Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 4

Article 1

2019

The Market for User Data

Olivier Sylvain
Fordham University School of Law, sylvain@law.fordham.edu

Recommended Citation

Olivier Sylvain, *The Market for User Data*, 29 Fordham Intell. Prop. Media & Ent. L.J. 1087 (2019).
Available at: https://ir.lawnet.fordham.edu/iplj/vol29/iss4/1

The Market for User Data

Cover Page Footnote

Professor at Fordham University School of Law and Director of the McGannon Center for Communications Research.

The Market for User Data

Olivier Sylvain*

Policymakers are today far more alert than ever before to the myriad ways in which tech companies collect and distribute consumers' data with third-party data brokers and advertisers. We can attribute this new awareness to at least two major news stories from the past six or so years. The first came in 2013, when Edward Snowden, the former National Security Agency contractor, leaked highly classified materials that revealed the ways in which United States national security officials, with the indispensable cooperation of U.S. telecommunications companies, systematically monitored telephone conversations and electronic communications of U.S. citizens and foreign nationals.[1] The story triggered a series of rebukes from civil rights groups, consumer advocates, and foreign leaders around the world. It is not clear whether or the extent to which the NSA or other government agencies have terminated those programs since Snowden's revelation.[2]

The second came in early 2018, when another whistleblower revealed to journalists that researchers to whom Facebook had allowed to collect and study dozens of millions of users' personal data, in turn, shared those troves of personal data with Cambridge Analytica, a political consultancy firm.[3] Cambridge Analytica had

[*] Professor at Fordham University School of Law and Director of the McGannon Center for Communications Research.

[1] *See* Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES, (Aug. 15, 2015), https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html [https://perma.cc/AXJ8-RZ6P].

[2] Ryan Gallagher & Henrik Moltke, *The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight US Cities,* The Intercept (June 25, 2018), https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/ [https://perma.cc/VY6V-Y5UL].

[3] Carole Cadwalladr, *'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower*, GUARDIAN (Mar. 18, 2018, 05:44 AM), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump [https://perma.cc/MW6Q-YSV2].

promoted their access to this data to peddle "psychographic targeting" to political campaigns, including that of Donald Trump in 2016.[4] This more recent revelation has exposed Facebook to what will likely be the largest fine imposed by the Federal Trade Commission ("FTC") in history.[5]

These stories were about the extraordinary misuse and abuse of consumer data by powerful tech companies. But they also are large-scale demonstrations of the *Private-Sector Ecosystem of User Data*—the theme of the fall 2018 symposium to which this volume of the *Fordham IPLJ* is committed. At a minimum, these recent episodes, along with others, have dramatically raised our collective awareness about the ways in which consumer data has become the lifeblood of the networked information environment.

Two decades ago, scholars and writers wondered whether online tech companies would ever find a sustainable business model. It appears, however, that, even at that time, some savvy entrepreneurs were on to something. DoubleClick, which is now owned by Alphabet, for example, had already developed techniques to track users' web browsing activity across their hundreds of affiliated sites.[6] There, of course, was nothing novel in the idea of an advertising-based business model; advertising has defined the political economy of the media and communications industry at least since the nineteenth century. But, at the turn of the century, it was not evident to anyone but just a relatively few scholars and entrepreneurs in the start-up world that targeted behavioral advertising would have purchase in the networked information economy.[7]

[4] Sue Halpern, *Cambridge Analytica and the Perils of Psychographics*, NEW YORKER (Mar. 30, 2018), https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics [https://perma.cc/7AZG-KHDM].

[5] Mike Isaac and Cecilia Kang, *Facebook Expects to Be Fined Up to $5 Billion by F.T.C. Over Privacy Issues*, N.Y. Times (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html [https://perma.cc/2V9V-63AG].

[6] *See In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[7] *See generally* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (1999); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1994).

Two decades later, companies have been refining the advertising-based business model. They have been developing ever more powerful algorithmic processes for harvesting, trading on, and exploiting personal consumer data for advertisers.[8] These computational techniques have empowered firms to collect extraordinary amounts of consumer data, anticipate consumer preferences based on that data, and microtarget advertising to individual users based on those predictions.[9] It is all a marketer's dream. And, if click-through rates are to be believed, consumers are sold.[10]

WHEN ALGORITHMS GO AWRY

But sometimes these algorithms make mistakes. While these errors are often innocuous, they are occasionally tone-deaf, as when Virginia Eubanks, who wrote a marvelous book about the ways in which algorithmic decisionmaking processes can be disastrous for the most vulnerable among us, received an advertisement for her own book.[11] Sometimes their mistakes are in very poor taste and offensive, as when Facebook created an advertisement out of a violently misogynistic Instagram post originally sent to a prominent female tech reporter.[12] Or when a social media algorithm distributed

[8] *See, e.g.*, TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (2016).

[9] *See* Zeynep Tufekci, *How Recommendation Algorithms Run the World*, WIRED (Apr. 22, 2019), https://www.wired.com/story/how-recommendation-algorithms-run-the-world/ [https://perma.cc/2ZFS-JFPD].

[10] *See* Rasmus Kleis Nielsen, *People Want Personalised Recommendations (Even as They Worry about the Consequences)*, DIGITAL NEWS REPORT (2016), http://www.digitalnewsreport.org/essays/2016/people-want-personalised-recommendations/ [https://perma.cc/3YP9-Q7NM].

[11] *See* @PopTechWorks, TWITTER (May 14, 2010, 1:11 PM), https://twitter.com/PopTechWorks/status/1128392383966654464 [https://perma.cc/A3VH-YQAF].

[12] *See* Sam Levin, *Instagram Uses 'I Will Rape You' Post as Facebook Ad in Latest Algorithm Mishap*, GUARDIAN (Sept. 21, 2017), http://www.theguardian.com/technology/2017/sep/21/instagram-death-threat-facebook-olivia-solon [https://perma.cc/55EM-X227].

an advertisement for gay conversion therapy to members of the LGBTQ community.[13]

Sometimes companies purposefully design their advertisements to target audiences in ways that, while lawful and rational, are unseemly. For example, in 2012, Orbitz, the travel fare aggregator, relied on consumer data to steer Mac users to pricier hotels on the finding that such users spend 30% more on hotels than PC users.[14] Price discrimination is not illegal, for the most part, but selective marketing techniques like these consumers are hardly harmless to those who are systematically chosen to pay more than others or, for that matter, to those who are never exposed to fancier lodging. Much more recently, we learned that Netflix tested advertising about movies based on their various audiences' race and gender by, for example, emphasizing black characters to black audiences even when those characters play minor roles.[15]

Every now and again, algorithmic microtargeting enables or encourages violations of law. Just this past spring, for example, Facebook agreed to settle a series of lawsuits that alleged that its Ad Manager generated marketing classifications that made it possible for advertisers to discriminate against people on the basis of protected categories like race, gender, and age in violation of civil rights laws.[16] The social media company had harvested and analyzed

[13] *See* Mary Elizabeth Williams, *Facebook Removes Ads for Gay Conversion Therapy After Backlash*, SALON (Aug. 31, 2018), https://www.salon.com/2018/08/31/facebook-removes-ads-for-gay-conversion-therapy-after-backlash/ [https://perma.cc/UN8S-G36C].

[14] *See* Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. JOURNAL (Aug. 23, 2012), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882 [https://perma.cc/E6TT-8JXA].

[15] *See* Lucas Shaw & Jordyn Holman, *Netflix Denies Tailoring Its Movie Promotions Based on Race* (Oct. 22, 2018), https://www.bloomberg.com/news/articles/2018-10-22/netflix-denies-tailoring-movie-promotions-based-on-users-race [https://perma.cc/38ZT-ZVJF].

[16] *See* Katie Benner, Glenn Thrush & Mike Isaac *Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says,* N.Y. TIMES (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html [https://perma.cc/UA5C-FKX9]. In the settlement, Facebook did not admit legal wrongdoing, but it nevertheless agreed, among other things, to discontinue its use of those categories in markets for housing, employment, and credit. *See id.*; *see also* Olivier Sylvain, *Discriminatory Designs on User Data*, EMERGING THREATS SERIES, KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY (Apr. 2018), https://knightcolumbia.org/content/discriminatory-designs-user-data [https://perma.cc/8QD5-AF3P].

its consumers' data to generate the unlawful categories. It is impossible that the vast majority of users wanted data about them to be used in this way.

Microtargeting techniques present challenges as much as they provide opportunities. So much of the algorithmic outputs depend on the data on which their designers "train" them.[17] If the algorithms do not learn from their masters to be law-abiding, those algorithms will of course break the law.

The same might be said about other classes of user information, including biometric data which can, on the one hand, be inputs through which algorithms might keep us safer and create new efficiencies.[18] (See, for example, fingerprinting on iPhones.) But, in the wrong hands, biometric data also can enable discrimination against classes of people.[19] This is to say nothing of the variety of ways in which the technology is easily susceptible to abuse by governments and private actors. This is why facial recognition technology may very well be too difficult to administer in democracies with longstanding constitutional commitments to procedural and substantive fairness.[20]

[17] *See generally* AI Now, DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI (Apr. 2019), https://ainowinstitute.org/discriminatingsystems.pdf [https://perma.cc/9S93-FGA4].

[18] *See* Elizabeth Joh, *Want to See My Genes? Get a Warrant*, N.Y. Times (June 11, 2019), https://www.nytimes.com/2019/06/11/opinion/police-dna-warrant.html [https://perma.cc/37AH-N6QR]; James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/QM34-Y5E3].

[19] *See* Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It.*, TIME (Feb. 7, 2019), http://time.com/5520558/artificial-intelligence-racial-gender-bias/ [https://perma.cc/C9UX-BGDT]; Steve Lohr, *Facial Recognition Is Accurate if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/4GAP-K5KH].

[20] Evan Selinger & Woodrow Hartzog, *Amazon Needs to Stop Providing Facial Recognition Tech for the Government*, MEDIUM (Jun. 21, 2018), https://medium.com/s/story/amazon-needs-to-stop-providing-facial-recognition-tech-for-the-government-795741a016a6 [https://perma.cc/RXL3-DPK3]. *See also* Kate Conger, *The Man Behind San Francisco's Facial Recognition Ban Is Working on More. Way More.*, N.Y. TIMES (May 15, 2019), https://www.nytimes.com/2019/05/15/technology/facial-recognition-san-francisco-ban.html [https://perma.cc/8KDW-ECWL].

WHERE AND HOW DOES LAW COME IN?

In the past couple of years, in light of mounting public concern, legislatures and regulators around the world have announced new protections for consumers. To be sure, consumers have had legal recourse since the nineteenth century.[21] But, today, policymakers have sought reforms in recognition of the massive scale and distinctive nature of the private-sector ecosystem of consumer data.

The European Union has been at the forefront of this effort, enacting the comprehensive General Data Protection Regulation ("GDPR").[22] It has only been a year since that law has been in effect, but we can already identify the important trends.[23] Under the GDPR, companies must give consumers (what the regulation calls "data subjects") access to the data that they have about them, and ensure meaningful user consent to process that information.[24] Consumers also have the right to withdraw this consent "at any time,"[25] as well as the right to "rectification"[26] and "erasure."[27] (These are concepts that had been set out in the now defunct EU Data Protection Directive and elaborated in the European Court of Justice's pre-GDPR opinions.[28]) The GDPR provides, moreover, that companies may not share a user's data to third parties for any purposes that are

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

[22] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

[23] *See, e.g.*, Mathew J. Schwartz, *GDPR: Europe Counts 65,000 Data Breach Notifications So Far*, GovInfo (May 16, 2019), https://www.govinfosecurity.com/gdpr-europe-counts-65000-data-breach-notifications-so-far-a-12489#.XOKLGMyqUjo.twitter [https://perma.cc/7JVM-NW4B]. *See generally* EUROPEAN DATA PROTECTION BOARD, *First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisor Authorities* (Mar. 18, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf [https://perma.cc/9LQ2-RWMW].

[24] GDPR, Ch. 2, Art 7.

[25] *Id.*

[26] GDPR, Ch. 16.

[27] GDPR, Ch. 17.

[28] European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, (1995)

"incompatible" with the ones for which that user shared their data to begin with.[29] The GDPR imposes significant fines for violations of its terms.[30] Questions remain about the new law's extraterritorial scope,[31] but it nevertheless is a significant reform, at least because U.S.-based companies that do business in Europe have been forced to change their consumer data management practices.

Federal lawmakers in the United States have not mustered a national consensus on anything that resembles the GDPR. Instead, here, federal privacy law has been sectoral for decades, with statutes addressing specific actors in delineated legislative fields through, for example, the Federal Educational Rights and Privacy Act, the Health Insurance Portability and Accountability Act, the Financial Credit Reporting Act, and the Video Privacy Protection Act.

For the past several decades, the FTC has relied on its organic statute to justify a wide range of enforcement actions and guidance for industry's administration of consumer data.[32] It has exercised this authority in fits and starts, largely because Congress substantially curtailed the agency's ability to promulgate "notice and comment" rules in the area.[33] In spite of the substantial hurdles imposed by Congress in 1975[34] the agency proposed this past March to fortify existing rules for the protection of "the privacy and security of customer information held by financial institutions."[35] It has also been in talks with Facebook following its investigation of

[29] GDPR, Ch. 2, Art. 5.

[30] GDPR, Ch. 8, Art. 83.

[31] *See, e.g.*, Joshua Blume, *A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR*, 49 GEO. J. INT'L L. 1425, 1446-55 (2019); Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY TECH. L. J. 287, 348-51 (2018).

[32] *See, e.g.*, *Federal Trade Commission v. Wyndham*, 799 F.3d 236 (3d Cir. 2015).

[33] *See* Magnuson Moss Warranty-Federal Trade Commission Improvements Act § 202, Pub. L. No. 93-637, 88 Stat. 2183 (amending 15 U.S.C. §§ 41 et seq. 57a–58 (1975)).

[34] Scholars have argued that Congress should increase the scope of the FTC's authority. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

[35] Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 314).

the Cambridge Analytica scandal.[36] The size and nature of their sanction against the social media giant will reveal how far the agency is willing to go to vindicate its position as the primary federal protector of consumer data.

State and city governments have stepped up in the absence of a comprehensive federal data protection law. Illinois became a leader among the states when, in 2008, its legislature passed the Biometric Information Privacy Act ("BIPA").[37] As the title suggests, BIPA imposes strict duties on the collection and storage of consumers' biometric data. It requires, among other things, that companies obtain consent from consumers to collect or disclose such information, destroy that data after a certain period of time, and securely store any information the company holds.[38] California's Consumer Privacy Protection Act ("CCPA"), which becomes effective in 2020, however, is probably the most sweeping state law to date, adopting many of the same protections set out in the GDPR, including the right of consumers to access the data that companies have about them, the right of consumers to have that data deleted, and the right to block the selling of the data.[39] San Francisco, for its part, is among the few local governments that have altogether banned government agencies from employing facial recognition technology.[40] New York is considering a similar ban on the use of facial recognition technology in public schools.[41]

[36] Cecilia Kang, *Facebook Set to Create Privacy Positions as Part of F.T.C. Settlement*, N.Y. TIMES (May 1, 2019), https://www.nytimes.com/2019/05/01/technology/facebook-ftc-settlement.html [https://perma.cc/EX94-HQEJ].

[37] Eileen King Bower, Theresa Le & James J. Moffitt, *Illinois Leads the Way for Biometric Privacy Legislation*, LEXOLOGY: CLYDE & CO LLP BLOG (Apr. 15, 2019), https://www.lexology.com/library/detail.aspx?g=b3538a7e-e33b-49fd-b523-a9608d12811f [https://perma.cc/P5NK-KJS3].

[38] 740 ILL. COMP. STAT. 14/15 (2008).

[39] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.175.

[40] Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/K2KC-TZ3H].

[41] *See* N.Y. Legis. Assemb. A-06787. Reg. Sess. 2019–2020 (2019); *see also* Davey Alba, *The First Public Schools in the US Will Start Using Facial Recognition Next Week*, BUZZFEED NEWS (May 29, 2019), https://www.buzzfeednews.com/article/daveyalba/lockport-schools-facial-recognition-pilot-aegis [https://perma.cc/LC36-ZG3C].

Legislators and government regulators have not been the only reformers. The courts have played an important role in delineating the extent to which private companies today may share consumer data with government officials. Consider the Supreme Court's 2018 opinion in *Carpenter v. United States*.[42] There, the Court held that law enforcement officials may only request and obtain subscribers' historical mobile phone location data from telecommunications companies on a showing of probable cause.[43]

Generally, under the Fourth Amendment, law enforcement officials must have probable cause to search "persons, houses, papers, and effects."[44] But, under the third-party doctrine, the Supreme Court has held that this probable cause standard does not apply to law enforcement requests for business records about consumer activity from banks and telecommunications providers.[45] The logic for this rule is relatively straightforward: the records that banks and telephone companies generate and collect about their consumers are an indispensable incident of the services they provide. Consumers do not have a reasonable expectation of privacy in those business records, the Court has explained, because they voluntarily give their data to banks and telephone companies in order to enjoy the services provided.[46]

In *Carpenter*, the Supreme Court decided not to extend the third-party doctrine to historical mobile phone location data. In the aggregate, it explained, location information reveals an unprecedented amount about subscribers that far exceeds the kinds of information that justified the third-party doctrine.[47] The Court did not do away with the doctrine. It only refused to extend it to mobile phone location, suggesting that the rule might be applied to other networked mobile technologies as well.[48]

[42] 138 S. Ct. 2206 (2018).

[43] *Id.* at 2221.

[44] U.S. CONST. amend. IV.

[45] Smith v. Maryland, 442 U.S. 735 (1979) (noncontent telephone records); United States v. Miller, 425 U.S. 435 (1976) (bank records).

[46] *See Smith*, 442 U.S. at 743–744; *Miller*, 425 U.S. at 440.

[47] 138 S.Ct. at 2220.

[48] *Id.* The Court considered whether the collection of location information for seven or more days required a warrant. It did not answer whether its decision would extend to

THE PRIVATE-SECTOR ECOSYSTEM OF USER DATA TODAY

The GDPR, BIPA, the CCPA, and the *Carpenter* decision are good indications that policymakers and courts today are adapting current laws to meet the challenges posed by today's networked information economy. Longstanding consumer protection norms like due process[49] and "notice and consent," for example, will continue to play a role, although there is growing evidence that the latter in particular is not especially protective of users.[50] The question policymakers will have to answer is: what should count as consent, when so much remains unknown to consumers and regulators?[51] In this vein, scholars have made the case for regulatory conventions like transparency and mandated impact assessments.[52] At least for now, these concerns—transparency and accountability—seem to be mobilizing voters and legislators.[53] We might suppose that, no matter how we come out of this important constitutive moment, policymakers ought to foster trust between consumers and the commercial entities that hold and manage their personal data.[54] But this is hardly an inevitable or necessarily optimal way of conceiving of data protection in light of the seductive commercial incentives to trade on access to consumer data.[55]

requests for fewer than seven days. *Id.* at 2217, n.3 (Roberts, J., majority), 2234 (Kennedy, J., dissenting).

[49] *See, e.g.*, Danielle Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2007).

[50] *See* Neil Richards & Woodrow Hartzog, *Pathologies of Digital Consent*, WASH. U. L. REV. (forthcoming 2019).

[51] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

[52] *See, e.g.*, Andrew Selbst, *Disparate Impact in Big Data Policing*, 52 GEORGIA L. REV. 109 (2017).

[53] *See, e.g.*, Margot E. Kaminski & Andrew D. Selbst, *The Legislation That Targets the Racist Impacts of Tech*, N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/tech-racism-algorithms.html [https://perma.cc/FL9Q-ZPX5]; Adi Robertson, *A New Bill Would Force Companies to Check Their Algorithms for Bias*, VERGE (Apr. 10, 2019, 3:52 PM), https://www.theverge.com/2019/4/10/18304960/congress-algorithmic-accountability-act-wyden-clarke-booker-bill-introduced-house-senate [https://perma.cc/DW5D-ZLKX].

[54] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016). *See also* ARI WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018).

[55] *See* Lina Khan & David Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. (forthcoming 2019).

Anyway, for consumers and data protection policymakers, the stakes seem especially high today because we are only now beginning to really comprehend the scale and pervasive integration of the market for user data. Techniques for the collection and distribution of user data define practically all of our experiences today—online and offline. It is not really until consumers and policymakers have a far better understanding of this scope that many of us can rest easy. The *Fordham IPLJ* symposium is one step in that direction.