Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 4

Article 2

2019

The Private-Sector Ecosystem of User Data in the Digital Age

fordhamiplj@gmail.com

The Private-Sector Ecosystem of User Data in the Digital Age

Cover Page Footnote

These summaries are brought to you by the staff and editors of the Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIX. The Journal would like to extend a special thanks to Chloe Curtis, IPLJ's Volume XXIX Symposium Editor, for organizing this 26th Annual IPLJ Symposium. For their help note-taking and transcribing our panels, the Journal would like to thank the Symposium Team Leads: Sarah Fabian Maramarosy, France Svistovski, Gian Mascioli, Roger Hewer-Candee, Hanna Feldman, and Marissa Saravis. Further thanks to Hanna Feldman and France Svistovski, the incoming Editor-in-Chief and Managing Editor of Volume XXX, and Jeffrey Greenwood and Michael Rivera, Editor-in-Chief and Managing Editor of Volume XXIX, for their help organizing, compiling, and editing the final content of these summaries. Finally, the Journal would like to thank all of the panelists and moderators of the Private-Sector Ecosystem of User Data in the Digital Age.

The Private-Sector Ecosystem of User Data in the Digital Age

Fordham Intellectual Property, Media & Entertainment Law Journal*

I. USER CONTROL PANEL

Moderated by Professor Ari Ezra Waldman,[1] the User Data Control panel focused on the ways in which data control can be navigated in today's digital environment. A central theme of the panel related to the preservation of users' privacy rights and the ways in which control can be returned to consumers. Panelists included Nizan Geslevich Packin, Associate Professor at City

* These summaries are brought to you by the staff and editors of the Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIX. The Journal would like to extend a special thanks to Chloe Curtis, IPLJ's Volume XXIX Symposium Editor, for organizing this 26th Annual IPLJ Symposium. For their help note-taking and transcribing our panels, the Journal would like to thank the Symposium Team Leads: Sarah Fabian Maramarosy, France Svistovski, Gian Mascioli, Roger Hewer-Candee, Hanna Feldman, and Marissa Saravis. Further thanks to Hanna Feldman and France Svistovski, the incoming Editor-in-Chief and Managing Editor of Volume XXX, and Jeffrey Greenwood and Michael Rivera, Editor-in-Chief and Managing Editor of Volume XXIX, for their help organizing, compiling, and editing the final content of these summaries. Finally, the Journal would like to thank all of the panelists and moderators of the Private-Sector Ecosystem of User Data in the Digital Age.

1 Ari Ezra Waldman, https://www.nyls.edu/faculty/faculty-profiles/faculty_profiles/ari-ezra-waldman/ (last visited Apr. 19, 2019) [https://perma.cc/SF55-E5C2].

University of New York's Zicklin School of Business;[2] Yafit Lev-Aretz, Associate Professor at City University of New York's Zicklin School of Business;[3] and Andrew Selbst, Postdoctoral Scholar at Data & Society Research Institute and Visiting Fellow at the Yale Information Society Project.[4]

Professor Geslevich Packin's segment focused on individuals' tendency to rely on mobile applications that use decision-making algorithms in order to solve problems as efficiently and inexpensively as possible. She argued that overreliance on algorithms lessens consumers' desires to obtain a proper second opinion. Geslevich Packin explained that consumers rely on the assumption that these services reach the best possible decision and are representative of the truth. However, algorithms are subject to the biases of their creators, and the results generated thus cannot be neutral or objective.[5] In addition, Geslevich Packin argued that overreliance on algorithms may hurt free choice, lead to complacency and stifled innovation, and may lead to the loss of psychological and social values. In addition, the consumers' right to privacy may be affected where consumers depend on algorithms which require the input of personal information. Geslevich Packin proposed adopting choice architecture[6] policies to resolve these issues in order to force consumers to consider issues in user data control and encourage a cultural change.

Professor Yafit Lev-Aretz focused on "data philanthropy," a potentially beneficial use of user data control where data-collecting companies donate private-sector data for socially beneficial

---

2 Nizan Geslevich Packin, https://zicklin.baruch.cuny.edu/faculty-profile/nizan-geslevich-packin/ (last visited Apr. 6, 2019) [https://perma.cc/CS2E-5UHN].

3 Yafit Lev-Aretz, https://zicklin.baruch.cuny.edu/faculty-profile/yafit-lev-aretz/ (last visited Apr. 6, 2019) [https://perma.cc/F66Q-ZMSC].

4 Andrew Selbst, https://andrewselbst.com (last visited Apr. 6, 2019) [https://perma.cc/NA4S-MTX6].

5 *See generally* Batya Friedman & Helen Nissenbau, *Bias in Computer Systems*, 14 ACM Transactions Info. Sys. 330 (1996); *see also* Engin Bozdag, *Bias in Algorithmic Filtering and Personalization*, 15 Ethics Inf. Tech. 209 (2013).

6 Richard Thaler and Cass Sunstein define "choice architecture" as an organization of the context in which people make decisions. *See* RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 3 (2008).

purposes.[7] One example she gave of data philanthropy was creating efficient rescue efforts.[8] Lev-Aretz's presentation emphasized the difficulty in balancing data philanthropy and privacy concerns. She argued that privacy-related concerns are overstated because people constantly waive their privacy rights in a real-world context. Lev-Aretz also considered the inherent conflict between data philanthropy and the current Fair Information Practice Principles ("FIPs").[9] The FIPs require a specifically aimed purpose and impose a "use limitation" where the data can only be used for its specified purpose; both these restrictions conflict with data philanthropy, which involves a repurposing of the data collected to solve an issue unanticipated at the time of the data collection. To resolve this issue, Lev-Aretz proposed a three-pronged exception to the FIPs: (1) require an analysis of the anticipated data use, in order to recognize the need to relax privacy protections in the face of an emergency; (2) conduct a risk assessment to identify when it is appropriate for the data to be employed; and (3) determine whether post-reuse retentions should occur once the emergency has been resolved.

During his section, Andrew Selbst discussed the General Data Protection Directive ("GDPR"), which provides several tools to empower data subjects.[10] Selbst argued that the GDPR's implementation of the notion of consent is problematic for two reasons. First, the right to withdraw consent for data processing

---

7 Yafit Lev-Aretz, *Data Philanthropy*, HASTINGS L. J. (forthcoming 2019).

8 *See* O'Reilly Media, *Data Philanthropy is Good for Business*, FORBES (Sept. 20, 2011), https://www.forbes.com/sites/oreillymedia/2011/09/20/data-philanthropy-is-good-for-business/#61054faf5f70 [https://perma.cc/3MJ4-H6KJ].

9 *See generally* The Privacy Office, U.S. Dept. of Homeland Security, PRIVACY POLICY GUIDANCE MEMORANDUM NUMBER 2008-01, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (Dec. 28, 2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf [https://perma.cc/7DKP-XYY3].

10 EU General Data Protection Regulation (GDPR): Regulation (EU) 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 (General Data Protection Regulation), OJ 2016 L 119/1 [hereinafter GDPR provisions].

inhibits machine learning, as the data set becomes unreliable.[11] Second, Selbst expressed concern for the possibility that the GDPR's terms will not be enforced as written, since the European Union is reluctant to test their power on a global stage. Ultimately, Selbst argued that the GDPR could go further in its approach in order to remedy the exploitation of user data; as an example, Selbst cited the GDPR's failure to police algorithmic decision-making.

Selbst posited that the GDPR's implementation of the data subject's right to an explanation regarding the use of their information should include a functionality threshold.[12] According to Selbst, this threshold is necessary to the extent that it would provide the data subject grounds for contesting decisions and an understanding of ways to achieve their desired income based on the decision-making model.[13] It is not enough to provide the algorithmic decision-making system's technical rationale.[14] Finally, Selbst highlighted the importance of understanding the algorithm's creators' unknown motivations and processes of creation, since it is the algorithm's process—not the ultimate decision—that requires justification. Selbst concluded his segment by highlighting the need for a cultural shift regarding the way consumers think about the data economy.

The panel's full conversation can be found on the Fordham Intellectual Property, Media & Entertainment Law Journal's website here: http://www.fordhamiplj.org/2018/11/06/episode-54-user-control-data-panel-26th-annual-iplj-symposium/.

---

[11] Nick Wallace & Daniel Castro, *The Impact of the EU's New Data Protection Regulation on AI*, CTR. DATA INNOVATION 1, 13 (2018), http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf [https://perma.cc/HYP5-GS3G] (noting that exercising the right to withdraw consent to data processing could undermine the algorithm's decision-making model).

[12] *See* Andrew D. Selbst & Julia Powle, *Meaningful Information and the Right to an Explanation*, 7 INT'L DATA PRIVACY L. 233, 233–42 (2017).

[13] Sandra Wachter et al., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 HARV. J. LAW & TECH. 841, 843 (2018).

[14] *Id.* at 842.

II. DATA GOVERNANCE REGIMES

Moderated by Professor Olivier Sylvain,[15] the Data Governance Regimes panel focused on the challenges of maintaining privacy and confidentiality of data as it continues to accumulate at a blinding rate. Professor Sylvain framed the panel's discussion around the claim that public laws are insufficient to regulate the collection, use, and protection of personal data in the current globalized world. Panelists included Lisa J. Sotto, Partner and Chair, Privacy and Cybersecurity Practice at Hunton Andrews Kurth LLP;[16] Boris Segalis, Partner and Global Vice Chair, Cyber/Data/Privacy at Cooley LLP;[17] Andrew Kopelman, Vice President, Assistant General Counsel, and Chief Privacy Counsel at Medidata Solutions;[18] and Anthony Ford, Senior Data Privacy Counsel at Medidata Solutions.[19]

Together, the panel described data governance, their perceptions of specific data regimes (such as the European Union's General Data Protection Regulation ("GDPR")[20] and the now-defunct Safe Harbor Agreement[21]), the United States' sectoral approach to data privacy combined with corporate self-regulation, and finally engaged in a critical dialogue surrounding the merits of the notice-and-choice regime dominating most of the world's approach to data governance.

---

15 Olivier Sylvain, Professor at Fordham University School of Law and Director of the McGannon Center for Communications Research, https://www.fordham.edu/info/23185/olivier_sylvain [https://perma.cc/688N-RRXN].

16 Lisa J. Sotto, Partner and Chair, Privacy and Cybersecurity Practice at Hunton Andrews Kurth LLP, https://www.huntonak.com/en/people/lisa-sotto.html [https://perma.cc/Q9TD-QPN9].

17 Boris Segalis, Partner and Global Vice Chair, Cyber/Data/Privacy at Cooley LLP, https://www.cooley.com/people/boris-segalis [https://perma.cc/EXX7-R8EN].

18 Andrew Kopelman, Vice President, Assistant General Counsel, and Chief Privacy Counsel at Medidata Solutions, https://www.pli.edu/faculty/andrew-kopelman-29932 [https://perma.cc/GD4D-P7UX].

19 Anthony Ford, Senior Data Privacy Counsel at Medidata Solutions, https://www.linkedin.com/in/anthonyford/ [https://perma.cc/2M3W-TNPK].

20 *See* Commission Regulation 2-16/679, 2016 O.J. (L119) (EU).

21 *See GDPR, the End of Safe Harbor, and What It Could all Mean for Businesses*, NEF (last visited Apr. 5, 2019), https://www.nefiber.com/blog/gdpr-changes-safe-harbor-mean-businesses/ [https://perma.cc/6BFF-HXAS].

Lisa Sotto characterized the confluence of data protection laws as a "cacophony" of rules and requirements, rendering it virtually impossible for any entity to comply with every law. To illustrate, Sotto described three distinct approaches to regulating data which currently exist. The first is the GDPR; the second comprises laws mimicking the old data protection directive;[22] and the third divides data protection regulations by sector. Sotto advocated for the establishment of data governance regimes by companies as an appropriate solution to the problem of compliance. Sotto argued that the best approach for companies in establishing these regimes is to pull basic elements from the existing legal framework in order to ensure the company responsibly handles data. Some of the principles of data governance which should be incorporated include transparency, notice and choice, an individual's right to access their own data, an individual's right for their data to be secure, and enforcement.[23]

Boris Segalis brought attention to the gaps between theory and practice relating to the European Union's GDPR and warned of hindrances to business if data governance is taken to an extreme. He explained that there are three elements to personal data governance: (1) the protection of the data, (2) pure compliance with laws put in place, and (3) leveraging of data protection and legal compliance in order to establish rights to data. The digital economy is driven by data, and Segalis stressed that data can be used for many positive purposes, such as clinical research, background checks, and advertising. Segalis acknowledged that it is important for companies to operate within parameters, but argued that when data governance is taken too far, it can result in an impediment to doing business. Segalis also discussed the GDPR's shortcomings. He stated that while the GDPR is strict on paper, it actually has many holes regarding business practices which results in limited enforcement. In contrast, Segalis stated

---

[22] *See generally* Nate Lord, *What Is the Data Protection Directive? The Predecessor to the GDPR*, Digital Guardian: DataInsider (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr [https://perma.cc/JLH8-VDHU].

[23] *See* Information Commissioner's Office Guide to the General Data Protection Regulation, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ [https://perma.cc/6BK4-CZS6].

that the United States' regime for compliance is significantly more robust for privacy protection.

Anthony Ford and Andrew Kopelman both represented Medidata Solutions at the Symposium, a business-to-business company which provides a platform for clients to acquire and use individual data in clinical trials.[24] Ford and Kopelman contributed a real-world application of a data governance regime by explaining how Medidata's data governance regime impacts the security practices of their company.

Anthony Ford stated that data governance regimes help to keep companies disciplined and accountable by monitoring where data is stored; what the data is being used for; who has access to the data; how many copies of the data are kept; and what level of security different data require. In other words, data governance regimes provide the ability for companies to respond quickly and accurately to outsiders about how Medidata's customers' data is being used. As a result of such fastidiousness, Ford posited that data governance regimes give organizations the ability to comply with the multitude of different legal regimes governing data privacy. Ford emphasized his belief that large firms like Medidata Solutions must identify the legal requirements of data governance most salient to the corporation and build policies and compliance around them.[25]

Andrew Kopelman discussed the need for large firms to have full accountability for customer data and how the concept of ownership in one's data is evolving as firms are beginning to find ways to monetize allegedly anonymized data. He emphasized that Medidata's current data governance regime was not based solely on the GDPR. In constructing the data governance regime, Medidata looked for an appropriate template, and found none that fit the company. Instead, Medidata relied on the overarching principles of data governance to construct a system that would

---

[24] *See* Medidata, https://www.medidata.com/en/professional-services/ [https://perma.cc/8WG5-JX8P].

[25] *See* Ronald Breaux and Sam Jo, *Designing and Implementing an Effective Privacy and Security Plan*, IAPP (Mar. 24, 2014), https://iapp.org/news/a/designing-and-implementing-an-effective-privacy-and-security-plan/ [https://perma.cc/HF5V-DKTL].

adequately address three important questions an individual may have for a corporation using its data: (1) What is the individual's data? (2) What does the company do with it? (3) How does the company do this? Being able to answer these questions results in a corporation that is accountable to the individuals whose data is being used.

The panel's full conversation can be found on the *Fordham Intellectual Property, Media & Entertainment Law Journal*'s website here: http://www.fordhamiplj.org/2018/11/21/episode-55-data-governance-regimes-panel-26th-annual-iplj-symposium/.

III. KEYNOTE SPEECH

Omer Tene, the Vice President and Chief Knowledge Officer at the International Association of Privacy Professionals,[26] centered his keynote speech around the questions of who should control personal data, and what principles and legal framework should govern privacy law. Tene began with a broad overview of the foundation of privacy law, from early conceptions of privacy in hunter-gatherer and agrarian societies 12,000 years ago,[27] through today's data revolution that began in the 20th century.[28] This broad history was cited to demonstrate that human attempts to regulate concepts such as property regulation,[29] industry, capital, and labor have not been perfect despite existing for thousands of years.[30]

---

[26] *About the IAPP*, INT'L ASS'N OF PRIVACY PROFS., https://iapp.org/about/person/0011a00000DlJ5bAAF/ (last visited Oct. 3, 2018) [https://perma.cc/QP75-529V]. Tene is also an Affiliate Scholar at the Stanford Center for Internet and Society and a Senior Fellow at the Future of Privacy Forum.

[27] *The Development of Agriculture*, NAT'L GEOGRAPHIC, https://genographic.nationalgeographic.com/development-of-agriculture/ (last visited Oct. 3, 2018) [https://perma.cc/Y5S3-K2JB].

[28] Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Feb. 12, 2012, at SR1.

[29] *See, e.g.*, Liam Kennedy, *The First Agricultural Revolution: Property Rights in Their Place*, 56 AGRIC. HIST. 379 (1982).

[30] Tene cited the fall of Lehman Brothers ten years ago, on September 15, 2008, and the nationalization of AIG a day later as examples of the failure to regulate land, capital, and industry. *See* Robert J. Samuelson, *Lehman Brothers Collapsed 10 Years Ago. Whose Fault Was It?*, WASH. POST (Aug. 26, 2018), https://www.washingtonpost.com/opinions/lehman-brothers-collapsed-10-years-ago-whose-fault-was-it/2018/08/26/79137b2e-a7dd-11e8-a656-943eefab5daf_story.html?noredirect=on&utm_term=.3c1590d1d661

This proclivity for trial-and-error carries through to the data revolution, with the principles governing data privacy being an artifact of a report written by Alan Westin forty years ago.[31]

Tene also emphasized that these revolutions demonstrate divisions established in society: for the agrarian revolution, it was between landowners and peasants—i.e. the feudal system; for the Industrial Revolution, it was between the capitalists and the proletariat; and now with the data revolution it will be, per Israeli philosopher Yuval Noah Harari, between two different species of humans: the digital users and the common class whose jobs are taken by machines.[32]

Tene stressed that relying on such antiquated principles and frameworks for data privacy is worrying when data is becoming, for many institutions, their most important and valuable asset, and so much power and control of data rests in the hands of so few institutions. Tene argues that data is becoming an asset more valuable than land, industry, or capital, and notes that the top companies in terms of market value on the stock exchange are, as a New York Times tech reporter coined it, the "Frightful Five": Apple and Amazon (both of which just crossed the $1 trillion mark in market capitalization), Google, Microsoft, and Facebook. [33] As data becomes increasingly interconnected[34] and exerts greater

---

[https://perma.cc/CZJ3-N7R2]; Ross Goldberg, *America Nationalizes AIG Group*, N.Y. SUN (Sept. 17, 2008), https://www.nysun.com/business/america-nationalizes-aig-group/86045/ [https://perma.cc/HFM5-XXWE].

[31] *See* SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERS. DATA SYS., U.S. DEPT. OF HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (0S) 73-94, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973) [Hereinafter Secretary's Report].

[32] YUVAL NOAH HARARI, HOMO DEUS: A BRIEF HISTORY OF TOMORROW, ch. 1 (2016).

[33] *See* Farhad Manjoo, *Tech's Frightful Five: They've Got Us*, N.Y. TIMES, May 11, 2017, at B1; *see also* Jason Hall, *The 30 Largest Companies on the Stock Market*, MOTLEY FOOL (Dec. 5, 2017, 10:00 AM), https://www.fool.com/investing/2017/12/05/the-30-largest-companies-on-the-stock-market.aspx [https://perma.cc/H4GU-26WZ]; *Amazon Becomes Second Trillion-Dollar Company in U.S.*, CBS NEWS MONEYWATCH (Sept. 4, 2018, 4:07 PM), https://www.cbsnews.com/news/amazon-worth-1-trillion-stock-price-surge-tuesday-2018-09-04/ [https://perma.cc/GAZ8-T3W7].

[34] *See Shedding Light on Smart City Privacy*, FUTURE PRIVACY F., https://fpf.org/2017/03/30/smart-cities/ (last visited Oct. 7, 2018) [https://perma.cc/3Z59-5V7F].

control over our lives,[35] Tene argued we shouldn't be relying on a traditional regulatory framework that governs older legal concepts as data is "ephemeral, it can be copied and replicated," and transferred "around the globe at the speed of light."[36] In response to data's increasing value, Tene questions whether firms and government institutions should have control of personal data, or whether it should be individuals themselves, what Europeans call "data subjects."[37]

Tene does not believe our worries end with the private market, however. Government control of data is becoming an equally frightening dilemma,[38] and the optimistic view of the Internet as a great equalizer and democratization tool during the Internet's nascent stages ten to fifteen years ago as seen in John Perry Barlow's[39] writings is being challenged by "the data economy as it [has] shaped up with these massive aggregations of power in government and corporate hands." Tene questioned whether the

---

[35] *See, e.g. Nanosensor Array for Medical Diagnoses*, NASA TECH. TRANSFER PROGRAM, https://technology.nasa.gov/patent/TOP2-169 (last visited Oct. 7, 2018) [https://perma.cc/27YY-E3NW]; Michael Specter, *How the DNA Revolution Is Changing Us*, NAT'L GEOGRAPHIC, Aug. 2016, https://www.nationalgeographic.com/magazine/2016/08/dna-crispr-gene-editing-science-ethics/ [https://perma.cc/6S6Z-X6XX]; Suzanne Barlyn, *John Hancock Will Only Sell Interactive Life Insurance with Fitness Data Tracking*, INS. J. (Sept. 19, 2018), https://www.insurancejournal.com/news/national/2018/09/19/501747.htm [https://perma.cc/Z962-CXZ8]; Rachel Botsman, *Big Data Meets Big Brother as China Moves to Rate Its Citizens*, WIRED (Oct. 21, 2017), https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion [https://perma.cc/67UY-EKRG].

[36] *See* Fergal Toomey, *Data, the Speed of Light, and You*, TECHCRUNCH (Nov. 8, 2015), https://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you/ [https://perma.cc/QB9M-QVCD].

[37] *See, e.g.* GEN. DATA PROTECTION REG. (GDPR) art. 4, ¶ 1 (defining "data subject" as an "identified or identifiable natural person").

[38] Tene cited China's attempted implementation of social credit scores on a national level and democratic institutions such as the "Five-Eyes" nations trying to force encryption backdoors to "ensure that no data is beyond the gaze of government." *See* Botsman, *supra* note 35; *see also* Juha Saarinen, *Five-Eyes Nations to Force Encryption Backdoors*, ITNEWS (Sept. 3, 2018, 6:59 AM), https://www.itnews.com.au/news/five-eyes-nations-to-force-encryption-backdoors-511865 [https://perma.cc/K386-ZWJX].

[39] John Perry Barlow, A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE, *available at* https://www.eff.org/cyberspace-independence (last visited Oct. 8, 2018) ("I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us [you being the government]") [https://perma.cc/A4ZR-5TFA].

policy choices society has made—i.e. concentrating markets and locking down data in "corporate coffers" and countries—have been helpful or have harmed us.[40] Regardless of whether it is corporate conglomerates or governments controlling data, Tene argued that individuals get the short end of the stick and often are locked out of sharing bits of their own data.

Tene discussed several regulatory regimes—i.e. property law,[41] antitrust,[42] the law of trusts,[43] and privacy law—that could be employed to counteract the conglomeration of power and control over data by major corporations and governments but ultimately focused on the evolution of the United States' current privacy regime and its antiquatedness.[44] Tene advocated for a change of

---

[40] Tene noted countries like China and Russia have data localizations laws, restricting the transport of data out of countries. *See e.g.* Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, INFO. TECH. INNOVATION. FOUND. (May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost [https://perma.cc/YTU4-Y25U]; *see also*, Editorial, *India's Misguided Move Towards Data Localisation*, FIN. TIMES (Sept. 10, 2018), https://www.ft.com/content/92bb34a8-b4e5-11e8-bbc3-ccd7de085ffe [https://perma.cc/KK3F-T4H4]. Even democratic institutions in Europe are trying to "lock" data in geography. *See* Michelle Rosenberg, *Cross-Border Transfers of Personal Data in Light of GDPR*, FOX ROTHSCHILD LLP (Mar. 23, 2018), https://dataprivacy.foxrothschild.com/2018/03/articles/european-union/gdpr/cross-border-transfers-of-personal-data-in-light-of-gdpr/ [https://perma.cc/3562-E35W].

[41] Tene argued that property law is not strictly applicable to data, since data is a difficult-to-capture, fungible entity.

[42] Tene briefly posited antitrust as a potential tool in this space and cited Pamela Jones Harbour's dissenting opinion in the merger case involving Google and DoubleClick, which put forth the possibility of using antitrust to govern data. *See* In the matter of Google/DoubleClick, 071 F.T.C. 0170 (2007) (Harbour, P.J., dissenting), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf [https://perma.cc/RUY3-GEY5].

[43] Tene mentioned Neil Richards, Woodrow Hartzog, and Jack Balkin as scholars who have written on this subject matter, arguing that companies have a role as information fiduciaries. *See e.g.* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

[44] Tene provided an extensive history of privacy law, from Warren and Brandeis' paper in 1890, to the Restatement of Torts and the Prosser Torts, to Alan Westin's introduction of Fair Information Practices (FIPs) in 1973. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also* Matt Reimann, *How the First Mass-Market Camera Led to the Right of Privacy and 'Roe v. Wade'*, TIMELINE (Mar. 9, 2017), https://timeline.com/how-the-first-mass-market-camera-led-to-the-right-to-privacy-and-roe-v-wade-4fb4cd87df7a [https://perma.cc/EGX5-4JU8];

framework in privacy law, since our current principles are grounded in Westin's FIPs,[45] which are now over forty years old and predate the Internet of Things, mobile phones, AI, and machine learning. Tene did not seem to advocate for one particular solution, although he suggested that a regime should be put in place that allows individuals to not only contribute, but also benefit from data aggregation, and that consent should come from proxies like regulators and consumer associations instead of individuals, because privacy enhancing technologies at the consumer level are not gaining traction.

Tene's full keynote speech can be found on the *Fordham Intellectual Property, Media & Entertainment Law Journal*'s website here: http://www.fordhamiplj.org/2019/05/06/26th-annual-iplj-symposium-keynote-speaker-with-omer-tene/.

IV. TRANSPARENCY OF NOTICE AND CHOICE

Moderated by Professor Ron Lazebnik,[46] the Transparency of Notice and Choice panel focused on website privacy policies and the user's "choice" in allowing companies' access to their private data, or not visiting the website at all. Professor Lazebnik framed the panel's discussion around his argument that even with this choice, the public became and remains exceedingly complacent about notice and choice.[47] Panelists involved in the discussion

---

RESTATEMENT (SECOND) OF TORTS § 652(c) ("One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."); William Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960); Secretary's Advisory Committee on Automated Pers. Data Sys., U.S. Dep't Of Health, Educ. & Welfare, Dhew Pub. No. (0s) 73-94, Records, Computers and the Rights of Citizens (1973).

45 *See* Privacy Policy Memorandum No. 2008-01 from The Privacy Off. of U.S. Dep't of Homeland Security (Dec. 29, 2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf [https://perma.cc/R5MG-8QSR]; *see also* Robert Gellman, *Fair Information Practices: A Basic History.*

46 Ron Lazebnik, Clinical Associate Professor of Law, https://www.fordham.edu/info/23156/ron_lazebnik (last visited Apr. 19, 2019) [https://perma.cc/P3MC-KU97].

47 *See* Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U Rev. L. & Soc. Change 253, 291 (2018). Only when incidents like the Facebook/Cambridge Analytica scandal occurs do people become concerned about their data being accessed and shared. See Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*,

were Paula Breuning, Counsel at Sequel Technology & IP Law;[48] Liz Woolery, Senior Policy Analyst for the Center for Democracy and Technology;[49] Maya Uppaluru, an Associate at Crowell & Moring LLP;[50] and Wendy Seltzer, Strategy Lead and Counsel at the World Wide Web Consortium.[51]

Paula Breuning's segment highlighted that companies often do not realize the ramifications of notice and choice. A significant amount of her work at Sequel is devoted to educating companies as to how to provide their customers with appropriate and meaningful notice. Within the context of this work, she emphasizes the importance of transparency. However, because most regulation is in the form of self-regulation,[52] there is significant variation in how much guidance is needed, or wanted, in the private sector. According to Breuning, some companies welcome specific guidance while others feel that significant prescriptions would hinder their operation in such a dynamic and evolving industry. Breuning also highlighted several different aspects to the transparency issue including: enforcement (to ensure the FTC knows what companies are doing);[53] informing consumers (to ensure the public knows what companies are doing);[54] and internal housekeeping (allowing companies to identify the role they play and how to best serve their customers). Finally, Breuning

N.Y. Times (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/77A5-UN39].

48 Paula Breunig, http://www.sequeltechlaw.com/?team=paula-bruening (last visited Apr. 6, 2019) [https:/perma.cc/ZHX2-Z3ME].

49 Liz Woolery, https://cdt.org/about/staff/liz-woolery/ (last visited Apr. 6, 2019) [https://perma.cc/Y2CF-2K5J].

50 Maya Uppaluru, https://www.crowell.com/Professionals/Maya-Uppaluru (last visited Apr. 6, 2019) [https://perma.cc/QF2S-6GQR].

51 Wendy Seltzer, https://www.w3.org/People/Seltzer/ (last visited May 28, 2019) [https://perma.cc/3U9J-2EQE].

52 Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 926 (2009); *see also* Natalie Kim, *Note, Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 HARV. J.L. & TECH. 325, 335-38 (2014).

53 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the Common Law of Privacy*, 114 COLUM. L. REV. 583, 598 (2014); *but see* Kim, *supra* note 52, at 339 (arguing the FTC lacks legal legitimacy to enforce its rulings while simultaneously overreaching the power entrusted to it by Congress).

54 *See* Kim, *supra* note 52, at 341.

emphasized that efforts to promote transparency cannot be abandoned.

Liz Woolery argued that increasing transparency should be achieved on the corporate side, as opposed to placing the burden on the consumer. She stressed the importance of user-designed controls. By manipulating such controls, companies can take more interesting approaches, in both format and language, to make their notices more accessible.[55] Woolery proposed sending updated privacy policies directly to consumers via email. She would also like to see companies make the red-line versions of previous policies available to the public so consumers can see the updates and changes for themselves. Woolery further argued that an ongoing major obstacle is incentivizing these companies to embrace transparency. She pointed to shareholders as the most influential avenue through which to change these practices.[56] However, while this might be the most pragmatic option, Woolery also advocated for the role and necessity of civil societies. She claimed that speaking to and working with policymakers and journalists will help change everyday habits. In addition, she contended that transparent reporting can help or hurt a company's public relations.[57] Finally, Woolery contended that the biggest hurdle is communicating the significance of privacy to the public. However, she averred that the increase in transparency reporting is a positive step, with companies such as Google and Twitter disclosing their policies about user privacy, security, and access to information.[58]

---

55 *Id.*

56 Carol Hansell et al., *The American College of Governance Counsel: Charting the Course to an Improved Model of Corporate Governance*, 41 DEL. J. CORP. L. 509, 520 (2017).

57 Woolery cited the mobile application Snapchat as an example. In 2015, rumors circulated that Snapchat's updated terms entitled the application to ownership of its users' content. *See* James Temperton, *Snapchat Doesn't Own Your Photos, Videos and Messages*, Wired (Nov. 2, 2015), https://www.wired.co.uk/article/snapchat-doesnt-own-your-pictures [https://perma.cc/GVT3-F8PA]. While this was not true, nor the company's intention when they issued their new policies, the poor communication backfired and led to negative PR.

58 Google Transparency Report, https://transparencyreport.google.com/?hl=en (last visited Oct. 4, 2018) [https://perma.cc/73HX-9TNE]. *See also* Twitter Transparency

Maya Uppaluru also stressed the need for companies to focus more on creating a user-friendly experience for privacy policies. She reasoned that companies already know how to create an engaging online user-experience; now they need to apply those tactics to their privacy policies. She contended that placing the onus on the consumer to parse through these inaccessible notices creates a full-time job. Instead, her solution would be to use reliable middle-men in the form of fiduciaries and "data stewards" who can better communicate with consumers. Additionally, Uppaluru dove deeper into current crossover issues between technology and the healthcare industry, focusing particularly on the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which protects individual's health information.[59] However, companies like FitBit currently operate outside the scope of HIPAA,[60] yet are in the business of collecting health and other sensitive data. Uppaluru argued that these companies should similarly be subject to some level of transparency, especially since there is currently a push towards people being able to access their own information. However, Uppaluru noted that once consumers authorize an application on their mobile device to access their information, "all bets are off." This concession raised the question of accountability: Is the consumer liable? Does Apple as owner and operator of the App Store selling the FitBit app to consumers have a role? Or are the entities covered under HIPAA still involved because the information originated with them? By highlighting these difficult questions, Uppaluru emphasized the tension between creating a better user experience and using data and data stewardship responsibly. User-centered design, or what she called "human-centered design," is expanding. She urged companies to prioritize creating the best user experience possible.

Report, https://transparency.twitter.com/en.html (last visited Oct. 4, 2018) [https://perma.cc/5JTH-ALJ9].

59 *Health Info. Privacy*, HHS.gov, https://www.hhs.gov/hipaa/index.html (last visited Oct. 5, 2018) [https://perma.cc/H7B4-5AWP].

60 Pamela Greenstone, *HIPAA Guidelines Should Evolve with Wearable Technology*, HILL (Mar. 14, 2018), https://thehill.com/opinion/healthcare/378450-hipaa-guidelines-should-evolve-with-wearable-technology [https://perma.cc/LM8V-JJDK] (discussing how FitBit's purchase of Twine Health, a HIPAA-compliant company, should expand FitBit and similar companies' responsibility in dealing with personal health data).

Wendy Seltzer's segment also advocated for increased transparency to consumers, stressing the inalienability of individuals' rights. Selzter noted that privacy policies are difficult to understand: per a study conducted in 2008, it would take the average user roughly forty minutes a day to understand the policies of each of the websites they interact with. The cost to the United States' economy of doing so would have been $781 billion.[61] Selzter emphasized that users do not have a real choice because the only choice is binary[62]: users can either "live like a hermit" or disclose their personal information. Furthermore, even if the websites are transparent with the content of their privacy policies, there is very little information as to what the company plans to do with any collected data in the future.[63] For example, Target was able to, as its namesake suggests, target individuals with advertisements for pregnancy and baby merchandise before family members even knew the individual was pregnant.[64] While helpful in this particular kind of situation, Seltzer argued that the regulation needed to compel companies to disclose other potential uses of personal data is sorely lacking.

Seltzer reiterated that in the context of privacy policies and data distribution, the "autonomy of individuals" should be "inalienable." Within this prerogative, Seltzer argued that in addition to giving meaningful notice, companies need to mirror the information being collected about consumers back to them. She supported the presence of informational fiduciary figures to maintain that autonomy, stating that those collecting the data should be subject to rules about its use and should be forced to consider the consumers' needs. However, she posited that anyone

---

61 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S J. L. & POL'Y 544, 563-64 (2008); *see also* Michael Kassner, *Reading Online Privacy Policies Cost Us $781 Billion Per Year*, TechRepublic (May 21, 2012, 12:12 AM), https://www.techrepublic.com/blog/it-security/reading-online-privacy-policies-cost-us-781-billion-per-year/ [https://perma.cc/FU68-E6WY].

62 *See* Gilman & Green, *supra* note 47, at 293.

63 *Id.*

64 Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, Forbes (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4761b4546668 [https://perma.cc/9UAV-6GFH].

who is collecting and using consumer data is assuming some fiduciary duty, or at least should be. She asserted that all parties functioning as data processors are in the pool of potentially liable entities and any party not already subject to transparency requirements should be.

Selzter also cautioned that the consuming public is not considering the long-term consequences of companies compiling years of information. To combat this, consumers need to act collectively, value autonomy, and develop and express their opinions. She issued a plea to avoid "privacy nihilism." She urges consumers to defend privacy and autonomy, saying "our humanity and democracy depend on it."

The panel's full conversation can be found on the *Fordham Intellectual Property, Media & Entertainment Law Journal's* website here: http://www.fordhamiplj.org/2019/02/05/episode-57-transparency-of-notice-and-choice-26th-annual-iplj-symposium/.