws—especially those related to mergers and other commercial combinations—offer a good way to police privacy violations. Their proposals generally fall into four categories. The first group would evaluate privacy as a non-price dimension of competition and examine transactions, like mergers involving large data sets, by determining whether the deal would reduce the merged firm's incentives to compete on consumer privacy protections.[60] The second group would balance the costs and benefits of consumer

---

[58] Tim Cook, *A Message About Apple's Commitment to Your Privacy*, APPLE, www.apple.com/privacy (last visited Dec. 7, 2014).

[59] *Id.*

[60] *See generally* Pamela Jones Harbour, Comm'r, Fed. Trade Comm'n, Dissenting Statement, Google/DoubleClick, FTC File No. 071-0170, at 1 (2007), *available at* www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf. Former Commissioner Harbour expressed concerns about the proposed merger between Google and DoubleClick along several dimensions, including privacy and data aggregation. She said, "I have considered (and continue to consider) various theories that might make privacy 'cognizable' under the antitrust laws, and thus would have enabled the Commission to reach the privacy issues as part of its antitrust analysis of the transaction." *Id.* at 10. She cited as a possible theory that network effects could lead to fewer search engines, reducing "incentives of search firms to compete based on privacy protections or related non-price dimensions." *Id.* at 10 n.25. She suggested a firewall between Google and DoubleClick's data as a potential solution. *Id.* at 9 n.23.

protection against the impact on competition in those situations where "conduct-distorting commerce implicates *both* consumer protection and competition principles."[61] Thus, for instance, supporters of this approach might suggest that if a consortium of competitors agreed to limit the use of certain sensitive data from marketing decisions, this could trump concerns about harm to competition. Advocates for this theory believe separating competition and consumer protection enforcement represents an "artificial dichotomy."[62] A third group would hold companies accountable under the antitrust laws to the extent those companies mislead or deceive consumers about data collection practices that helped the companies achieve or maintain monopoly power.[63] The fourth, and perhaps most aggressive, group would look for the possible harm to privacy from transactions *beyond* just analyzing the harm to privacy as an existing dimension of competition.[64] Thus, for instance, under

---

[61] Julie Brill, Comm'r, Fed. Trade Comm'n, *The Intersection of Consumer Protection and Competition in the New World of Privacy*, COMPETITION POL'Y INT'L, Spring 2011, at 7, 10. Commissioner Brill has also written that the 2010 Merger Guidelines offer federal agencies "ample room to consider the impact of a transaction on privacy-based competition." Julie Brill, *Competition and Consumer Protection: Strange Bedfellows or Best Friends?*, ANTITRUST SOURCE, Dec. 2010, at 10, www.abanet.org/antitrust/at-source/10/12/Dec10-Brill12-21f.pdf. She offered as examples of potential tension between competition and consumer protection the FTC's actions against state dental groups in California, South Carolina, and North Carolina, in which the agency challenged these groups' policies as anticompetitive despite claims they were intended to protect public health. *Id.* at 2–4. The Commissioner argued that, in matters such as these, "before competition principles can trump consumer protection concerns, any legitimate consumer protection issues must be identified and balanced against the competitive harm." *Id.* at 3.

[62] 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, 773 (2010).

[63] *See generally* J. Thomas Rosch, Concurring and Dissenting Statement of Commissioner J. Thomas Rosch Regarding Google's Search Practices, Google Inc., FTC File No. 111-0163 (Jan. 3, 2013), *available at* www.ftc.gov/sites/default/files/documents/public_statements/concurring-and-dissenting-statement-commissioner-j.thomas-rosch-regarding-googles-search-practices/130103googlesearchstmt.pdf. Commissioner Rosch wrote that "Google has monopoly or near-monopoly power in the search advertising market and this power is due in whole or in part to its power over searches generally . . . ." *Id.* at 1 n.1. He went on to explain that he had a strong concern that the Commission had not acted to prevent "Google from telling 'half-truths'—for example, that its gathering of information about the characteristics of a consumer is done solely for the consumer's benefit, instead of also to maintain a monopoly or near-monopoly position." *Id.* Commissioner Rosch cited to *International Harvester* and *North American Phillips* for support of his concern about half-truths. These citations may indicate he would have been interested in pursuing Google for a consumer protection violation, although he did not offer any further clarification of this point in a later interview. *See* Ron Knox, *An Interview with Tom Rosch*, GLOBAL COMPETITION REV., Feb. 2013, at 51.

[64] For example, in 2012 U.S. Senator Al Franken spoke to the ABA Section of Antitrust Law about the need for antitrust laws to help protect privacy. The Senator explained that privacy had become an antitrust issue in part because "[i]f you don't want your search results shared with other Google sites [or a] super-profile being created for you based on everything you search, every site you surf, and every video you watch on YouTube—you will have to find a search engine that's comparable to Google. Not easy." Sen. Al Franken, Speech at the American Bar Ass'n Section of Antitrust Law Spring Meeting Dinner: How Privacy Has Become an Antitrust Issue (Mar. 29, 2012), *available at* www.huffingtonpost.com/al-franken/how-privacy-has-become-an_b_1392580.html. He observed that "[y]ou might not like that Facebook shares your

this approach a federal agency would be able to block a merger of two companies that own large consumer databases even if those companies had no meaningful vertical or horizontal competitive relationship.

One of the first calls to introduce privacy into a particular competition analysis came in 2007 in conjunction with the FTC's investigation of the proposed Google-DoubleClick acquisition.[65] Arguing that the "right of privacy is a personal and fundamental right in the United States,"[66] the Electronic Privacy Information Center (EPIC) sought direct consideration of personal privacy concerns as part of the FTC's analysis of the merger. It noted that the "acquisition of DoubleClick will permit Google to track both a person's Internet searches and a person's web site visits"[67] and stressed that "Google has already expressed an intent to merge data from Google and DoubleClick to profile and target Internet users."[68] EPIC couched much of its argument in consumer protection terms, asking the FTC to halt the proposed deal in large part because "Google will operate with virtually no legal obligation to ensure the privacy, security, and accuracy of the personal data that it collects."[69]

Rejecting the idea that such normative considerations of privacy could be a factor in a merger analysis,[70] the Commission noted:

> [T]he sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition. Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry.[71]

In early 2014, consumer groups raised similar privacy concerns with two proposed transactions involving large online companies. The first of these

---

political opinions with *Politico*, but are you really going to delete all the photos, all the posts, all the connections . . . you've spent years establishing on the world's dominant social network?" He concludes that "The more dominant these companies become . . . the less incentive they have to respect your privacy. . . . Because accumulating data about you isn't just a strange hobby for these corporations. It's their whole business model. And you are not their client. You are their product." *Id.*

[65] Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007) [hereinafter FTC DoubleClick Statement]. At the time, Google competed in sponsored search advertising and online ad sales and intermediation, and DoubleClick was the leader in the related business of third-party ad serving.

[66] *See* Elec. Privacy Info. Cntr., Complaint and Request for Injunction, Google & DoubleClick, Inc. at 2 (Apr. 20, 2007), *available at* epic.org/privacy/ftc/google/epic_complaint.pdf.

[67] *Id.* at 6.

[68] *Id.*

[69] *Id.* at 10.

[70] *See* FTC DoubleClick Statement, *supra* note 65, at 2.

[71] *Id.*

transactions was Facebook's $16 billion acquisition of Internet text messaging service WhatsApp. In a complaint to the FTC, EPIC and the Center for Digital Democracy argued that WhatsApp had built a large user base on its commitment not to collect user data for advertising revenue.[72] Facebook, on the other hand, made it clear that it intended to incorporate the information shared by WhatsApp users into its consumer profiling business model.[73] Unlike its complaint about Google's purchase of DoubleClick, here EPIC complained that the acquisition would be a consumer protection violation *if* Facebook was able to proceed with its plans to use WhatsApp consumer data in a way that would violate WhatsApp's privacy policies.[74] The FTC did not move to block the transaction. Instead, FTC Staff responded to these concerns with a letter from the Director of the Bureau of Consumer Protection, reminding the parties of their continuing obligation to adhere to their respective pre-merger privacy policies covering data and information collected pursuant to those policies and recommending that they allow consumers an opportunity to opt out of uses of WhatsApp subscriber data inconsistent with such policies.[75]

The second transaction was Google's purchase of Nest Labs, a company focused on the manufacture and sale of smarter home devices like thermostats and smoke alarms. A number of privacy advocates and media outlets raised concerns about this deal, claiming, "A lot of people are made uneasy because they entered an agreement (to share their personally identifiable stream of data) with one company (Nest) but now that agreement has been transferred to another company (Google)."[76] The transaction closed in February 2014 without challenge.[77]

---

[72] Elec. Priv. Info. Cntr. & Cntr. for Digital Democracy, Complaint, Request for Investigation, Injunction, and Other Relief, WhatsApp, Inc. (Mar. 6, 2014), *available at* www.centerfordigitaldemocracy.org/sites/default/files/WhatsApp%20Complaint.pdf; *see also* Elec. Priv. Info. Cntr. & Cntr. for Digital Democracy, Supplemental Materials In Support of Pending Complaint, Request for Investigation and Injunction, and Other Relief, WhatsApp, Inc. (Mar. 21, 2014) [hereinafter EPIC & CDD Supplemental Materials], *available at* www.centerfordigitaldemocracy.org/sites/default/files/WhatsApp-Nest-Supp-1.pdf.

[73] EPIC & CDD Supplemental Materials, *supra* note 72, at 1.

[74] *Id.* at 10–11.

[75] Letter from Jessica Rich, Fed. Trade Comm'n, to Erin Egan, Facebook, and Anne Hoge, WhatsApp (Apr. 10, 2014), *available at* www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

[76] Rakesh Sharma, *Google's Acquisition of Nest and Your Privacy*, FORBES (Jan. 13, 2014) (quoting Parker Higgins, Electronic Frontier Foundation), www.forbes.com/sites/rakeshsharma/2014/01/13/googles-acquisition-of-nest-and-your-privacy.

[77] Google Inc., Annual Report (Form 10-K, for the Fiscal Year Ended Dec. 31, 2013) 83 (Feb. 11, 2014).

B. COMPLEMENTARITY AND THE DUAL MANDATE OF THE FTC ACT

We contend that such commingling of the competition and consumer protection laws under any of these approaches is unnecessary and could lead to confusion and doctrinal issues in antitrust, without true gains to consumer protection. The history of the FTC's approach to competition and consumer protection offers valuable lessons about the bifurcated, but complementary, nature of the antitrust and consumer protection laws. This history also strongly suggests a compelling way forward in evaluating privacy under the FTC Act and other laws as both a social norm and a commercial good or service. Below we examine the evolution of these concepts and touch on their relevance today.

The complementary nature of the consumer protection and competition laws is best illustrated by examining the creation and early history of the FTC. The FTC has long fulfilled its charge under Section 5 of the FTC Act to prevent unfair methods of competition and unfair or deceptive acts or practices.[78] The first clause of Section 5(a) of the FTC Act, which appeared in the agency's original mandate in 1914, established the agency's competition law authority; the second clause, added in 1938, cemented its consumer protection authority.[79]

1. *The Early Years: An Era of Doctrinal Confusion*

The early era of enforcement between 1914 and 1938, before Congress passed the Wheeler-Lea Act to add consumer protection authority to the FTC Act, offers a unique window into the natural complementarity of competition and consumer protection and the doctrinal risks attendant to conflating them. In the early 1920s, the FTC began testing the boundary of its authority over consumer deception, arguing that this conduct constituted an unfair method of competition.[80] In 1922, the Supreme Court reviewed an FTC case against Winsted Hosiery Co., in which the Commission contended that the company had mislabeled its knit goods as wool.[81] This led buyers and retailers to think that the products were entirely, rather than partially, wool.[82] The Commission reasoned that this could harm those competitors labeling their products truth-

---

[78] 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 enforce directly 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. *See infra* Part II.B.1.

[79] *See* 15 U.S.C. § 45(a)(1).

[80] *See, e.g.*, FTC v. Winsted Hosiery Co., 258 U.S. 483 (1922); Royal Baking Powder Co. v. FTC, 281 F. 744 (2d Cir. 1922).

[81] *See Winsted Hosiery*, 258 U.S. at 490.

[82] *See id.* at 492–93.

fully—as the Court noted: "For when misbranded goods attract customers by means of the fraud which they perpetrate, trade is diverted from the producer of truthfully marked goods."[83] The Supreme Court upheld this reasoning and concluded, "[S]ince the business of its trade rivals who marked their goods truthfully was necessarily affected by that practice, the Commission was justified in its conclusion that the practice constituted an unfair method of competition."[84]

The FTC used the *Winsted Hosiery* decision as a license to embark on an ambitious consumer protection enforcement campaign, bringing numerous investigations for competition violations such as "Selling or Offering with Tendency and Capacity to Deceive"; "Misbranding"; and "False and Misleading Statements."[85] By 1925 roughly 70 percent of the FTC's orders involved deceptive advertising.[86] The agency in this era regarded its mission as "protect[ing] the public against those methods . . . opposed to good morals because characterized by deception, bad faith, fraud or oppression . . . ."[87] The agency also noted that "the law is not made for the protection of experts but for the public—that vast multitude which includes the ignorant, the unthinking and the credulous who, in making purchases, do not stop to analyze, but are governed by appearances and general impression."[88]

But to maintain its consumer protection claims as unfair methods of competition, the FTC had to tie each violation to some harm to competition. And it did, at least nominally, which frequently led to awkward and strained analyses that tested the agency's credibility with the business community and the courts. For example, in 1919, the Commission ordered Sears, Roebuck & Company to cease and desist from conduct involving a combination of false advertising, predatory pricing, and tying. The agency explained that Sears was "[s]tifling and suppressing competition by means of false and misleading advertising offering sugar and other commodities for sale at prices lower than offered by competitors and actually below cost but conditioned on the purchase of other goods on which the profit is made and by false and misleading advertisements relative to competitors."[89]

---

[83] *Id.* at 493.

[84] *Id.* at 494.

[85] FED. TRADE COMM'N, STATEMENT OF THE WORK OF THE FEDERAL TRADE COMMISSION 4 (1932) [hereinafter FTC 1932 STATEMENT].

[86] 6 THE LEGISLATIVE HISTORY OF THE FEDERAL ANTITRUST LAWS AND RELATED STATUTES 4808 (Earl W. Kintner, ed. 1983) [hereinafter WHEELER-LEA HOUSE REPORT].

[87] FTC 1932 STATEMENT, *supra* note 85, at 4 (citing FTC v. Gratz, 235 U.S. 421, 427 (1920)).

[88] *Id.*

[89] FED. TRADE COMM'N, BRIEF SKETCH OF THE FEATURES OF THE LEGAL WORK OF THE FEDERAL TRADE COMMISSION AND INQUIRIES MADE BY IT THROUGH THE ECONOMIC DIVISION SINCE ITS ORGANIZATION 5 (1921). Another example involved the deceptive sale of sponges. In 1921, the agency investigated respondent Lasker & Bernstein for "knowingly and deceptively en-

The FTC's expansive interpretation of unfair methods of competition quickly ran into trouble in the courts. In 1931, the Supreme Court was called on again to evaluate the scope of the FTC's authority in *FTC v. Raladam Co.*[90] The agency had ordered Raladam to cease and desist making false and misleading claims about the safety, effectiveness, and scientific basis for a purported obesity cure.[91] The Commission had made no factual finding of prejudice or injury to any competitor, instead inferring such harm because "the practice of respondent was to the prejudice of the public and respondent's competitors . . . ."[92]

The Court reversed the Commission, and in its opinion offered a careful study of the Commission's authority and a nuanced interpretation of unfair methods of competition. Justice Sutherland, writing for the Court, stated, "It is obvious that the word 'competition' imports the existence of present or potential competitors, and the unfair methods must be such as injuriously affect or tend thus to affect the business of these competitors—that is to say, the trader whose methods are assailed as unfair must have present or potential rivals in trade whose business will be, or is likely to be, lessened or otherwise injured."[93] The Court went on to severely limit the FTC's authority, noting, "It is that condition of affairs [the loss of competition] which the Commission is given power to correct, and it is against that condition of affairs, and not some other, that the Commission is authorized to protect the public."[94] The Court closed its analysis by proclaiming, "Unfair trade methods [such as false advertising] are not per se unfair methods of *competition*. . . . If broader powers be desirable, they must be conferred by Congress."[95]

2. *Codification of Complementarity: The Wheeler-Lea Act*

In 1935, Senator Wheeler of Montana submitted a report on behalf of the Senate Committee on Interstate Commerce recommending a bill to amend the FTC Act in response to the Supreme Court's *Raladam* decision. The Committee report offered a thorough exposition of the limits of the FTC's competition law mandate under the original Act. The Committee explained that because of the Supreme Court's narrow view of the competition laws expressed in *Raladam*, the FTC would be unable to protect consumers from deception and un-

---

gag[ing] in loading, doping, and saturating sponges with foreign matter, thereby falsifying the weight of said sponges, creating a fictitious price, defrauding and misleading customers, and causing prejudice and injury to competitors." *Id.* at 13.

[90] FTC v. Raladam Co., 283 U.S. 643 (1931).

[91] *See id.* at 644–46.

[92] *Id.* at 646.

[93] *Id.* at 649.

[94] *Id.*

[95] *Id.*

fair acts under its unfair methods of competition authority where it could be shown that: "all competitors in the industry practiced the same unfair methods, [such that] the Commission may be ousted of its jurisdiction no matter how badly the public may be in need of protection from said deceptive and unfair acts."[96]

The House Committee on Interstate and Foreign Commerce also observed:

> [The] act is construed as if its purpose were to protect competitors only and to afford no protection to the consumer without showing injury to a competitor. Thus, if a person, partnership, or corporation has a monopoly in a certain field, so that there is no competitor, his acts, no matter how deceptive or misleading and unfair to the consuming public, may not be restrained.[97]

Congress's intent was clear: "Since it is the purpose of Congress to protect the consumer as well as the honest competitor, the Commission should be empowered to prevent the use of unfair or deceptive acts or practices in commerce, regardless of whether such acts or practices injuriously affect a competitor."[98] The Wheeler-Lea Act passed Congress in 1938, giving the FTC its consumer protection authority to police unfair or deceptive acts or practices (UDAP) and underscoring the complementarity of these two areas of law.[99]

3. *Complementarity in the Courts*

In *Raladam*, and in subsequent decisions, the Supreme Court has upheld the separate and distinct roles of the competition and consumer protection laws. Just as the Senate observed during its deliberation of the Wheeler-Lea Act that competition laws do not extend to noncompetition issues, the modern Court has been clear that although antitrust is central to national economic policy, it should remain limited to this sphere.[100] Across several decisions regarding

---

[96] S. REP. NO. 74-46, at 1 (1935).

[97] H.R. REP. NO. 75-1613, at 3 (1937), *reprinted in* WHEELER-LEA HOUSE REPORT, *supra* note 86, at 4879.

[98] *Id.*

[99] *See* 15 U.S.C. § 45(a)(1) (providing that"[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful").

[100] *See, e.g.*, Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 690 (1978); *see also* Standard Oil Co. v. FTC, 340 U.S. 231, 248 (1951) ("The heart of our national economic policy long has been faith in the value of competition."). *But cf.* FTC v. Algoma Lumber Co., 291 U.S. 67, 79–80 (1934) (noting that false or misleading advertising could have an anticompetitive effect where lumber companies renamed pine being sold as a higher quality white pine, gaining a cost advantage over those sellers producing the actual higher quality white pine lumber). The Supreme Court underwent a considerable evolution in its approach to antitrust issues over the course of the 20th century, moving from frequent consideration of noncompetition factors to a heavy reliance on economic evidence in its decisions. *Compare* Brown Shoe Co. v. United States, 370 U.S. 294, 344 (1962) (noting a Congressional desire to promote decentralization of business even in the face of higher prices), *with* NCAA v. Bd. of Regents of the Univ. of Okla.,

professional associations, the Court has set the outer boundaries of the antitrust laws short of setting social policy.

In *National Society of Professional Engineers v. United States*, the Court held unlawful an ethical canon of a trade group that prohibited the submission of "any form of price information to a prospective customer which would enable that customer to make a price comparison on engineering services."[101] The Society argued this ethics canon was needed to protect against competitive price bidding that could lower the resulting quality of engineering services. Such bidding, it claimed, could prove "dangerous to the public health, safety, and welfare."[102] On the basis of this public interest, the Society asserted that the rule was not an unreasonable restraint.

The Court disagreed, reasoning that the Sherman Act reflects a legislative judgment that competition is the best way to allocate resources in a free market and that "all elements of a bargain—quality, service, safety, and durability—and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers."[103] Thus, the Court confirmed that the competition laws are limited in scope and avoid moral determinations. Citing to *Standard Oil v. United States*, the Court wrote, "[T]he inquiry is confined to a consideration of impact on competitive conditions."[104] This narrow scope leaves out moral decisions as to whether, for instance, more "competition is good or bad."[105]

Several years later, in *FTC v. Indiana Federation of Dentists*,[106] the Supreme Court analyzed a similar set of circumstances and again concluded that noncompetition defenses like health and safety are not cognizable for alleged Sherman Act violations. The Court reasoned that allowing such a defense would represent a "frontal assault on the basic policy of the Sherman Act."[107] It concluded that the prevention of "unwise and even dangerous choices" could not justify unlawful collusion.[108]

---

468 U.S. 85, 107 (1984) (acknowledging consumer welfare as the fundamental goal of antitrust and viewing restrictions on price and output as inconsistent with that goal).

[101] *Professional Engineers*, 435 U.S. at 683.

[102] *Id.* at 685.

[103] *Id.* at 695.

[104] *Id.* at 690 (citing Standard Oil Co. v. United States, 221 U.S. 1, 65 (1911)).

[105] *Id.* at 695; *see also* Cooper, *supra* note 40, at 1133–34 (discussing Supreme Court's rejection of noncompetition factors in a competition law analysis). *But see* Associated Press v. United States, 326 U.S. 1, 19–20 (1945) (intimating consideration of diversity of viewpoints in media markets competition analysis).

[106] FTC v. Ind. Fed. of Dentists, 476 U.S. 447 (1986).

[107] *Id.* at 463 (quoting *Professional Engineers*, 435 U.S. at 695).

[108] *Id.*

This evolution in the Congress and the Courts of two distinct but complementary bodies of law—competition and consumer protection—reflects a consensus in the United States about the outer limits of our competition laws.[109] They are not designed to address conduct that may be unjust or immoral, unless it also happens to harm competition. Instead, American competition law enforcement objectives are, and for a long time have been, primarily focused on economic efficiency.[110] By contrast, as the Wheeler-Lea Act legislative history illustrates, the focus of the FTC's consumer protection authority is on harm to individuals.

C. PRIVACY, DATA, ANTITRUST, AND UNFAIR METHODS OF COMPETITION

With these boundaries in mind, we next examine how agencies and the courts have evaluated the concept of privacy within a competition law framework.

1. *Agency Approaches to Consumer Data as a Commercial Good*

As noted by the FTC in its Google/DoubleClick decision, the agencies have stayed away from requests to conflate normative privacy concerns and competition analysis; however, they have analyzed consumer data in the context of merger reviews.[111] For example, in 2009, the DOJ acknowledged data as an

---

[109] Federal circuit decisions also reflect the modern consensus that social welfare and public safety goals should remain outside the ambit of the antitrust and competition laws. The Fourth Circuit examined an agreement between two health plans to pay for clinical psychology services only to the extent that those services were billed through a physician. *See* Va. Acad. of Clinical Psychologists v. Blue Shield of Va., 624 F.2d 476 (4th Cir. 1980). The health plans claimed this policy was needed to encourage physician supervision of psychologists, thereby improving healthcare services. *Id.* at 484. The court rejected this argument and found the agreement an unlawful restraint of trade, noting that "we are not inclined to condone anticompetitive conduct upon an incantation of 'good medical practice.'" *Id.* at 485. Similarly, the Seventh Circuit reviewed an alleged boycott of chiropractors by members of the medical community, including the American Medical Association. *See* Wilk v. Am. Med. Ass'n, 719 F.2d 207 (7th Cir. 1983). The court discounted the public safety arguments. It explained that "a generalized concern for the health, safety and welfare of members of the public as to whom a medical doctor has assumed no specific professional responsibility, however genuine and well informed such a concern may be, affords no legal justification for economic measures to diminish competition with some medical doctors by chiropractors." *Id.* at 228.

[110] 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." Transcript of Fed. Trade Comm'n, Workshop on Section 5 of the FTC Act as a Competition Statute 67 (Oct. 17, 2008) (remarks of Robert Pitofsky), *available at* www.ftc.gov/bc/workshops/section5/transcript.pdf.

[111] *See* FTC DoubleClick Statement, *supra* note 65, at 2. Federal agencies have experience with data related issues in other industries with multisided platform economics similar to digital platforms. For example, the DOJ has reviewed several proposed mergers among financial exchanges over the last several years. Financial exchanges are two-sided markets that function as platforms to match buyers and sellers of securities. *See* United States, *Note on Competition and Financial Markets* at 6, OECD Competition Comm., Doc. JT03258951, DAF/COMP/WD/

input to digital platforms with implications for a unilateral effects analysis in the context of a proposed consolidation. At the time, Microsoft and Yahoo! had announced a joint venture to combine portions of their online search and search advertising technology. This combination would reduce the number of major search and search advertising competitors in the United States from three to two, with Google retaining the lead and a 65 percent share of searches.[112] Despite this, the DOJ cleared the transaction, apparently relying heavily on the importance of search data as an input necessary to improve the competitive performance of the combined engine. The agency concluded that increased volume of search data could spur more vigorous competition with Google.[113]

In 2011, the DOJ considered data access as a potential vertical restraint in its review of the proposed acquisition by Google of ITA.[114] ITA provided electronic pricing and shopping (P&S) systems to online travel agencies, powering the comparative flight search queries for leading websites like Kayak, Orbitz, and Bing Travel.[115] ITA's systems had two main components, which included "a continuously-updated database of airline pricing, schedule and seat availability information, and a software algorithm used to search the database for flight options that best match consumers' search criteria."[116]

Although the DOJ did not define a separate data market, it recognized these data-rich P&S systems as a relevant product market in that matter. The agency expressed concerns that Google, which intended to buy ITA and also enter the

---

(2009)11 (Jan. 30, 2009), *available at* www.justice.gov/atr/public/international/270439.pdf. They exhibit strong network effects and economies of scale and scope. *See* Jêdrzej Mazur, Economic Analysis of Stock Exchange Consolidation 17 (Jan. 15, 2012) (unpublished Master Thesis, Goethe Univ.), *available at* www.professionsfinancieres.com/sites/default/files/docsupload/u213/M%20Jedrzej%20MAZUR.pdf. As with digital platforms, data is vital to exchanges both as an input and as a commodity asset and exchanges regularly handle (and benefit from) very sensitive financial information for their customers. Unlike digital platforms, securities markets are highly regulated, as is the data generated by financial exchanges. In this unique environment, the DOJ applied standard market definition rules to define a relevant market of "real-time proprietary equity data." *See* Complaint at 8, United States v. Deutsche Börse AG, No. 1:11-cv-02280 (D.D.C. Dec. 22, 2011); *see also* Alexander P. Okuliar, *Financial Exchange Consolidation and Antitrust: Is There a Need for More Intervention?*, ANTITRUST, Spring 2014, at 66 (discussing the prevailing relevant product market analysis relating to financial exchange data).

[112] *See* Press Release, comScore, comScore Releases June 2009 U.S. Search Engine Rankings (July 16, 2009), www.comscore.com/Insights/Press-Releases/2009/7/comScore-Releases-June-2009-U.S.-Search-Engine-Rankings.

[113] Statement of the Department of Justice Antitrust Division on Its Decision to Close Its Investigation of the Internet Search and Paid Search Advertising Agreement Between Microsoft Corporation and Yahoo! Inc. 1–2 (Feb. 18, 2010), *available at* www.justice.gov/atr/public/press_releases/2010/255377.pdf.

[114] Complaint at 3, 10–13, United States v. Google Inc., No. 1:11-cv-00688 (D.D.C. Apr. 8, 2011), *available at* www.justice.gov/atr/cases/f269600/269618.pdf.

[115] *Id.* at 2.

[116] *Id.* at 8.

online travel search business, would have the incentive and ability to foreclose or raise the costs of P&S and comparative flight search systems to online travel websites.[117] In part, the agency's concern appears to have arisen from the possibility that the transaction could mean downstream online travel search competitors would have degraded or more costly access to the data they needed as a critical input to their platforms. The DOJ and Google entered a consent decree resolving these issues requiring Google to continue licensing the P&S systems and protect ITA's customers with fair, reasonable, and non-discriminatory access to the systems. The consent decree also prohibited Google from using customer data for its own benefit.[118]

2. *Court Approaches to Consumer Data as a Commercial Good*

Courts, too, have evaluated data as a commercial good, particularly credit data. For instance, in *Fair Isaac Corp. v. Experian Information Solutions, Inc.*,[119] the court examined the antitrust claims of Fair Isaac Corp (FICO), a credit scoring firm, against the three leading credit bureaus: TransUnion, Experian, and Equifax.[120] FICO did not sell its credit scores directly to lenders and consumers, but instead licensed the scores to the credit bureaus to sell as part of bundled packages including credit reports.[121] FICO claimed that the credit bureaus violated the antitrust laws by forming a competing joint venture to provide credit scores, thereby reducing their demand for FICO scores. Al-

---

[117] *Id.* at 10–13.

[118] Competitive Impact Statement at 13–14, United States v. Google Inc., No. 1:11-cv-00688 (D.D.C. Apr. 8, 2011), *available at* www.justice.gov/atr/cases/f269600/269620.pdf. The FTC has also examined the collection of data and information in the context of a merger. For instance, the agency challenged Reed Elsevier's acquisition of ChoicePoint in 2008, alleging that the two entities were the primary head-to-head competitors in the market for electronic public records services to law enforcement customers. *See* Complaint at 3, Reed Elsevier NV, FTC Docket No. C-4257 (June 5, 2009), *available at* www.ftc.gov/enforcement/cases-proceedings/081-0133/reed-elsevier-nv-et-al-matter. The agency entered a consent agreement with the parties requiring the divestiture of ChoicePoint's electronic records services to ThomsonReuters. *See* Decision and Order, Reed Elsevier NVl., FTC Docket No. C-4257 (June 5, 2009), *available at* www.ftc.gov/enforcement/cases-proceedings/081-0133/reed-elsevier-nv-et-al-matter.

Similarly, in 2010 the agency settled a challenge to Dun & Bradstreet's acquisition of Quality Educational Data because it allegedly would have created a monopoly in the market for certain educational marketing databases. *See* Complaint at 3, Dun & Bradstreet Corp., FTC Docket No. 9342 (May 6, 2010), *available at* www.ftc.gov/enforcement/cases-proceedings/091-0081/dun-bradstreet-corporation-matter; Decision and Order, Dun & Bradstreet Corp., FTC Docket No. 9342 (Sept. 10, 2010), *available at* www.ftc.gov/sites/default/files/documents/cases/2010/09/100910dunbradstreetdo.pdf. For a detailed discussion of analysis in data markets, see, e.g., Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, ANTITRUST SOURCE (Dec. 1, 2014), www.americanbar.org/content/dam/aba/publishing/antitrust_source/dec14_full_source.authcheckdam.pdf. For a comparative discussion of approaches to privacy and merger enforcement, see Lisa Kimmel & Janis Kestenbaum, *What's Up with WhatsApp? A Transatlantic View of Privacy and Merger Enforcement in Digital Markets*, ANTITRUST, Fall 2014, at 48.

[119] 645 F. Supp. 2d 734 (D. Minn. 2009).

[120] *Id.*

[121] *Id.* at 738.

though the court granted summary judgment to the credit bureaus, it acknowledged the possibility of aggregated credit data markets.[122] The Ninth Circuit accepted an alleged relevant market consisting of wholesale credit data in a case with similar allegations.[123] These decisions, and others within the context of financial markets, demonstrate that acquisitions or conduct implicating consumer data can be examined under the antitrust laws, but only to the extent that they satisfy customary antitrust analyses, including the definition of relevant markets, and allow for the resolution of a commercial issue.

D. Privacy, Data, and Unfair or Deceptive Acts or Practices

Since the early 1970s, as noted earlier, the FTC has taken the lead nationally in monitoring and policing privacy abuses by commercial entities, first in credit reporting practices under the FCRA and later in online data collection and use. Through its enforcement work under Section 5 of the FTC Act,[124] the agency has applied and adapted to changing cultural norms of consumer privacy in the face of technological innovation. This enforcement offers a natural adjunct to the agency's competition enforcement mission.

1. *The FTC's UDAP Authority and Privacy*

Guidance for the Commission's approach to privacy as a consumer protection issue under Section 5 lies mainly in the agency's two policy statements interpreting its UDAP authority: the 1980 Unfairness Statement and the 1983 Deception Statement. The Unfairness Statement sets out the blueprint for pursuing actions, including privacy violations, on the basis of consumer harm. It defines an act or practice as "unfair"—and thus potentially actionable under the law—when the harm it causes is "substantial," not outweighed by any offsetting consumer or competitive benefits, and not reasonably avoidable by the consumer.[125] It goes on to identify financial, health, and safety as catego-

---

[122] *Id.*

[123] Standfacts Credit Servs. v. Experian Info. Solutions, Inc., 294 Fed. App'x 271, 272 (9th Cir. 2008).

[124] 15 U.S.C. § 45. In addition to Section 5, Congress has given the Commission authority to enforce several privacy-related laws and rules. As previously mentioned, the FCRA grants authority to the FTC to prevent the unauthorized disclosure of consumer information used in credit, employment, and insurance decisions. *Id.* § 1681. The Gramm-Leach-Bliley Act gives the Commission authority to protect consumer financial data. *Id.* §§ 6801–6809. The Children's Online Privacy Protection Act provides authority over the collection of information about children. *Id.* §§ 6501–6506. The CAN-SPAM Act authorizes the FTC to regulate unsolicited commercial electronic messages. *Id.* §§ 7701–7713. The Telemarketing and Consumer Fraud and Abuse Act gives the Commission authority to target unsolicited telemarketing calls. *Id.* §§ 6101–6108.

[125] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (Dec. 17, 1980), *available at* www.ftc.gov/bcp/policystmt/ad-unfair.htm. The Unfairness Statement, as modified in 1982, was largely codified in 15 U.S.C. § 45(n). Specifically, Congress codified the three-factor unfairness test, but also prohibited the Commission from relying on public policy considerations as a primary basis for an unfairness determination.

ries of substantial harm, while excluding more subjective injuries such as emotional impact.[126]

The three-part unfairness analysis permits the FTC to protect widely recognized consumer privacy interests. The statutory substantial harm requirement as described by the unfairness statement covers widely shared privacy interests in information about individuals' finances, medical conditions, children, as well as intrusions into the home.[127] It likewise excludes the types of privacy concerns that are not societal norms, such as avoiding emotional impact, which may not be widely shared among consumers.[128] It also requires the FTC to balance the substantial harm with the benefits to consumers and competition of the practice affecting privacy.

The Deception Statement makes unlawful those representations, omissions, or practices that are likely to mislead a reasonable consumer under the circumstances about a material fact.[129] Rather than focusing on harm directly, deception focuses on materiality, meaning a representation that is likely to affect a consumer's choice or conduct regarding a product. This definition of deception also leaves room for the consideration of privacy as norm, both in terms of what is a reasonable consumer and what is a material fact to such a consumer. In practice, however, the FTC has used its deception authority primarily to challenge overt misrepresentations about privacy practices that are presumptively material. The deception approach helps to protect consumers who choose a particular product based upon the company's representations about that product's privacy impact. Enforcement under the deception standard vindicates such choices, even though the protected privacy interests may not rise to the level of a societal norm. Such an approach protects consumer choice and it avoids mandating that all products offer that heightened level of privacy.[130] In turn, the FTC's unfairness authority provides a baseline protection for privacy preferences that most consumers share.

Although the concepts of deception and unfairness play large roles in the FTC's approach to privacy, the agency has over time shifted from an initial reliance on deception to a greater focus on harms-based unfairness theories. The FTC based its first online privacy framework, the "notice and choice model," on Fair Information Practice Principles (FIPPs) developed by the

---

[126] *Id.*

[127] *The FTC at 100: Views from the Academic Experts: Hearing Before the House Subcomm. on Commerce, Manufacturing, and Trade Committee on Energy and Commerce*, 113th Cong. 15 (Feb. 28, 2014) (statement of J. Howard Beales, III).

[128] *Id.*

[129] Fed. Trade Comm'n, FTC Policy Statement on Deception (Oct. 14, 1983), *available at* www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[130] *The FTC at 100*, *supra* note 127, at 4.

U.S. Department of Health Education and Welfare in 1973.[131] As applied by the FTC, these principles require businesses to provide consumers with: (1) *notice* of a business's information practices; (2) *choice* as to the use and dissemination of information collected from or about the consumer; (3) *access* to collected and stored consumer information; and (4) appropriate *security* and *integrity* of any collected information.[132]

The practical effect of this focus on notice and choice was that companies created privacy policies describing how they collect and use customer information. This had the beneficial effect of allowing consumer groups and other privacy advocates, as well as consumers willing and able to read and comprehend such notices, to get information about a company's privacy practices.[133] Early online enforcement actions targeted companies that failed to comply with promises in their privacy policies about how they collected and used data.[134]

Over time, it became apparent that notice and choice policies had weaknesses, potentially allowing companies to overwhelm consumers with lengthy policies filled with legalese.[135] In a detailed critique of FIPPs, Professor Fred H. Cate observed:

---

[131] U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS 40–41 (1973).

[132] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS ii (1998). In the 1990s, the FTC repeatedly urged industry to adopt practices that reflect these principles. In 1998, based on a survey of commercial websites, the FTC concluded that "the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness)." *Id.* at 41. (The survey cited in the 1998 Report revealed that almost all web sites (92% of the comprehensive random sample) were collecting personal information from consumers, few (14%) disclosed anything about their information practices, and it encouraged companies to adopt all four principles. *See id.* at iii, 23 fig.1.) The agency repeated this recommendation in a 1999 report to Congress. *See* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 12–13 (1999). In 2000, the Commission followed up with a recommendation for federal legislation to require "[c]onsumer oriented commercial Web sites that collect personal identifying information from or about consumers online . . . to comply with the four widely-accepted fair information practices . . . ." FED TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000).

[133] Privacy watchdog groups very quickly surface and circulate any privacy policy containing unsavory or surprising collections or uses. *See, e.g.*, Zachary Rodgers, *Advocacy Groups Coalesce to Fight NebuAd*, CLICKZ (June 27, 2008), www.clickz.com/clickz/news/1707124/advocacy-groups-coalesce-fight-nebuad ("At least six advocacy groups have banded together to share information, conduct legal analysis, and meet with officials on Capitol Hill. The coalition brings together a significant number of Net policy groups, including the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF), the Center for Democracy and Technology (CDT), the Center for Digital Democracy (CDD), Public Knowledge, and Free Press.").

[134] Complaint, Geocities, FTC Docket No. C-3850 (Feb. 5, 1999), *available at* www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm.

[135] Some parties have criticized the notice-and-choice approach, arguing that it results in long, densely written privacy policies that consumers do not read and that fail to provide any real

> As theoretically appealing as this approach may be, it has proven unsuccessful in practice. Businesses and other data users are burdened with legal obligations while individuals endure an onslaught of notices and opportunities for often limited choice. Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice.[136]

Thus, by the late 1990s, observers began to argue that a deception-based approach to privacy was not enough.

In the early 2000s, the Commission changed tack to focus more explicitly on specific harms to consumers in connection with privacy.[137] This tactic did not discard the notice and choice rubric but rather honed in on the practices that most spurred consumers' concerns about privacy. Rather than focusing on notice and choice for all data collection and uses, the harms-based approach asks whether a firm's practices cause or could likely cause physical or economic harm, or "unwanted intrusions in [consumers'] daily lives."[138] Under this unified conceptual approach, the Commission continued to act when companies did not comply with the material terms of their posted privacy policies, but also has emphasized harms-based privacy violations often based on its unfairness authority, extending its enforcement into several areas, such as data security, identity theft, spam, spyware, and unwanted telemarketing.[139] In response to technologies that collect and use consumer data in new ways, such as the advent of online behavioral advertising, the Commission has offered guidance to consumer-facing businesses about how to avoid deception or unfair handling of consumer data. The FTC has typically done so by issuing

---

choice about or true informed consent to the collections and uses detailed in such policies. *See, e.g.*, Walker, *supra* note 7.

[136] Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 341, 341 (2006); *cf.* Adam Thierer, *In Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 446–47 (2013) ("[S]imply because consumers do not necessarily read or understand every word of a company's privacy policy does not mean a market failure exits. Consider how other disclosure policies or labeling systems work. . . . [A] certain amount of 'rational ignorance' about privacy policies should be expected.").

[137] The harms-based approach also has had its share of criticism. Some have described it as reactive. *See* Brill, *supra* note 61, at 19 (offering a different privacy approach that "may move regulators and businesses away from a reactive model that focuses on privacy concerns after harm is done"). Others may believe that it takes too narrow a view of consumer harms because it does not consider less tangible harms, such as emotional distress or dignity. *See, e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1152, 1161 (2004) ("Continental privacy protections are, at their core, a form of protection of a right to respect and personal dignity.").

[138] Timothy J. Muris, Remarks at the Privacy 2001 Conference: Protecting Consumer's Privacy: 2002 and Beyond (Oct. 4, 2001), *available at* www.ftc.gov/speeches/muris/privisp1002.htm.

[139] *See generally* Beales & Muris, *supra* note 45, at 109.

reports that attempt to capture existing privacy norms as applied to new data uses.[140]

III. FACTORS FOR THE RIGHT APPROACH TO PRIVACY

Identifying the right approach to privacy under the law has been a topic of discussion, on and off, for over a century. Attempting to craft a universal definition of privacy is notoriously contentious and, likely, impossible.[141] This is especially true given the range of privacy preferences even within the United States, no less around the world. Nonetheless, to find the right enforcement approach, one must acknowledge that privacy is subjective, contextual,

---

[140] For example, in 2009 the FTC staff issued *Self-Regulatory Principles for Online Behavioral Advertising*. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009). These principles call for transparency and consumer control and reasonable security for consumer data, which reflect the FIPPs principles. They also call on companies to obtain affirmative express consent from consumers before they use data in a manner that is materially different than was promised at the time of collection and before they collect and use "sensitive" consumer data for behavioral advertising. In 2012, the Commission issued a comprehensive privacy report with legislative recommendations that championed ideas like privacy by design, simplified consumer choices, and heightened transparency in keeping with the FIPPs principles. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012). The FTC recommendations are similar, but not identical, to the Obama Administration's proposed Consumer Privacy Bill of Rights, which includes individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability. THE WHITE HOUSE, CONSUMER PRIVACY BILL OF RIGHTS ACT (Jan. 2015).

The FTC has also tried to guide the behavior of certain non-consumer facing entities that aggregate and analyze consumer data. In May 2014, the Commission issued a report based on its in-depth study of data broker practices outside the scope of the FCRA, including how they use, share, and secure consumer data. FTC DATA BROKERS REPORT, *supra* note 47. The study revealed that data brokers engage in practices similar to those that had raised concerns more than 40 years ago about the credit reporting industry: collection of information about nearly every U.S. consumer from numerous sources (both online and offline), largely without consumers' knowledge; extensive sharing of such consumer information with other data brokers; and use of data to make inferences about consumers, including potentially sensitive inferences. *Id.* at iv–v.

As with credit reporting, data broker products offer certain commercial and consumer benefits. Specifically, the Commission found that the brokers' marketing products, risk mitigation products, and people search products offer benefits to consumers, such as improved products and reduced fraud. The Commission further found that data brokers' collection and use of consumer data also pose risks, such as the denial of benefits without recourse or the insecure maintenance of data.

Based on its findings, the FTC recommended that Congress consider legislation to increase transparency for consumers and provide some rights similar, albeit not identical, to those offered by the FCRA. The legislative proposals would require that data brokers provide consumers access to their data, including sensitive data held about them, at a reasonable level of detail, and the ability to opt out of having it shared for marketing purposes. *Id.* at viii–iv, 49–54 (detailing legislative recommendations). The agency also recommended that consumers receive notice when a company uses a risk mitigation product that limits the consumer's ability to engage in a transaction (in situations not already covered by the FCRA) and the right to access and correct the relevant data.

[141] *See, e.g.*, Thierer, *supra* note 136, at 411 ("Privacy has long been a thorny philosophical and jurisprudential matter; few can agree on its contours or can cite firm constitutional grounding for the rights or restrictions they articulate.").

and has commercial value. Privacy therefore increasingly represents a non-price dimension of competition. Similarly, consumer data is an increasingly important commercial good for digital platforms.

Given these developments, privacy issues may have some role in an antitrust analysis but that role must be consistent with the goal of antitrust, which is to promote economic efficiency that enhances consumer welfare,[142] not to address other types of harm. Similarly, any approach to privacy must comport with the goal of modern consumer protection policy, which is "to protect consumer sovereignty by attacking practices that impede consumers' ability to make informed choices, such as fraud, unilateral breach of contract, and unauthorized billing."[143] Based on these points, we recommend analytical screens that would help distinguish between privacy-related issues best handled under the competition laws from those best addressed by consumer protection laws or sectoral privacy laws.

A. PRIVACY AND COMPETITION: ANALYTICAL CONSIDERATIONS

Most of the proposals to use competition law to address privacy are concerned about mergers or acquisitions by data-rich companies that combine previously separate pools of information about consumers. They contend the combination of data itself raises a privacy concern warranting intervention, rather than arguing that the transaction reduces privacy as a non-price attribute of competition or that it will create undue power in the market for consumer data.

Although concerns about the creation of large datasets with personal information are not baseless, attempting to address these concerns by fitting them into an analytical rubric preoccupied with economic efficiency creates more issues than it solves. First, it ignores the fact that consolidation of data across business platforms often creates significant efficiencies and gains in consumer welfare. These efficiency gains animated the DOJ's decision to approve Microsoft's search engine venture with Yahoo![144] Any similarly orthodox antitrust analysis could well endorse such a transaction on an empirical basis while leaving the potential privacy harms of certain consumers untouched. Second, if the traditional antitrust analysis is modified to allow for subjective determinations of harm to consumer privacy, it could result in differential

---

[142] RICHARD A. POSNER, ANTITRUST LAW 1–2, 9–32 (2d ed. 2001) (explaining goal of antitrust is to promote economic efficiency and highlighting reduction in output by monopolist).

[143] Timothy J. Muris, Remarks Before the Aspen Summit, Cyberspace and the American Dream, The Progress and Freedom Foundation: The Federal Trade Commission and the Future of U.S. Consumer Protection Policy (Aug. 19, 2003), *available at* www.ftc.gov/public-statements/2003/08/federal-trade-commission-and-future-development-us-consumer-protection.

[144] *See discussion supra* Part II.C.1; *see also* Lande, *supra* note 8, at 1 (arguing that the deal would harm competition).

treatment among mergers—the outcome of each depending heavily on the identity of the reviewers and their unique perceptions of privacy—and as between mergers and other forms of data accumulation with similar privacy implications.[145] Notably, concerns about data brokers and big data likewise revolve around the concept that compilations of even small and disconnected pieces of data—including data previously gathered and held by different parties—may be analyzed to reveal additional personal information about individuals, which may then be used for new purposes. If the perceived privacy harm is the same, however, it would be anomalous to treat data combined through a merger differently from that compiled piecemeal by a data broker or by another type of entity, such as a large Internet company, through its own collection and analysis. Finally, modifying the antitrust laws to encompass normative privacy concerns creates incentives for firms to alter deal structures or enter alternative contractual relationships to take advantage of this asymmetric treatment under the law.

An even more troubling concern is that this approach risks reducing competition and innovation from new products that the combined data may enable, making all consumers worse off, even those who do not share the same privacy preferences or are willing to trade some diminution in privacy for increased quality or new offerings. For example, if the DOJ had focused on privacy implications of Microsoft/Yahoo!, it may very well have blocked the deal, foreclosing the possibility that these search engines would remain in the market. Similarly, if the FTC took this approach in Facebook/WhatsApp, rather than issuing a letter reminding Facebook/WhatsApp of their privacy obligations, it could have moved to prevent the acquisition without offering any reasonable empirical basis.

B. CHOOSING THE RIGHT APPROACH

Rather than expanding antitrust law as some have proposed, we instead recommend applying three screens to discern the best body of law to handle a potential privacy issue. First, we suggest that the type of harm should continue to guide the choice of law, as set out by Congress and developed by the agencies and courts for decades. That is, the application of competition law is appropriate only where the potential harm is grounded in the actual or potential diminution of economic efficiency. If there is likely no efficiency loss because of the conduct or transaction, another legal avenue for enforcement is more appropriate and efficient. Second, the scope of the potential harm also should aid in the choice of law. Antitrust laws are focused on broader,

---

[145] Indeed, scale and efficiencies in data usage can be achieved in many ways—there is no basis to conclude that organic growth is somehow better than synergistic growth by merger or acquisition. *See, e.g.*, BOSTON CONSULTING GROUP, GROWING THROUGH ACQUISITION 6–8 (2004).

macroeconomic harms, mainly the maintenance of efficient price discovery in the markets, whereas the consumer protection laws are preoccupied with ensuring the integrity of each specific contractual bargain. These are complementary, but discrete, enforcement goals. Third, and finally, the available remedies must be able to address effectively the potential harm. Enjoining a merger may do little to prevent a privacy violation if the parties can simply share the same consumer information under a contractual arrangement.

1. *Focus on the Type of Harm*

John Locke noted, "The great and chief end [ ] of . . . government, is the preservation of [citizens'] property," which includes their "lives, liberties, and estates."[146] As we have shown, the government has over time pursued specific laws narrowly tailored to address particular harms. This trend to more nuanced and sophisticated legal mechanisms has allowed for deepened expertise and greater analytical precision in both competition and consumer protection. Splicing them together again, and using the modern antitrust laws, which are empirically focused on economic efficiency, to remedy harms relating to normative concerns about informational privacy contradicts the specialized nature of these laws and risks distorting them in ways that would leave both the law and consumers worse off. The better approach would be to continue the measured improvement of precise legal tools directed to specific harms.

A blended approach to antitrust that encompasses normative privacy concerns also would provide cover for the injection of other noncompetition factors into the analysis. As a normative matter, privacy is conceptually unsettled and, depending on who you ask, could include other rights, like property rights or human dignity.[147] The introduction of these factors could shift antitrust law's focus away from efficiency and alter its relatively predictable and transparent application.

Arguments in response to this concern about doctrinal distortion posit that, for example, the merged entity will have an increased incentive to break privacy promises it made to consumers when it collected the information, making the issue cognizable under the antitrust laws.[148] Or that the aggregation of

---

[146] John Locke, *The Second Treatise of Government* §§ 123–124, *in* TWO TREATISES ON GOVERNMENT 395 (P. Laslett rev. ed. 1963) (3d ed. 1698).

[147] *See, e.g.*, *Privacy*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Aug. 2013 ed.), plato.stanford.edu/entries/ privacy (discussing evolution of privacy and the debate over its definition).

[148] While the Clayton Act allows for the pursuit of certain prospective violations of the law, the issues that it confronts, for example supracompetitive pricing resulting from an undue concentration of suppliers, are fundamentally different than what the consumer protection laws contemplate. Whereas the Clayton Act is quantitative and agnostic in its characterization of a merger as a violation of law, the consumer protection standards are qualitative, requiring that an "act or practice" be either deceptive or both unfair and cause substantial harm to the consumer.

consumer data represents a reduction in quality, diminution in consumer choice, or a heightened barrier to entry.[149] Although these concerns could be relevant where privacy is an actual dimension of competition, a substantial body of literature challenges application of these arguments more broadly by pointing out the lack of limiting principles for theories of harm tethered to reductions of choice and the heterogeneous consumer demand for privacy.[150] But, for our purposes, perhaps the most important point is that attempting to distort the antitrust laws to pursue subjective noncompetition harms is *unnecessary* and would take us back to a less sophisticated approach to law enforcement.

Following Congressional design, the FTC for decades has successfully challenged failures to adhere to privacy promises through its deception authority.[151] Moreover, the arguments for using competition law to address privacy have as an undercurrent the idea that the insights gleaned from the combined data will allow companies to disadvantage consumers without consumers' knowledge or any right to redress. As previously noted, the FTC can use unfairness to challenge uses of data that cause substantial harm to consumers that are not outweighed by countervailing benefits to competition or consumers and which the consumer cannot reasonably avoid. And the FCRA limits the ability of entities to use individual consumer information in connection with credit, housing, insurance, and employment without providing safeguards such as notice, access, and correction rights. These laws are all carefully tailored to address specific harms. There is simply no need to inject deeply subjective privacy considerations into the antitrust laws, or to extend antitrust law to fill putative gaps in consumer protection enforcement, as some suggest.

2. *Look to the Scope of Harm*

Similarly, the antitrust laws and the consumer protection laws, while complementary tools for the protection and promotion of consumer welfare, are trained on different aspects of the commercial environment. The consumer protection laws are in some respects narrow in their scope. They focus on the reasonable consumer and ensuring individual consumers get the benefit of the bargain. Both deception and unfairness seek to safeguard "consumer sover-

---

[149] *See* Cooper, *supra* note 40, at 1129–33 (summarizing attempts to incorporate privacy into the antitrust laws).

[150] *See, e.g.*, Shelanski, *supra* note 38, at 1675–79 (discussing this debate); Farrell, *supra* note 8 (exploring issues relating to monetization of consumer data); Oz Shy & Rune Stenbacka, Customer Privacy and Competition (Working Paper Nov. 2014); Alessandro Acquisiti, *The Economics of Personal Data and the Economics of Privacy* (OECD Background Paper No. 3, Dec. 2010) (describing the history of the economic debate surrounding privacy).

[151] *See, e.g.*, Complaint, Geocities, FTC Docket No. C-3850 (Feb. 5, 1999), a*vailable at* www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm.

eignty," allowing for informed choice when the consumer enters a transaction or uses a product or service.[152] As such, a consumer protection analysis examines the reasonable consumer's conduct and focuses on the relatively narrow domain of preserving the viability of the individual transaction.

By contrast, antitrust law does not try to protect individual consumer expectations or use in its analysis the anticipated conduct of a reasonable consumer. Its pursuit is broader, to promote economic efficiency and long-run consumer welfare, which may include the welfare of consumers who are not even in the market at the time of the transaction. Therefore, the more the scope of the potential privacy harm turns on individual consumer conduct and relates to the viability of the discrete bargain, the less likely it is to be a competition violation and more likely a consumer protection violation or other kind of harm.

3. *Evaluate the Potential Effectiveness of the Remedy*

A third factor to consider is whether the remedies available under the laws can actually address the claimed harms. Although antitrust laws can be used to block transactions, they are not a panacea for privacy issues. If the FTC were to block a transaction between two companies with large datasets, this would not eliminate the problem. Presumably, the parties would then have a strong incentive to structure another transaction, perhaps through licensing arrangements or divestiture of their respective data to third-party data warehouses, which could avoid triggering antitrust review. Moreover, as noted above, the antitrust laws cannot easily remedy privacy issues that may arise from the long-term accumulation of data by a single entity.

By contrast, the consumer protection laws offer more effective remedies in response to privacy violations. They allow for actions against companies that violate promises to consumers about how their data will be collected, used, and shared. The antitrust laws offer no such remedial authority for failure to keep promises, unless there also has been harm to competition—something we have shown the FTC at times risked its credibility to find in its earliest false advertising cases. In addition, if a transaction changes a company's incentives and it subsequently uses data in a way that causes substantial harm to consumers, as defined by the Unfairness Statement, the FTC can stop that action and require the company to take steps to make consumers whole and prevent its reoccurrence.[153]

---

[152] Muris, *supra* note 143.

[153] A variety of commentators have suggested approaches that focus on how personal information may be used to affect an individual, rather than attempting to safeguard privacy primarily by focusing on consumer notice and choice about data collection and usage. These approaches emphasize the difficulty of specifying unforeseen but valuable subsequent uses of data. To alleviate these failings, they offer (in various formulations collectively called use-based) a framework that

IV. CONCLUSION

Despite claims to the contrary, competition law offers at best a convoluted and indirect approach to protecting people's expectations of privacy online. Attempting to unify the competition and consumer protection laws creates needless risks for the Internet economy and could destabilize the modern consensus on antitrust analysis, again pulling it away from rigorous, scientific methods developed in the last few decades and reverting back to the influence of subjective noncompetition factors. Indeed, trying to expand competition law as some have proposed better reflects legal thinking in 1915, not 2015. Although privacy can be (and is today) a dimension of competition, the more direct route to protecting privacy as a norm lies in the consumer protection laws.

---

focuses on preventing harmful uses of personal information, *see, e.g.*, Cate, *supra* note 136, at 368 ("Data protection laws should regulate information flows when necessary to protect individuals from harmful uses of information [and] . . . to prevent tangible harms [defined as damage to persons or property] to individuals . . . The government should not regulate uses that present no reasonable likelihood of harm."); WORLD ECONOMIC FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 12 (Feb. 2013) ("It will require a shift from controlling data collection to focusing on data usage. . . . [P]ermissions, controls and trustworthy data practices need to be established that enable the value-creating applications of data but prevent the intrusive and damaging ones."), accountability for use of personal data however collected, *id.*, a respect for context, *id.*, and transparency about the use of such data with a concomitant ability of consumers to know if data has been used to disadvantage them. *Id.* Another key attribute of the use-based model is its appreciation that, to obtain the best outcome for society, we must balance the benefits of data usage with its risks, rather than treating privacy as unalloyed social good. *Id.* ("In some cases, failure to use data (for example, to diagnose a medical condition) can lead to bad outcomes—not only at an individual or societal level, but also in economic terms, just as its use can create risks."); Cate, *supra* note 136, at 369 ("Data protection is not an end in itself, but rather a tool for enhancing individual and societal welfare. To be effective, data protection must rest on the recognition that both information flows and individual privacy have value and are necessary in a democratic society and market economy.").