THE YALE LAW JOURNAL FORUM

APRIL 1, 2019

Data Rights and Data Wrongs: Civil Litigation and the New Privacy Norms

Joseph V. DeMarco & Brian A. Fox

ABSTRACT. Significant media and scholarly discussion has focused on the civil liberties implications of government access to electronically stored personal data held by third-parties. This essay, however, argues that that civil litigation between private parties in the data privacy and security space is also shaping important cybersecurity and privacy norms. Because no comprehensive data privacy law exists in the United States, litigants in these disputes must rely on conventional civil legal doctrines that are ill-suited to the legal questions raised by the rise of the mass collection of personal data. As a result, it is unclear how courts will resolve emerging questions and we believe that the law will develop in an uneven and unpredictable ways.

INTRODUCTION

In recent years, significant media and scholarly attention has focused on the emerging legal questions surrounding government access to private data held by, or accessible to, third parties. Two of the most prominent examples were the Department of Justice's attempts in 2016 to force Apple to decrypt an iPhone belonging to the perpetrator of the December 2015 mass shooting in San Bernardino, California,[1] and in 2018 to compel Facebook to decode the encryption in

1. *See, e.g.*, Eric Lichtblau & Katie Benner, *Apple and U.S. Bitterly Turn Up Volume in iPhone Privacy Fight*, N.Y. TIMES (Mar. 11, 2016), https://www.nytimes.com/2016/03/11/technology/apple-iphone-fight-justice-department.html [https://perma.cc/L7TY-8NPD]; *cf.* Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599 (2016) (discussing law enforcement's desire for exceptional access to technological data); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99 (2018) (exploring how companies act as "surveillance intermediaries" to constrain law enforcement surveillance efforts).

its Messenger application.[2] Last year, the Supreme Court adjudicated whether a warrant based on probable cause was required to access cell-site records created and maintained by third-party wireless service providers.[3] The popular press has also reported on the legal debate surrounding what access the government should have to facial recognition technologies and databases run by providers such as Amazon, Microsoft, and Google, among others. Yet although constitutional and civil-liberties scholars and the media have extensively examined these issues in the criminal context, few have paid attention to the many and varied ways that civil litigation between private parties in the data privacy and security space is shaping important cybersecurity and privacy norms.

This phenomenon is occurring for several reasons. To begin with, data collection and analytics are increasingly vital to operating a business—and are becoming integral to the way businesses deliver products and services to their customers. For their part, consumers, too, are also using more devices and programs that produce data—data that is regularly stored and can be analyzed for a range of purposes.[4] As the market grows for devices and services that collect data and the amount of data amassed by companies increases exponentially—and is shared, sold, or stored with third parties—courts and lawyers alike should expect civil litigants to seek access to this data during the normal course of discovery. In addition to geolocation data, which might be relevant in a wide variety of civil contexts, it is almost inevitable that data collected by wearable fitness technology, appliances, drones, or automated vehicles will become the type of information that is routinely sought in civil ligation. Relatedly, as we will see below, fundamental questions about what data companies can collect about individuals, what they can do with it, and the circumstances under which it can be disclosed to third parties, will be shaped to a great extent through civil litigation.

This Essay discusses some of the potential ways that these new legal questions will arise in civil litigation and the potential effects they will have on cybersecurity and privacy norms—norms which will, for better or worse, confront courts and litigants in criminal and civil liberties cases. First, we briefly analyze how data incidents involving businesses may shape the development of privacy norms in the private sector. Second, we explore how, in the absence of a comprehensive data privacy regulation, legal norms surrounding the collection, analysis, and sale of personal information will be formed in civil litigation using existing

2. *See, e.g.*, Kevin Kelleher, *DOJ Reportedly Asks Facebook to Break Encryption to Tap into Messenger Calls*, FORTUNE (Aug. 17, 2018), http://fortune.com/2018/08/17/doj-facebook-break-encryption-tap-messenger-calls [https://perma.cc/MJS9-CUVT].

3. Carpenter v. United States, 138 S. Ct. 2206 (2018).

4. According to a recent Pew survey, 95% of Americans own a cell phone, and 77% of those are smartphones—up from 35% in 2011. *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile [https://perma.cc/FY9Y-25KQ].

laws—laws that are ill-suited to the emerging complexity of data privacy disputes.

I. BUSINESS-TO-BUSINESS LITIGATION AND OUR DATA

As readers of law journals and the popular press are well aware, data breaches have become a regular source of reputational and legal risk for companies. High-profile breaches such as the 2017 Equifax breach—which exposed the social security numbers, birthdates, and addresses of 145.5 million people[5]—garner significant media attention. Yet while there are state laws, discussed in the next section, that articulate a company's notification obligations to individual consumers, at least to date, there are no comparable state or federal laws that define the legal obligations that apply to businesses that share information with each other, whether involving the personal information of individuals or confidential business information. In the absence of any governing legislation, companies typically manage risks associated with data sharing among themselves through pre-contract due diligence or through various contractual provisions that define data security obligations and procedures.[6] Perhaps not surprisingly, the increase in data sharing inevitably means that more disputes will wind up in litigation when data mishaps occur as between two businesses.

A few recent examples highlight the core questions at issue in business-to-business litigation over data-security. In 2017, Aetna settled a lawsuit for $17 million after 12,000 insurance members received an envelope that, through a clear plastic window, revealed the member's HIV status,[7] a violation of the privacy provisions of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as various state privacy laws.[8] The mailings in question involved a third-party company who arranged and actually mailed the envelopes

5. Stacy Cowley, *2.5 Million More People Potentially Exposed in Equifax Breach*, N.Y. TIMES (Oct. 2, 2017), https://www.nytimes.com/2017/10/02/business/equifax-breach.html [https://perma.cc/TAY5-PT8R].

6. Joseph V. DeMarco & Urvashi Sen, *Strategies for Navigating Business-to-Business Data Breaches*, N.Y.L.J. (July 6, 2015, 1:00 AM), https://www.law.com/newyorklawjournal/almID/1202731233079/strategies-for-navigating-businesstobusiness-data-breaches [https://perma.cc/L74L-2PCT].

7. Elana Gordon, *Aetna Agrees to Pay $17 Million in HIV Privacy Breach*, NPR (Jan. 17, 2018, 5:15 PM ET), https://www.npr.org/sections/health-shots/2018/01/17/572312972/aetna-agrees-to-pay-17-million-in-hiv-privacy-breach [https://perma.cc/YS2Y-FJTY].

8. *See* Assurance of Discontinuance at 3-4, *In re* Investigation by Eric T. Schneiderman of Aetna Inc., No. 18-001 (Jan. 19, 2018), https://ag.ny.gov/sites/default/files/aetna_aod_0.pdf [https://perma.cc/B4PG-AR2L] (settling claims against Aetna and admitting that the incident constituted a HIPAA privacy violation).

and a plaintiffs' attorney.[9] After the $17 million dollar settlement, Aetna sued the third party, seeking indemnity, contribution, reimbursement, and damages for their purported negligence.[10] The mailing company then filed an action against Aetna, arguing that Aetna, as a large and sophisticated insurance company, was responsible for ensuring the mailing complied with applicable state and federal law.[11] Among other things, they accused Aetna of transmitting to them far more personal information than was required to complete the mailing.[12,13]

Business-to-business litigation often directly follows a business-to-consumer data breach. For example, breaches involving credit card, debit card, and banking information are burdensome on financial institutions who must deal with a wave of fraud claims, questions from consumers, and the possibility of losing customers. In the summer of 2018, JPMorgan Chase and its payment processing arm, Paymentech, sued Houston-area hospitality chain Landry's over a 2015 data breach involving credit card information.[14] The breach was caused by a program that was installed on payment devices at Landry's restaurants that read the information on the magnetic stripe of the card reader, which included cardholder name, card number, expiration date, and CVV number.[15] A similar breach happened to Wendy's in 2015 when malware infected a small portion of its point-of-sale systems and permitted the use of compromised third-party vendor credentials. In that case, issuing banks sued Wendy's for the costs they incurred in compensating cardholders for fraudulent charges made on the compromised cards and for the cost of re-issuing new cards.[16]

Although on the surface these lawsuits involved traditional negligence and contract questions, at their heart they present two critical and fundamental

9. *See* First Amended Complaint at 3, KCC Class Action Servs., LLC v. Aetna Inc. (W.D. Cal. Feb. 27, 2018) (No 2:18-cv-01018-JFW-JEM).

10. Complaint at 13-14, Aetna, Inc. v. Kurtzman Carson Consultants, LLC (E.D. Pa. Feb. 5, 2018) (No. 2:18-cv-00470-JS).

11. *See* First Amended Complaint at 7, *KCC Class Action Servs*. (W.D. Cal. Feb. 27, 2018) (No 2:18-cv-01018-JFW-JEM).

12. *Id.* at 12-15.

13. Aetna also sued the attorneys who represented the plaintiffs involved in the underlying class action resulting in the mailing, alleging that they were responsible for hiring the third-party mailing company and were responsible for approving the mailing. Complaint at 4-6, Aetna, Inc. v. Whatley Kallas, LLP (Cal. Super. Ct. May 23, 2018) (No. BC707386). Aetna also alleged that the private medical information that the third-party mailing company received was sent by Aetna at the demand of the plaintiffs' attorneys. *Id.* at 5.

14. Complaint, Paymentech, LLC v. Landry's Inc. (S.D. Tex. May 17, 2018) (No. 4:18-cv-01622).

15. *Id*. at 5-6.

16. *See The Wendy's Company Reports Strong First-Quarter 2016 Results*, WENDY'S (May 11, 2016), http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle_pf&ID=2167361 [https://perma.cc/R5S2-TDHA].

issues. First, who is responsible for data breaches where information travels between two commercial parties? Second, what security standards will be expected between companies that process sensitive information, especially if that information is protected by a federal privacy statute? In a nutshell, what are—and should be—the norms about securing data, and the penalties if those expectations are not fulfilled? As more companies process or store information in the cloud, we are likely to see more cases involving unauthorized access to sensitive personal information and valuable corporate information. These cases will—for better or for worse—build a body of case law that answers the questions posed above and which constitute data privacy norms for information shared between businesses. And, in so doing, these norms will create the "atmosphere" of an ecosystem that also informs how attorneys and courts frame arguments and decisions concerning how data is handled, shared, secured, and analyzed in criminal and civil rights litigation.

II. THE WILD WEST OF DATA COLLECTION

The amount of data we produce each day is staggering. By 2025, the proliferation of data-producing devices and services means that each person with an internet-connected device will have at least one data interaction—sending or receiving from a continually expanding universe of such devices every 18 seconds, or almost 5000 per day.[17] Reports of Cambridge Analytica's mass collection of Facebook user data[18] have raised the public's awareness of some of the potential policy issues raised by the rise of big data. As demonstrated by that episode, even if the average person knows that companies or their cell phone carriers are collecting immense amounts of data about their lives, many may not know where that data winds up.[19] They are often outraged when they find out.

17. David Reinsel et al., *The Digitization of the World – From Edge to Core*, SEAGATE 5 (Nov. 2018), https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf [https://perma.cc/NWU4-HLHB].

18. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/X9NC-3PTT?type=image].

19. *See Americans Conflicted About Sharing Personal Information with Companies*, PEW RES. CTR. (December 30, 2015), http://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies/ [https://perma.cc/4RCM-RJ96] ("A significant minority of American adults have felt confused, discouraged or impatient when trying to make decisions about sharing their personal information with companies. When asked if they felt confident they understood what would be done with their personal information as they were deciding whether or not to share it, 50% said they felt confident they understood – but 47% said they were not confident.").

Even so, at present, data privacy in the United States is governed by patchwork of federal and state laws that typically only concern certain classes of sensitive data or cover certain entities. This leaves a vacuum in which important privacy concerns are left unaddressed by law.

Many cell-phone owners may know, for example, that their carriers are collecting geolocation data from their phone. What they may not know is that their carrier also may sell that real-time location data to third parties. According to recent reporting, geolocation data from AT&T, Sprint, and T-Mobile phones were accessed by 250 bounty hunters and related businesses through a company called CerCareOne.[20] Although some of the largest carriers have recently decided to end the practice in light of this reporting,[21] their decision to do so does not answer the fundamental question of the limits of permissible use and the consent required from the person from whom the data is collected.

The rise of automobile-tracking technologies presents another challenge. Electronic toll-collection systems like EZ-Pass have long been subject to criminal and civil subpoenas to obtain evidence of a vehicle's given location at a particular time.[22] Over the past few years, New York has implemented a cashless toll system that ensures that a record is created of every car that passes through a toll. Operated by the same contractor that administers EZ-Pass, the New York system takes a photo of a driver's license plate and sends that information to the relevant government entity, which then sends a bill to the address registered with the vehicle.[23] But private companies gather this information as well. A Texas-based company, Digital Recognition Network (DRN), has taken 6.5 *billion* photographs of license plates that it then geotags, stores, packages, and sells to automotive lenders, insurance companies, and vehicle-recovery professionals.[24] Of significance to civil liberties advocates, DRN also partners with a company called

---

20. Joseph Cox, *Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years*, VICE: MOTHERBOARD (Feb. 6, 2019), https://motherboard.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years [https://perma.cc/NB87-X22C].

21. Mallory Locklear, *Sprint Is the Latest Carrier to Stop Selling Location Data*, ENGADGET (Jan. 16, 2019), https://www.engadget.com/2019/01/16/sprint-stops-selling-location-data [https://perma.cc/5476-W2PF] (noting that Sprint, Verizon, and AT&T announced they will stop selling location data to third parties).

22. *See, e.g.*, Chris Newmarker, *E-ZPass Records Out Cheaters in Divorce Court*, NBC NEWS (Aug. 10, 2007), http://www.nbcnews.com/id/20216302/ns/technology_and_science-tech_and_gadgets/t/e-zpass-records-out-cheaters-divorce-court [https://perma.cc/M7E5-CC8P].

23. Frank Esposito, *Cashless Tolls: Welcome to the Dark Future*, LOHUD (Apr. 11, 2018), https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002/ [https://perma.cc/M87P-FHLN].

24. *See* DIGITAL RECOGNITION NETWORK, https://drndata.com [https://perma.cc/X5Y5-X8SS].

Vigilant Solutions that provides data and image analytics for vehicle location to law enforcement, who can use the location data—notably, without the high stands of proof and procedural protections of a warrant.[25]

As is characteristic of other privacy laws, the response of legislators to the intrusiveness of these technologies has largely been reactive and piecemeal. Sixteen states have enacted statutes limiting the use of license plate readers to law enforcement and related entities and requiring that the records be destroyed after a certain period of time.[26] Although there is a federal statute that governs the disclosure of personal information gathered by state motor vehicle departments, it was passed in 1994, long before lawmakers contemplated these companies.[27] Not surprisingly, many pre-internet, decades-old laws simply did not account for the way data is generated, collected, and used today.

Other countries have taken steps to address existing gaps in data-privacy laws. For instance, under the European Union's General Data Protection Regulation (GDPR), an entity is only able to collect personal information[28] about a "data subject" if it has a legal basis to do so, for example by obtaining the data

---

25. *See FAQs*, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/about/faqs [https://perma.cc/3KK4-XE5K]. The company's own FAQs unintentionally highlight how current laws have not caught up to this type of data collection: "License plate reader data, by itself, is completely anonymous; an LPR detection consists of a color image of the vehicle, an infrared image of the license plate, the license plate read as interpreted by the system, a time and date stamp, GPS coordinates of the vehicle making the license plate capture, as well as information on the operator of the LPR system and the camera making the capture. There is no personally identifiable information contained in a license plate capture." *Id.*

26. ARK. CODE ANN. §§ 12-12-1801-1808 (2018); CAL. CIV. CODE §§ 1798.29 & 1798.90.5 (West 2018); COLO. REV. STAT. § 24-72-113 (2018); FLA. STAT. § 316.0777 (2018); GA. CODE ANN. § 35-1-22 (2018); ME. STAT. tit. 29-A § 2117-A (2017); MD. CODE ANN., PUB. SAFETY § 3-509 (West 2018); MINN. STAT. §§ 13.82, 13.824 & 626.8472 (2018); MONT. CODE ANN. §§ 46-5-117-119 (2017); NEB. REV. STAT. § 60-3201-3209 (2018); N.H. REV. STAT. ANN. §§ 261.75-b & 236.130 (2018); N.C. GEN. STAT. §§ 20-183.30-32 (2018); OKLA. STAT. tit. 47, §§ 47-4-606.1 (2018); TENN. CODE ANN. § 55-10-302 (2018); UTAH CODE ANN. §§ 41-6a-2001-2005 (West 2018); VT. STAT. ANN. tit. 23, §§ 1607 & 1608 (2018).

27. The Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2018).

28. The definition of "personal information" is broad. It means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." 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), 2016 O.J. (L 119) 1, art. 4.

subject's consent.[29] The regulation also contains provisions governing how data is processed, stored, and transferred and gives data subjects the right to request information about what data is collected and how it is used, to correct information, and even to request the deletion of the data.[30] The GDPR may be enforced with administrative sanctions or through a private right of action.[31]

The United States has no national privacy law like the GDPR. As a general matter, data privacy in the United States is governed by a series of federal and state laws that only cover certain classes of sensitive data or certain entities.[32] The Federal Trade Commission (FTC) has used its authority under section 5 of the Federal Trade Commission Act[33] to expand its focus on privacy issues over the past decade and, acting under that authority, has issued nonbinding guidance on online behavioral advertising.[34] In addition to section 5 of the FTC Act, some prominent federal privacy laws include the Health Insurance Portability and Accountability Act[35] and related regulations,[36] which govern private medical information; the Fair Credit Reporting Act,[37] which regulates consumer credit information; and the Financial Services Modernization Act,[38] which governs certain banks and financial institutions with respect to the collection and use of financial information. There are also federal laws that protect the privacy of written

---

29. *Id.* at art. 6.

30. *See A New Era for Data Protection in the EU: What Changes After May 2018*, EUR. COMMISSION, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf [https://perma.cc/2AFM-SRA3].

31. *See* General Data Protection Regulation, 2016 O.J. (L 119) 1.

32. For an illustrative exploration of data-privacy laws in the United States, see Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/UXT6-Q8NM].

33. 15 U.S.C. § 45 (2018).

34. *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, FED. TRADE COMMISSION (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [https://perma.cc/WVX3-W7QW].

35. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

36. 45 C.F.R. § 160.101-534 (2000).

37. 15 U.S.C. § 1681 (2018).

38. Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

electronic communications,[39] student education records,[40] and personal information collected online from a child under thirteen years of age.[41] While these federal laws provide some protections, they fail to provide the comprehensive privacy protections of the GDPR.

At the state level, all fifty states and the District of Columbia[42] have statutes that require consumer and regulator notification in the event of a data breach involving personally identifiable information, but the various provisions in these statutes vary from state to state in terms of what information is covered[43] and under what circumstances notification is required.[44] In addition, these statutes only govern a company's obligations to make certain notifications *after* a breach of information has occurred rather than the collection, storage, and transfer of data. And, like the federal statutes, they generally only apply to certain narrow classes of sensitive private information, such as Social Security numbers and bank-account and credit-card information. Apart from the California Consumer Privacy Act discussed below, which does not take effect until 2020 and may be significantly revised before then, there is no federal or state statute to specifically address the enormous amount of varied consumer data that modern companies collect.

---

39. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2019); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

40. Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2018); 34 C.F.R. § 99.1-67 (2018).

41. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§§ 6501-6505 (2018).

42. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sep. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/EU9L-UT3E] (listing statutes for each state, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands).

43. *Compare* KY. REV. STAT. ANN. § 365.732 (West 2018) (providing protections for private information including first name or first initial and last name, plus (1) Social Security number; (2) driver's license number; or (3) account, credit card, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account), *and* N.C. GEN. STATE § 75-66(c) (2018) (covering the same plus other types of personal information such as biometric data and digital signatures), *with* TEX. BUS. & COM. CODE ANN § 521.002 (West 2018) (including, in addition to other personal data, information regarding a resident's physical or mental health or the provision of or payment for health care to the resident).

44. *Compare* WASH. REV. CODE § 19.255.010(1) (2018) ("Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm."), *with* N.Y. GEN. BUS. LAW § 899-a (McKinney 2018) (requiring notification regardless of the likelihood of harm).

Because there is no comprehensive framework governing data ownership and use, the scope of a data collector's ability to collect and sell personal data in the United States is—and will continue to be—litigated using legal theories advanced to, and ultimately decided by, civil judges and juries. Examples of this phenomenon are not hard to find. For example, in a recent civil suit filed by the City of Los Angeles, the City alleged that the company that operates the Weather Channel app[45] deceived consumers, under the pretext of providing weather information, into permitting the application to collect a massive amount of geolocation data that the company then shared with its parent company, IBM, and various third parties.[46] The complaint alleges that the company has referred to itself as "a location data company powered by weather" capable of collecting more than one billion pieces of geolocation data per week.[47] The information collected from the data powers IBM's "audience-derived location targeting platform" JOURNEYfx.[48] According to IBM's own website, JOURNEYfx "uses one of the world's largest continuous streams of first party location data—The Weather Channel—to find and reach relevant audiences. It leverages people's real-world behaviors over time to shed light on their wants, needs, preferences, consumption habits, and anticipated future activities."[49]

Because there are no rules governing the company's collection of data and the manner in which any disclosures should be made to consumers, the suit was brought under California's Unfair Competition Law[50] based on the theory that the data collection constitutes "unlawful, unfair or fraudulent business act or practice."[51] Specifically, the court will need to determine whether the City's allegations that the disclosures in the privacy policy, which were only accessible after

---

45. The company that owns the Weather Channel application, TWC Product and Technology, LLC, and the Weather Channel television network are separate corporate entities that do not share the same parent company. *See IBM Closes Deal to Acquire the Weather Company's Product and Technology Businesses*, WEATHER COMPANY (Jan. 29, 2016), https://business.weather.com/news/ibm-closes-deal-to-acquire-the-weather-companys-product-and-technology-businesses [https://perma.cc/WS62-LDVH].

46. Complaint at 1, California v. TWC Prod. & Tech., LLC, No. 19STCV00605 (Cal. Sup. Ct. Jan. 3, 2019).

47. *Id.* at 11-12 (quoting Michelle Manafy, *The Weather Company's JOURNEYfx Location-Based Ads See the Bigger Picture*, DIGITAL CONTENT NEXT (Oct. 18, 2016), https://digitalcontentnext.org/blog/2016/10/18/the-weather-companys-journeyfx-location-based-ads-see-the-bigger-picture/ [https://perma.cc/F58B-MJ2R]).

48. *Data Solutions*, IBM, https://www.ibm.com/watson-advertising/solutions/data [https://perma.cc/LB8B-R252].

49. *Id.*

50. *See* CAL. BUS. & PROF. CODE § 17200 (West 2018).

51. Complaint at 13, California v. TWC Prod. & Tech., LLC (Cal. Sup. Ct. Jan. 3, 2019).

the app was installed and the user was prompted to turn on location services, did not sufficiently describe the purpose for which the data was collected, and whether that conduct meets the definition of an unfair or fraudulent business practice or deceptive advertising.[52] Rather than tailor the inquiry to the unique context of data collection, the court will almost certainly be applying the same language as it has in cases involving, for example, the terms of residential mortgages[53] and the health claims of breakfast-food manufacturers.[54] Even if this case produces a clear precedent in California for how disclosures should be made, state unfair and deceptive trade practices laws vary widely in terms of prohibited conduct, available remedies, and whether private rights of action or class actions are available.[55] With dozens of separate state statutes and bodies of caselaw, it is easy to imagine a confusing mess of contradictory rules emerging. While traditional federalism arguments concerning the benefits of state innovation and varying approaches may seem appealing, the pace of those developments will simply not match the pace of technical innovation and emerging legal issues that results from that change.

In 2018, the California legislature may have shown a potential way forward when it passed the California Consumer Privacy Act (CCPA).[56] The statute, which goes into force in 2020, requires companies subject to the Act to inform consumers that the company is collecting information, allow consumers to opt out of the sale of their personal information, provide consumers—at their request—information about how their data is used, and delete a consumer's information when asked to do so.[57] Critically, it provides an expansive definition of personal data that reflects what companies are actually collecting.[58] The CCPA

52. *Id.* at 9-10.

53. Khan v. CitiMortgage, Inc., 975 F. Supp. 2d 1127, 1144 (E.D. Cal. 2013).

54. Hadley v. Kellogg Sales Co., 273 F. Supp. 3d 1052, 1063 (N.D. Cal. 2017).

55. *See generally* Carolyn Carter, *Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws*, NAT'L CONSUMER L. CTR. (Mar. 2018), http://www.nclc.org/images/pdf/udap/udap-report.pdf [https://perma.cc/SS2P-MH3N] (summarizing the ways that these statutes vary from state to state).

56. CAL. CIV. CODE §§ 1798.100-1798.199 (West 2018).

57. 2018 Cal. Legis. Serv. ch. 55 (West); CAL. CIV. CODE § 1798.120 (West 2018) (right to opt out); CAL. CIV. CODE § 1798.110 (West 2018) (right to request information); CAL. CIV. CODE § 1798.105 (West 2018) (right to deletion).

58. "Personal information" means "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This includes, but is not limited to names, IP addresses, e-mail addresses, online identifiers, purchasing histories, biometric information, internet network activity, geolocation data, employment information, and other types of data. CAL. CIV. CODE § 1798.140(o) (West 2018).

could potentially serve as a model law for other states,[59] or perhaps even a federal law, but given the current political climate and industry opposition, it is unlikely that will happen in the near future. Over fifteen years elapsed between the passage of the first data breach notification law in California in 2002[60] and the passage of Alabama's,[61] the last state to do so, and there is still no federal law. It will be impossible to know how the CCPA will affect covered companies' compliance decisions until after the statute takes effect, but the demand for consumer information is expected to grow significantly over the next decade as businesses become more data-driven.[62] Lawyers interested in privacy rights would do well, therefore, to expect this gap in consumer protection to persist.

For privacy advocates, the stakes of the regulatory void in which these data collectors operate to collect vast quantities of data are far higher than, for example, directing personalized advertisements and discounts for fast food restaurants based on geolocation information—a project that JOURNEYfx advertises.[63] If recent news reports are accurate, the third-party data merchants who purchased geolocation data from cell phone carriers subsequently, and inappropriately, sold real-time location information to bounty hunters, bail bondsman,[64] and in one case, a law enforcement officer who tracked phones without a warrant.[65] It is with these private sector actors that process increasingly immense amounts of data that many of the most pressing future privacy questions arise. Aside from the legislative process (which is often hampered by gridlock) and criminal litigation (which infrequently raises these issues due to the relative paucity of criminal cases as compared to civil filings), the only way for concerned

---

59. One limitation of the CCPA is that, unlike the GDPR, which expressly governs how and when a data collector may collect a consumer's information, General Data Protection Regulation, 2016 O.J. (L 119) 1, Art. 6 , the CCPA only limits a for-profit company's ability to *sell* a California resident's information if he or she affirmatively opts out, CAL. CIV. CODE § 1798.120 (West 2018).

60. CAL. CIV. CODE § 1798.82 (West 2018).

61. S.B. 318, Alabama Data Breach Notification Act, Reg. Sess. (Ala. 2018).

62. *See* Louis Columbus, *10 Charts That Will Change Your Perspective of Big Data's Growth*, FORBES (May 23, 2018, 7:02 AM) https://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/#5c32798e2926 [https://perma.cc/6WV9-S264] (describing a projection that the global demand for big data" software and services will more than triple over the next ten years).

63. *See McDonald's Leverages IBM Watson Advertising's JOURNEYfx and IBM Predictive Audiences to Drive In-Store Visits*, IBM, https://www.ibm.com/case-studies/mcdonalds-watson-advertising [https://perma.cc/X6NW-PWFX].

64. Cox, *supra* note 20.

65. Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. TIMES (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html [https://perma.cc/SP7K-M582].

individuals to object to the mass collection of data is through ligation using conventional civil law doctrines.

CONCLUSION

As we produce more data that companies can farm for value or lose, questions surrounding data ownership and responsibility for liability following a data mishap will continue to become more pressing. When has an individual consented to the type of data that a company is collecting? What type of data can they share with third parties and under what circumstances? What recourse will an individual have it their data falls into unauthorized hands or the government? These questions increasingly touch on fundamental notions of privacy. Yet barring significant and comprehensive federal data legislation in the United States, these questions will be principally answered in the context of civil lawsuits—often in lawsuits between businesses. And precisely because the outcomes of these lawsuits will shape norms and laws concerning privacy and security in years to come, litigators would be well-served by closely following these civil cases.

Joseph V. DeMarco is the founding partner of DeVore & DeMarco LLP, a boutique law firm that specializes in the law of data privacy and security and cybercrime prevention and response. From 1997-2007, he served as an Assistant United States Attorney for the Southern District of New York where he led cybercrime investigations and prosecutions. Brian A. Fox is an associate attorney at DeVore & DeMarco LLP.