RIDE OVERSHARING: PRIVACY REGULATION WITHIN THE GIG ECONOMY

INTRODUCTION

In January of 2016, Uber reached a settlement with New York Attorney General Eric Schneiderman after an investigation of its internal "God View" tool, which allows Uber executives to access riders' locations.[1] The investigation stemmed from several reports of inappropriate geotracking, including one from Johana Bhuiyan, a

[1] *See* Press Release, New York State Office of the Attorney General, A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy (Jan. 6, 2016) (on file with author).

Buzzfeed reporter who was greeted at Uber New York headquarters with this comment from a General Manager: "There you are. I was tracking you."[2] God View was viewed as troublesome in the hands of Uber, a private ridesharing company which tracks geolocation even after a user exits the app; the settlement, therefore, requires Uber to use its information for business purposes only.[3]

Digital firms, such as Uber, that facilitate transactions between independent service providers and their consumers over Internet-based platforms collectively compose the "gig economy."[4] The gig, or "sharing," economy is rapidly expanding; from 2005 to 2015, the percentage of gig workers, including Uber drivers, agency workers, independent contractors, and freelancers, rose from 10.1% to 15.8%.[5] This is especially notable given that there was no meaningful change from 1995 to 2005.[6] While only 0.5% of total workers worked through an online intermediary as of 2015,[7] the online gig workforce is nevertheless growing in a steep upward trajectory—the percentage was 0% as recently as October 2012.[8]

While the settlement with Attorney General Schneiderman requires Uber to limit geolocation tracking information to legitimate business purposes,[9] this current *ex-ante* scheme of self-regulation followed by suits and settlements will prove to be ineffective and costly as the gig economy entrenches itself as a mainstream venue for transportation, housing, and services.[10] Consumers readily share private information with an app, which sends strangers to walk their dogs, rent their homes, and ride in their cars. The online platform collects these users' locations and personal information without meaningful privacy protection at the corporate or regulatory level.[11] Because Uber and other sharing platforms collect user data that can be used to geolocate or

---

[2] *Id.*

[3] *Uber Privacy Statement*, UBER (July 15, 2015), https://www.uber.com/legal; Schneiderman, *supra* note 1.

[4] U.S. Dep't of Commerce, Econ. & Statistics Admin., Office of the Chief Economist, Digital Matching Firms: A New Definition in the "Sharing Economy" Space (June 2, 2016), http://www.esa.gov/reports.

[5] Lawrence F. Katz & Alan B. Kreuger, *The Rise and Nature of Alternative Work Arrangements in the United States, 1995–2015* (Nat'l Bureau of Econ. Research, Working Paper No. 22667, 2016).

[6] *Id.*

[7] *Id.*

[8] *See* J.P. MORGAN CHASE & CO. INST., PAYCHECKS, PAYDAYS, AND THE ONLINE PLATFORM ECONOMY: BIG DATA ON INCOME VOLATILITY 21 (2016), https://www.jpmorganchase.com/corporate/institute/document/jpmc-institute-volatility-2-report.pdf.

[9] Schneiderman, *supra* note 1.

[10] Stephen R. Miller, *First Principles for Regulating the Sharing Economy*, 53 HARV. J. ON LEGIS. 147, 149 (2016).

[11] David Lazarus, *Europe and U.S. Have Different Approaches to Protecting Privacy of Personal Data*, LOS ANGELES TIMES (Dec. 22, 2015).

contact passengers, the lack of regulation creates a danger that sharing platforms will use their access to user data to inappropriately track, analyze, and contact users.

This Note argues that the current regulatory scheme for privacy inadequately protects consumers in the gig economy. While privacy is considered a fundamental human right in Europe,[12] American law has neglected the right to privacy. This has become increasingly important as digitization continues into the sharing economy system. This Note proposes that the federal government, through the Federal Trade Commission ("FTC"), establish a regulatory framework that borrows standards from the Federal Communications Commission ("FCC")'s 2016 privacy rules for broadband Internet service providers ("ISPs"),[13] the California Online Privacy Protection Act ("CalOPPA"),[14] and Regulation (EU) 2016/679. This would act as a model scheme for states to implement stronger privacy standards for companies. For example, states could require warrants for governmental access to data. This would, in turn, deter gig economy platforms from intruding upon consumer privacy and keeping data for any purpose except for essential business use. Specifically, Part I of this Note begins by outlining the historical background of privacy law, with emphasis on technological influence on the law. Part II discusses the current state of the sharing economy's self-regulation regarding privacy. Part III delves into issues surrounding governmental access to data and its circumvention of Fourth Amendment protection, and Part IV suggests that the United States federal government supplement the current system with a broad, regulatory framework akin to the recently repealed FCC privacy rules. Lastly, this Note in Part V discusses alternative solutions, including congressional and local regulation.

I. PRIVACY: A HISTORY

A. *The American Approach: Self-Regulation and Segmentation*

Before delving into the respective histories of privacy law in the United States and Europe, it is important to differentiate between "privacy" and "data protection." Privacy refers to the right of *respect* for private life, while data protection refers to the *security* of the individual's personal data.[15] The history of these sectors of law shows

[12] *See Reform of EU data protection rules*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last visited Sept. 30, 2016) [hereinafter *Reform*].

[13] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64 (2016).

[14] California Online Privacy Protection Act of 2003, CAL. BUS. & PROF. §§22575–79 (2004) [hereinafter CalOPPA].

[15] Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, STATEWATCH,

that, while the United States has been on the forefront of data protection, it has neglected to establish a strong privacy law scheme in the post-Internet age.[16] While Europe has developed a strong regulatory presence over the human right to privacy, the United States is scrambling to develop a similar regulatory scheme.[17]

The geneses of privacy common law in the United States occurred in 1890, when the dissemination of the "snap camera"[18] inspired Samuel Warren and Louis Brandeis to write "The Right to Privacy," published in the Harvard Law Review.[19] As technology that allowed instantaneous photography threatened privacy and inspired a prediction that "what is whispered in the closet shall be proclaimed from the house-tops,"[20] Warren and Brandeis inspired a new area of law protecting the "right of the individual to be let alone."[21] Privacy law continued to develop along common law routes until the rise of computers in the 1960s renewed interest in privacy law.[22] By the mid-seventies, Congress passed the Privacy Act of 1974.[23] While the Act regulated privacy issues relating to federal agencies and the individual right to access and change personal information, it did not apply to the private sector.[24] The principal federal standard for private sector privacy law, Section 5 of the FTC Act, generally prohibits "unfair or deceptive acts or practices in or affecting commerce."[25] Since 1998, the FTC has brought actions against companies that violate their own privacy policies.[26] This systematic self-regulation leaves the "protection of privacy to markets rather than law."[27]

While the comprehensive history of U.S. federal privacy law is scarce, state law is a patchwork of individual requirements.[28] The most

http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf (last visited Nov. 30, 2016).

16 See Ryan Moshell, . . . And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection, 37 TEX. TECH L. REV. 357, 374 (2005).

17 *Id.*

18 Daniel J. Solove, *A Brief History of Information Privacy Law* (George Washington Law Sch. Pub. Law Research Paper No. 215, 2016), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

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

20 *Id.* at 2.

21 *Id.* at 6.

22 Solove, *supra* note 18, at 1–24.

23 5 U.S.C. § 552a (2014).

24 *See* Solove, *supra* note 18.

25 15 U.S.C. § 45 (2006).

26 *See* Solove, *supra* note 18, at 1–39.

27 Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 730–31 (2001).

28 See State Laws Related to Internet Privacy, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research (last visited Jan. 25, 2017).

stringent state law, California's CalOPPA,[29] requires certain additions to a company's privacy policy, such as a "delete" button that allows minors to redact information and content they provided to the site.[30] Many online gig economy companies simply choose to comply with California's stringent privacy policy laws in the interest of streamlining resources.[31] Currently, this is a possible strategy, given California's lone status at the forefront of privacy. However, as other states consider the importance of privacy protection, gig economy companies will have to implement tailored guidelines for each state they interact with to comply with the separate regulations.[32]

The United States has declined to create a streamlined regulatory scheme for the private corporate sector, including the online gig economy. Yet Congress has developed comprehensive privacy regulations within niche industries, such as the Health Insurance Portability and Accountability Act (HIPPA)[33] and the Children's Online Privacy Protection Rule (COPPA).[34] The HIPPA privacy rules, for example, establish national standards to protect personal health information and set requirements for use or disclosure of such information.[35] COPPA requires the FTC to issue and enforce the regulation of children's online privacy.[36] Credit information and student educational records are similarly statutorily protected.[37] These statutes do not, however, cover medical or educational data that users input into an online application—e.g. HIPPA does not cover medical information that a FitBit collects.[38]

B. *The European Approach: The Human Right to Private Life*

While the United States struggles to create a patchwork of privacy law focusing on segmented protection of data, the European Union has historically considered privacy to be a fundamental human right and has, therefore, focused its legislative attention on setting standards that protect consumers from businesses that might infringe upon that

[29] CalOPPA, *supra* note 14.
[30] Chrissie N. Scelsi, *Recent Developments in Online Privacy Laws*, 90 FLA. B.J. 72, 74 (2016).
[31] *See id.*; Kirk J. Nahra, *State Privacy Laws and Their HIPAA Implications for Pharmaceutical Manufacturers*, WILEY REIN LLP (Nov. 2002), http://www.wileyrein.com/newsroom-newsletters-item-266.html.
[32] *See* Nahra, *supra* note 31.
[33] 42 U.S.C. § 201 (1996).
[34] 15 U.S.C. § 6501 (1998).
[35] 42 U.S.C. § 1302d-2 (2010).
[36] 15 U.S.C. § 6501.
[37] *See, e.g.*, 15 U.S.C. §1681 (2012) (Credit information is protected by the Fair Credit Reporting Act); 20 U.S.C. §1232g (2012) (The Family Educational Rights and Privacy Act protects student education records).
[38] *See* Rebecca Lipman, *Online Privacy and the Invisible Market for our Data*, 120 PENN ST. L. REV. 777, 788 (2016).

inalienable right.[39] In fact, the origin of European privacy protections came from the European Convention on Human Rights after World War II, which established a right to respect private life.[40] The scope of the protection was expanded through a series of judgments by the European Court of Human Rights, in which the court asked whether there was interference with the right to respect private life and whether that interference was "necessary and proportionate" to the interests at stake.[41]

Throughout the latter half of the twentieth century, the European Commission continued to keep privacy on its legislative agenda. However, as the 1990s approached, it became worried that the lack of consistency across the Member States would impede the development of markets in online corporate areas where personal data would inevitably be collected.[42] In 1995, the EU Data Protection Directive 95/46/EC (the "Directive"), which sought to protect the right to privacy in personal data processing and maintain that same high standard for all Member Counties, was adopted.[43]

In 2009, the EU launched a review of the Directive and planned to modernize its framework for privacy rules, this time focusing on data protection.[44] Consequently, the EU has undergone a comprehensive data protection reform.[45] Regulation (EU) 2016/679, known as the General Data Protection Regulation ("GDPR"), became effective in May of 2016 and will be enforceable by 2018.[46] As a regulation, it will apply directly to all Member States without any requirement for corresponding national legislation.[47] The GDPR repeals the Directive and emphasizes that organizations are responsible for protecting personal privacy and must be proactive in their data management systems.[48] The provisions of the GDPR are further examined in Part IV of this Note, *infra*.

The GDPR affects U.S. businesses: the EU-U.S. Privacy Shield, adopted in July 2016, provides companies in both networks with a mechanism to comply with EU data protection requirements.[49] Joining

---

[39] *See* Hustinx, *supra* note 15, at 9.
[40] *Id.* at 3.
[41] *Id.* at 4.
[42] *Id.* at 9.
[43] *Id.*
[44] *See EU Data Protection Directive*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/intl/eu_data_protection_directive.html (last visited Nov. 30, 2016).
[45] See Protection of Personal Data, EUR. COMM'N, http://ec.europa.eu/justice/data-protection/ (last visited Oct. 19, 2016).
[46] Reform, *supra* note 12.
[47] *Regulations, Directives and Other Acts*, EUR. UNION, https://europa.eu/european-union/eu-law/legal-acts_en#opinions (last visited Jan. 25, 2017).
[48] *See* Hustinx, *supra* note 15.
[49] *Privacy Shield Program Overview*, INT'L TRADE ADMIN.,

the Privacy Shield Framework is voluntary, but once a company joins, compliance is enforceable under U.S. law.[50] 2,535 organizations have joined as of November 2017; many of them are online platforms and gig economy companies, such as Couchsurfing International and orderTalk, Inc.[51]

II. OVERSHARING IN THE ONLINE GIG ECONOMY

A. *Privacy*

To comprehend why privacy issues are especially prevalent within the gig economy, it is necessary to explain how sharing platforms work. The online gig economy is defined by four characteristics: (i) companies provide an online platform that connects customers with contractors; (ii) the contractors have freedom to choose their hours; (iii) the customers pay for a single task at a time; and (iv) the platform facilitates payment for the service.[52] Because of the online nature of this sector, customers regularly input personal information into mobile applications, allowing access to not only the platform that facilitates the service, but also temporarily to the individual contractors who physically provide the single service to the customer.[53] The contractors' data is also collected by the online platform.[54] Layers of privacy concerns exist within the gig economy, depending on whether the party under surveillance is a customer, contractor, or third party.

The federal standard for consumer protection has not been updated to account for the array of private information collected by companies in the online context.[55] Consequently, the U.S. system of sporadic privacy law is insufficiently regulating the sharing economy. When businesses publish a privacy policy promising customers that they will safeguard the customers' personally identifiable information ("PII"), the FTC is tasked with enforcing these promises.[56] Typically, the FTC brings suit under Section 5 of the FTC Act, which bars unfair and deceptive acts and practices.[57] This "unfair and deceptive" language has

https://www.privacyshield.gov/Program-Overview (last visited Sept. 30, 2016).

[50] *Id.*

[51] Privacy Shield Framework, https://www.privacyshield.gov/list (last visited Nov. 1, 2017).

[52] *See* Paychecks, Paydays, and the Online Platform Economy, *supra* note 8.

[53] *See* Uber Privacy Statement, *supra* note 3.

[54] *See* Driver Privacy Statement, UBER (July 15, 2015), https://www.uber.com/legal/.

[55] See Bryan R. Kelly, #PrivacyProtection: How the United States Can Get its Head out of the Sand and into the Clouds to Secure Fourth Amendment Protections for Cloud Journalists, 55 WASHBURN L. J. 669, 682 (2016).

[56] *See Enforcing Privacy Promises*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Jan. 25, 2017).

[57] *Id.*

been the FTC standard since 1938.[58]

Yet the 1938 Congress could not have predicted the inherent difference in surveillance that the online context presents.[59] To illustrate, if a customer walks into a physical store, and a security guard recorded her name and other personal information, noting which items she looked at and for how long, even following her home and to her office, the customer would notice that she was under surveillance. She could then make a choice about this data collection regime.[60] Through the online platform, however, tracking is not similarly visible. Even if the company requires the consumer to click "I agree to the Privacy Policy" before purchasing a service or allows for consent by continued use of the service, she is unlikely to read or comprehend the policy, even if privacy is important to her.[61] It is more difficult for the customer to meaningfully consent to privacy infringement online because in this context, "surveillance is not self-authenticating."[62] "Unfair and deceptive" is an unfair standard for the online customer, when compared to the real world context in which the statute was written. A company can simply use its privacy policy as a liability shield in the online context; the FTC's primary offense alleged in this space is that the company has failed to comply with the company's own voluntarily adopted privacy policy, and yet, the FTC rarely finds harm and usually settles with the companies against which it brings suit.[63] Because the FTC essentially only requires transparency, a customer waives any outside privacy rights by clicking "I agree" to a company's privacy policy in order to use the application. If this company represents in its privacy policy that it can sell consumer data to any third party, for instance, the consenting customer waives any right to limit the sale of her data.

The 1938 FTC standard is especially concerning in the context of the sharing economy, where users consent to broad personal data and geolocation collection in exchange for facilitation of a service. This data is often analyzed for purposes other than those strictly for the business of ridesharing or apartment renting.[64] Gig companies keep customers under surveillance by tracking geolocation, using cookies to record the websites they visit before and after the company's site, and collecting

[58] 15 U.S.C. § 45 (1938).
[59] *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 505 (1999).
[60] *Id.*
[61] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L.REV. 587, 588 (2007).
[62] *Id.*
[63] ADAM D. THIERER & CLYDE WAYNE CREWS JR., WHO RULES THE NET?: INTERNET GOVERNANCE AND JURISDICTION 306 (2003).
[64] *See, e.g.*, *TaskRabbit Privacy Policy*, TASKRABBIT (July 14, 2014), https://www.taskrabbit.com/privacy; *see also* Uber Privacy Statement, supra note 3.

other identifying information.[65] Ninety–one percent of Americans believe that consumers have lost control of how companies collect and use their personal information, and younger Americans are more privacy assertive.[66] A stronger regulatory scheme could reinstate Americans' faith in their online privacy within the gig market.

B. *Uber-Serious Privacy Concerns*

Uber exemplifies the privacy concerns regarding the online platform's interaction with consumers. Electronic Privacy Information Center ("EPIC"), a privacy group, filed a complaint with the FTC last year, alleging that Uber's 2015 update to its privacy policy threatens privacy rights and personal safety of consumers.[67] EPIC claims that the privacy policy violates even the lenient FTC standard of unfair and deceptive trade practice.[68] The 2015 update only increased transparency in Uber's privacy policy; it did not significantly alter Uber's existing policies.[69]

EPIC claims that Uber skirts around the FTC unfair and deceptive standard by disclosing its practices in its privacy policy.[70] Consumers have access to the privacy policy via the app and website, which protects the company from liability under CalOPPA.[71] Uber's privacy policy, like many gig economy platforms' policies, gives the company the right to collect personal contact information and geolocation data, to read text messages sent to drivers, and to store riders' address books on its servers, even after the rider exits the app.[72] The customer's only choice is to accept the privacy policy or refuse to use the service. Uber's new redesign allows customers to sync their contacts with the app, so that the customer can request a ride to a contact's location instead of a physical destination. Uber then will send the contact a one-time request to use her location, and subsequently send the car directly to the contact.[73] It is unclear whether the contact must accept the entire privacy policy and terms of service when consenting to this tracking or

---

65 *TaskRabbit Privacy Policy*, *supra* note 64.

66 *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RESEARCH CTR (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

67 *See In re: Uber Privacy Policy*, ELEC. PRIVACY INFO. CTR, https://epic.org/privacy/internet/ftc/uber/ (last visited Nov. 30, 2016).

68 EPIC Complaint, Request for Investigation, Injunction and Other Relief at 1, In the Matter of Uber Technologies, Inc. (2017), No. 152 3054.

69 *Id.*

70 *Id.*

71 Eric Newcomer, *Uber Broadens Rider Privacy Policy, Asks for New Permissions*, BLOOMBERG TECHNOLOGY, https://www.bloomberg.com/news/articles/2015-05-28/uber-broadens-rider-privacy-policy-asks-for-new-permissions (last visited Sept. 30, 2016).

72 *See* Uber Privacy Statement, *supra* note 3.

73 *See* Katie Benner, *Updated Uber App Will Connect Your Calendar with Your Ride*, N.Y. TIMES (Nov. 2, 2016), https://www.nytimes.com/2016/11/03/technology/updated-uber-app-will-connect-your-calendar-with-your-ride.html?mcubz=0.

simply consent to a one-time geolocation. Under either circumstance, Uber will keep the contact information in the app until it is requested for use.[74]

Similarly, Airbnb's 2016 privacy policy update expanded its right to data, while simultaneously becoming more transparent.[75] The increased transparency made the company more compliant, even though it now collects more user information for deep background checks and other broadly described "business purposes."[76] EPIC has brought complaints under the FTC to a number of other online platforms, which have typically ended in settlements and minor improvements in transparency that lack substantive change.[77]

While it is unclear what sharing platforms such as Uber will use the data they collect from consumers for, Uber openly blogged at the beginning of this decade about its non-business purpose analysis.[78] For example, in one notorious blog post "Rides of Glory," Uber aggregated its data to complete a social science study determining which nights "brief overnight stays," or "one-night stands" were most prevalent.[79] The blog analyzes these trips by day of the year, noting peaks on certain nights, such as Cinco de Mayo, and valleys on others, such as Valentine's Day.[80] One past Uber blog even described the company as "a technology company revolutionizing transportation" only "on the surface." Underneath, the blog post continues, Uber collects data in "so many ways" that "aren't immediately relevant to the core part of [their] business."[81] While Uber has refrained from these public blog posts of late, they have continued to expand the breadth of information collected from its riders and have used geolocation to promote new features, including an integration with Snapchat.[82]

In another context, much research has taken place to address the important topic of racial discrimination in the gig economy.[83] The

---

[74] Uber Privacy Statement, *supra* note 3.

[75] Airbnb Privacy Policy, AIRBNB (October 27, 2016), https://www.airbnb.com/terms/privacy_policy.

[76] *Id.*

[77] In re: Uber Privacy Policy, *supra* note 67.

[78] *See, e.g.*, Voytek, *Rides of Glory*, UBER BLOG (Mar. 26, 2012), http://blog.uber.com/ridesofglory; *see also*, Uber Team, *How Crime Location Knowledge is a Proxy for Uber Demand*, UBER BLOG (Sept. 13, 2011), http://blog.uber.com/2011/09/13/crime-knowledge-demand-proxy/.

[79] Voytek, *supra* note 78.

[80] *Id.*

[81] Uber Team, *supra* note 78.

[82] *See* Natasha Singer & Mike Isaac, *Uber Data Collection Changes Should Be Barred, Privacy Group Urges*, N.Y. TIMES (June 22, 2015), https://www.nytimes.com/2015/06/23/technology/uber-data-collection-changes-should-be-barred-privacy-group-urges.html?_r=0; Andrew Chen & Miraj Rahematpura, *Uber to Your Friends and Snap Along the Way!*, UBER NEWSROOM (Dec. 21, 2016), https://newsroom.uber.com/ubertofriends.

[83] *See, e.g.*, Yanbo Ge, Christopher R. Knittel, Don MacKenzie & Stephen Zoepf, *Racial and*

privacy question here is whether Uber, Lyft, or Airbnb adequately disclosed that personal data would be handed over to third-party universities to conduct this type of research. Under the current FTC standard of "unfair and deceptive," Uber's privacy policy discloses that Uber may use collected information to conduct data analysis, testing and research, but fails to disclose that they may share that information to a third party for the same purpose.[84] Researchers from the Massachusetts Institute of Technology, Stanford University and the University of Washington published a recent study that found the following: Uber drivers in Boston canceled rides for men with black-sounding names at a rate double those for other men; drivers took female users for longer, more expensive rides than male users; and black users in Seattle waited a significantly longer period of time (as much as a 35% increase) for a ride than white users.[85] This type of data analysis is critical to decreasing these discriminatory practices in the gig economy. It denotes important issues for companies to systematically address through trainings and acquisition of independent contractor practices. The benefits of the research, however, do not mask the privacy issue at hand: Uber did not disclose that they would be handing over data to universities for study without disclosing that fact to users and contractors through its privacy policy.

Independent contractor privacy issues also arise in the sharing economy. Uber drivers are under even more surveillance than riders.[86] Uber has adamantly contested that its drivers are independent contractors, and not employees.[87] Therefore, surveillance of the driver has resulted in a power imbalance between Uber and these independently contracted drivers.[88] For instance, contractors driving on "dead miles" without carrying a fare are still generating useful data for Uber, which is relayed to the platform where the company analyzes traffic patterns and improves its algorithm.[89] The automatic aggregation of driver data even while the driver is not receiving payment differentiates the gig economy's privacy and surveillance issues from those of a traditional service economy, where employees are provided with payment in consideration for relinquishing some rights to generate

Gender Discrimination in Transportation Network Companies (Nat'l Bureau of Econ. Research, Working Paper No. 22776, 2016).

84 Uber Privacy Statement, *supra* note 3.

85 Yanbo Ge, *supra* note 83.

86 Uber Privacy Statement, *supra* note 3.

87 *See* Dan Levine, *Uber Drivers Remain Independent Contractors as Lawsuit Settled*, REUTERS TECH. NEWS (Apr. 21, 2016, 10:43 PM), https://uk.reuters.com/article/us-uber-tech-drivers-settlement/uber-drivers-remain-independent-contractors-as-lawsuit-settled-idUKKCN0XJ07H.

88 Alex Rosenblat & Luke Stark, *Uber's Drivers: Information Asymmetries and Control in Dynamic Work*, 10 INT'L. J. OF COMMC'N. 3758 (2015).

89 *Id.*

greater benefit to the company.[90] Furthermore, customers act as "watchers" for the company when they rate drivers.[91] Riders' ability to view the drivers' location has been another concern, as they can track the driver even after departing the car.[92]

C. Autonomous Cars

Driver data is even used for autonomous car research, which could ironically take drivers' jobs away altogether.[93] Uber has been testing and plans to introduce driverless cars in Pittsburgh, where the mayor claims it is not the city government's role to regulate or limit sharing economy companies.[94] Cities like Pittsburgh are giving free reign to gig economy companies in order to transition from Rust Belt manufacturing cities into technology hubs.[95] The price of the autonomous car's convenience and forward-thinking technology is extremely detailed surveillance, a natural and essential extension of its functionality.[96] At a Congressional hearing on March 15, 2016, Senators Ed Markey and Richard Blumenthal questioned industry leaders regarding whether they would support mandatory privacy restrictions on personal data collected from self-driving cars.[97] The executives avoided the question, agreeing instead to comply with their own privacy policies.[98] Senator Markey answered: "We don't pass murder statutes for our mothers. They're not going to murder anybody. We do it for the people who might murder others. So we have some sort of standard."[99] This response is relevant not only to Uber's driverless cars, but to privacy concerns across the board. The only non-industry representative on the panel, Mary Louise Cummings, director of the humans and autonomy lab at Duke University, agreed with the Senator that these cars will become "big data-gathering"[100] machines, and that it is unclear what will be done with that data. Senator Markey assembled a congressional report in

90 *Id.*
91 *Id.*
92 *Id.*
93 *See* Max Chafkin, *Uber's First Self-Driving Fleet Arrives in Pittsburgh this Month*, BLOOMBERG (Aug. 18, 2016), https://www.bloomberg.com/news/features/2016-08-18/uber-s-first-self-driving-fleet-arrives-in-pittsburgh-this-month-is06r7on.
94 *See* Cecilia Kang, *No Driver? Bring It On. How Pittsburgh Became Uber's Testing Ground*, THE N.Y. TIMES (Sept. 10, 2016), https://www.nytimes.com/2016/09/11/technology/no-driver-bring-it-on-how-pittsburgh-became-ubers-testing-ground.html?mcubz=0.
95 *Id.*
96 *See* Adrienne Lafrance, *How Self-Driving Cars Will Threaten Privacy*, THE ATLANTIC, (Mar. 21, 2016), https://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/.
97 Pete Bigelow, *Four takeaways from the Congressional hearings on self-driving cars*, CSPAN (March 17, 2016), https://www.autoblog.com/2016/03/17/senate-self-driving-cars-autonomous-privacy-google/.
98 *Id.*
99 *Id.*
100 *Id.*

which he explains that customers are often not made aware of data collection in new vehicles with technological integrations, and when they are, they often cannot opt out without disabling important features, including navigation.[101]

While this report does not explicitly refer to shared cars, it describes precisely the ultimatum that all gig economy customers face, whether entering a car with an autonomous driver through Uber, or renting a vacation home through VRBO: should I relinquish all requested data privacy rights, or should I refuse to use the service? The only current restriction on these companies is self-regulation – they cannot violate their own privacy policies. While they abide by the law, in some cases even requiring a consumer to click "I agree" to the privacy policy, they refrain from offering the customer any meaningful choice when contracting with the platform. Consumers act reasonably when they decline to read every privacy policy they consent to. Users would waste thousands of hours if they did read and cognize every term in every online agreement. Furthermore, there is no mechanism in place for users to advocate for themselves if they do read, but disagree with the company's use of their data. Data usage in privacy policies is often formulated through vague phrases such as to "[p]rovide, maintain, and improve our Services."[102] Because gig economy customers have no opportunity to meaningfully contract, the government should protect customers. Leaving regulation to the market allows corporations, who have little incentive to protect consumer data, to capitalize on their users' inadequate bargaining power in data collection.

III. GOVERNMENTAL ACCESS TO DATA

A. Municipal Requests for Traffic Data

While most gig economy participants are unwilling to allow governmental access to their personal data, they will allow private entities access in exchange for a service.[103] The gig economy allows municipalities to end run a citizen's predilection to protect his personal data from the government.[104] Waze, Uber, and Airbnb, among others, have partnered with city governments to provide troves of data that raise further privacy concerns, albeit with the potential to improve governance.[105] Municipalities have requested data for genuine purposes

[101] Staff of S. Edward J. Markey, 114th Cong., Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (Feb. 2015).
[102] Uber Privacy Statement, *supra* note 3.
[103] *See* Charlie Sorrel, *Waze Now Shares its Data with Cities to Improve Roads and Speed Up Journeys*, FAST CO. (Oct. 21, 2016), https://www.fastcoexist.com.
[104] *Id.*
[105] *See* Nestor M. Davidson & John J. Infranca, *The Sharing Economy as an Urban Phenomenon*, 34 YALE L. AND POL'Y. REV. 215, 274 (2016).

of improving housing and traffic, which are traditional city government roles.[106] In New York City, the Taxi and Limousine Commission is seeking to obtain passengers' individual pick-up and drop-off locations, as well as names and credit card data.[107] Uber has resisted the request, citing governmental data breach concerns which would harm its users and reputation.[108]

When presented with other city governments' requests for traffic data, Uber's strategy had been to provide the municipality with anonymized data.[109] As recently as 2014, Uber argued against California regulators that its traffic data was a "trade secret," and therefore not subject to any governmental appropriation.[110] At that time, Uber required the California Public Utilities Commission ("CPUC") to bring its request for detailed ride data to administrative court.[111] To differentiate this from Uber's current regime, the company recently agreed to share *anonymized* data with Boston, claiming the compromise allowed them to assist with city planning and traffic analysis, while simultaneously protecting individual customers' PII.[112]

Anonymizing data records allows the data to stand alone, unassociated with a specific person and therefore not in violation of privacy norms.[113] However, security issues can arise depending upon the type of encryption used.[114] As the size and diversity of the data increases, the likelihood of being able to re-identify individual data also increases substantially.[115] As municipalities are able to collect more data from gig economy platforms, anonymizing will likely provide only a false expectation of privacy, as the government will be able to identify an individual's geolocation, among other data.[116]

B. Fourth Amendment Implications

Most sharing economy platforms do not even provide the

106 *See, e.g.*, Adam Vaccaro, *Boston Wants Better Data from Uber, and is Taking a Roundabout Route to Try and Get it*, BOSTON.COM (June 28, 2016), https://www.boston.com/news/business/2016/06/28/uber-data-boston-wants.

107 *See* Faiz Siddiqui, *Uber and New York City Spar Over Rider Data*, WASH. POST (Jan. 5, 2017), https://www.washingtonpost.com/news/dr-gridlock/wp/2017/01/05/uber-and-new-york-city-spar-over-rider-data/?utm_term=.b3011e3bf1da.

108 *Id.*

109 *Id.*

110 Sarah McBride, *Uber's Fight of California Data-Sharing Rule Highlights Its Bumpy Road*, REUTERS TECH. NEWS (Dec. 18, 2014), http://www.reuters.com/article/us-uber-california-data/ubers-fight-of-california-data-sharing-rule-highlights-its-bumpy-road-idUSKBN0JX01320141219.

111 *Id.*

112 Vaccaro, *supra* note 106.

113 President's Council of Advisors on Sci. & Tech. Executive Office of the President, Big Data and Privacy: A Technological Perspective (2014) at 38.

114 *Id.* at 39.

115 *Id.*

116 *Id.*

anonymized protections from government grasp of data that Uber and Airbnb do. Platforms like TaskRabbit, VRBO, Getaround and Postmates do not require a warrant before providing users' content or geolocation to the government, and do not inform their users of governmental data requests.[117] For instance, in Uber's 2014 battle with the CPUC, discussed above, its rivals Lyft and Sidecar released the data to California regulators with less pushback.[118]

These concerns enter constitutional territory when a governmental or law enforcement entity requests data. The Fourth Amendment protects individuals' right to privacy and freedom from arbitrary intrusions by the government,[119] specifically providing the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[120] It further requires warrants to be issued only upon "probable cause" and "particularly describing the place to be searched, and the persons or things to be seized."[121] This right is activated where the individual has a "reasonable expectation" of privacy by society's standards under the circumstances.[122]

As technology has developed, what constitutes a reasonable expectation of privacy has drastically changed, as the analysis requires a foray into the contemporary role of the technology used to collect data.[123] For example, given geolocation's ubiquity, a Getaround car renter who consents to geotracking might later fail to establish a reasonable expectation of privacy from the government.[124] Under the current legal framework, technological advances require gig economy companies themselves to protect their users' data from the government.[125] Uber, for example, represents to its customers through its law enforcement guidelines that it will require a warrant before handing over rider geolocation data to the government.[126] An Uber rider, therefore, might consequently have a reasonable expectation of privacy and Fourth Amendment protection based on that promise. Because many smaller startup companies, such as Getaround, do not promise user privacy from governmental requests, they allow law

117 *See* Nate Cardozo, Kurt Opsahl & Rainey Reitman, The Electronic Frontier Foundation, Who Has Your Back?: Protecting Your Data from Government Requests: Sharing Economy Edition (2016), https://www.eff.org/files/2016/05/04/who-has-your-back-2016.pdf.
118 McBride, *supra* note 110.
119 U.S. CONST. amend. IV.
120 *Id.*
121 *Id.*
122 Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).
123 *See* Kyllo v. United States, 121 U.S. 2038 (2001); *see also* Adam R. Pearlman & Erick S. Lee, National Security, Narcissism, Voyeurism, and Kyllo: How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment, 2 TEX. A&M L. REV 719 (2015).
124 Pearlman & Lee, *supra* note 123.
125 Cardozo, Opsahl & Reitman, *supra* note 117.
126 *Id.* at 23.

enforcement to circumvent the Fourth Amendment, acting as a conduit for governmental overreach.[127] As compared with the rest of the tech industry,[128] gig economy companies have failed to safeguard user data against unwarranted governmental requests.[129] It is unclear, however, whether a representation in a privacy policy that a gig economy company will protect user data from government overreach is binding upon the government. The user might be able to bring action against the startup economy company on breach of contract, but this might not be viable to render evidence inadmissible in a criminal case.

Because of this constitutional concern, courts have adapted traditional Fourth Amendment principles to modern technology.[130] Unlike when the Fourth Amendment was adopted, there are no longer pragmatic constraints of time and resources on police surveillance. Therefore, police departments are currently incentivized to "track, gather, and analyze" limitless amounts of data.[131] To combat this culture of tracking, courts implement Fourth Amendment-based controls requiring law enforcement to procure a warrant to access personal information, depending on a fact-specific examination of the technology used to gather the data.[132]

The Eleventh Circuit has ruled that law enforcement does not need a warrant to obtain cell phone tower information.[133] This court rationalizes its decision based on principles of the 'reasonable expectation of privacy and ownership of information'.[134] The court explains the first principle by saying the public is sufficiently aware that tracking exists and that police use information based on cell phone tower location.[135] They therefore have no reasonable right to expect privacy relating to those records. Secondly, the court says the information found through cell phone towers is not the defendant's information at all, but is owned by the cell phone carrier in this case, like a surveillance video tape is owned by the store.[136] The court explains that "those surveillance camera images show [the defendant's]

127 *Id.*

128 *See, e.g.*, *Breaking Down Apple's iPhone Fight with the U.S. Government*, N.Y. TIMES (March 21, 2016), https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html?_r=0.

129 Cardozo, Opsahl & Reitman, *supra* note 117.

130 *See, e.g.*, California v. Carney, 471 U.S. 386 (1985) (holding that a mobile home is primarily a vehicle by focusing on the characteristic of an RV's mobility and functionality, rather than the traditional lexicon of "home"); Riley v. California, 134 U.S. 2473 (2014) (discussing the difference between a physical search of the subject and a search of the subject's cell phone data).

131 Steven I. Friedland, *Of Clouds and Clocks: Police Location Tracking in the Digital Age*, 48 TEX. TECH L. REV. 165, 184 (2015).

132 *Id.*

133 United States v. Davis, 785 F.3d 498 (11th Cir. 2015).

134 *Id.*

135 *Id.*

136 *Id.*

location at the precise location of the robbery, which is far more than [the carrier's] cell tower location records show,"[137] focusing on the specificity of data collected.

Conversely, the Supreme Court has held that the government needs a warrant to access hotel records and personal cell phones.[138] The Court recently held that a municipal code provision requiring hotel owners to provide law enforcement with specified information about guests upon demand violated the Fourth Amendment.[139] In another case, the Supreme Court explicitly stated "[their] answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[140] The Court focused on the amount of sensitive personal data that is stored on cell phones, and suggested it would render warrantless cell phone *tracking* unconstitutional as well.[141] It differentiated between a cell phone and physical records based on quantity and quality, explaining how browsing history could reveal "an individual's private interests or concerns" and can "reconstruct someone's specific movements down to the minute."[142]

Based on these parameters, data from gig economy applications might be protected by the Fourth Amendment. On one hand, the Supreme Court's protection against warrantless cell phone search can be logically extended to data within applications. Geolocation that extends even after the user exists the application can also reconstruct specific movements, and online tracking can provide private user information. The issue remains, however, whether the acknowledgement of the company's privacy policy essentially amounts to a user's waiver of the Fourth Amendment in this context, as the user might not be able to claim a reasonable expectation of privacy after consenting to provide so much data. This could potentially be analogous to the cell phone tower, since the online gig economy platform now owns the information, not the user.

Assuming a reasonable expectation of privacy does exist, the question remains whether accessing digital data constitutes a "search" for Fourth Amendment purposes. Given the large troves of customer and contractor data collected by online gig economy platforms, law enforcement officials have turned to this data as part of their investigations, thus constituting a "search" under the meaning of the Fourth Amendment.[143] Police GPS surveillance, for example, "generates

137 *Id.* at 511.
138 City of Los Angeles, Calif. v. Patel, 135 U.S. 2443 (2015); *Riley*, 134 U.S. 2473 (2014).
139 *Patel*, 135 U.S. at 2443.
140 *Riley*, 134 U.S. at 2495.
141 *Id.*
142 *Id.* at 2490.
143 U.S. v. Jones, 132 S. Ct. 945 (2012) (noting GPS tracking constitutes a search within the

a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,"[144] and the Supreme Court has therefore observed that GPS monitoring constitutes a search under the meaning of the Fourth Amendment.[145] Because some gig economy platforms continue to track users' locations even after they have exited the application, they collect compounding data over a period of time that can reveal finances, consumer preferences, and health data, among a myriad of other information.[146] If the police are able to request and receive that data without protection for the consumer, the spirit of the Fourth Amendment will be invalidated.[147]

IV. FTC GUIDANCE FOR STATE LAW AS A SOLUTION

Strong regulatory guidance by the FTC could standardize and explain the "unfair and deceptive" standard. This would protect gig economy customers' privacy, allowing them to safely provide personal information to gig economy platforms without exposing themselves to serious risk factors, including manipulation of data for non-business purposes or open governmental access to personal data.

Government entities in other contexts have created solid starting points for the FTC to implement guidance applicable to the gig economy.[148] The FCC, through its adaptation of subsequently repealed privacy rules protecting broadband customers, coupled with CalOPPA and the GDPR, provided many strong regulatory points that the FTC should borrow from when constructing their own report regarding privacy in gig commerce.[149]

A. *The FTC's Jurisdiction*

As discussed above, Section 5 of the FTC Act provides the FTC with authority to prohibit "unfair or deceptive" practices.[150] However, these situations require the FTC to catch violations *ex-ante*.[151] Companies can lean on broad or vague privacy policies to render Section 5 inapplicable.[152] The FTC can only issue guidelines, and has no jurisdictional authority to mandate accountability without supporting

meaning of the Fourth Amendment.); Cardozo, Opsahl & Reitman, *supra* note 117.

144 *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

145 *Id.*

146 *See, e.g.*, Uber Privacy Statement, *supra* note 3.

147 *See* Friedland, *supra* note 131 at 184.

148 *See, e.g.*, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64 (2016).

149 *Id.*

150 15 U.S.C. § 45 (2006).

151 Lipman, *supra* note 38.

152 *Id.*

congressional legislation.[153] The FTC has nevertheless regulated privacy in some contexts by creating "soft law."[154] FTC soft law consists of guidelines, workshops and press releases, e.g., a report on mobile applications for children.[155] The boundaries of these materials lack clarity, however, as the FTC has never expressly articulated which of these recommendations are mandatory as opposed to mere best practices.[156]

At any rate, this soft law illuminates the FTC's privacy philosophy. Companies give weight to these materials, as evidenced by, for example, the institution of privacy policy provisions to protect against contracting with children online.[157] The FTC's soft law has been compared to judicial dicta; it incentivizes companies to comply by providing notice of how it will interpret its regulatory authority in Section 5 settlements.[158] While the FTC lacks statutory jurisdiction to extend privacy regulation beyond the transparency standard under Section 5 of the FTC Act, it has essentially created rules through its own "common law,"[159] and any guidance issued will have practical force upon gig economy companies.

As one such guidance, the FTC recently released a report specific to issues in the sharing economy.[160] This report acknowledges the existence of substantial privacy concerns within the sharing economy, yet it only briefly addresses them.[161] Several panel participants remarked on the tension of balancing privacy concerns with the flow of necessary information.[162] The FTC stated that further Commission work will provide guidance in this area.[163]

B. *State Response to the Proposed FTC Guideline*

Moreover, the FTC's hypothetical privacy guidelines would evidence the importance of privacy protection for state legislatures. Forty-three states have enacted laws with a broad prohibition of deceptive acts, enforceable by consumers.[164] These and similar acts,

153 *Id.*

154 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 625 (2014).

155 *See* Lipman, *supra* note 38.; *see also id.*

156 Solove & Hartzog, *supra* note 154 at 626.

157 *Id.*; *Children's Online Privacy Policy*, THE WALT DISNEY CO. (July 14, 2016), https://disneyprivacycenter.com/kids-privacy-policy/english/.

158 *See* Solove & Hartzog, *supra*, note 154 at 626.

159 *Id.*

160 *See* Fed. Trade Comm'n, The "Sharing" Economy: Issues Facing Platforms, Participants & Regulators (2016).

161 *Id.*

162 *Id.*

163 *Id.*

164 *See* Carolyn L. Carter, Nat'l Consumer L. Ctr., Consumer Protection in the States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes (2009).

known as "Little FTC Acts," purport to achieve the same goals as the FTC Act at the state level.[165] Little FTC Acts essentially fill gaps where the FTC has not yet acted on behalf of the consumer or where the harm is felt locally.[166] Little FTC Acts have taken on a "broader consumer protection function than the FTC"[167] and therefore have jurisdiction to provide citizens with stronger privacy protection than at the federal level. If the FTC were to release a report on online personal information privacy, states would likely respond by adopting at least as stringent a privacy protection standard as the FTC. This would complement the FTC report and provide the second step in the solution to privacy infringement by gig economy companies.

Little FTC Acts typically provide a private right of action, stronger remedies, and fewer limitations when compared with the FTC Act.[168] Unlike the federal version, these laws allow private actors to pursue claims of unfair and deceptive practices under the state's standard.[169] Consumer attorneys act as private attorneys general who, unlike the FTC, are not bound by political pressure.[170] Little FTC Acts also provide substantial compensation for wronged consumers; half of these Acts allow private parties to recover treble damages.[171] Enforcement is also broader than the federal standard, as consumers are able to pursue any case.[172] At the state level, they are unbarred by the FTC restriction that the consumer protection action be in the "public interest."[173]

California's Unfair Competition Law ("UCL") exemplifies the expansive consumer rights prevalent in Little FTC Acts. The UCL goes beyond "unfair and deceptive" to prohibit unlawful business practices as well.[174] The UCL's unfairness standard is broader than the FTC's: it asks whether a business practice offends the policy of a regulation.[175] The UCL's fraudulent prong mirrors the FTC's deceptive prong. However, this state action need not be pled with the specificity the FTC requires; a California court will find a cause of action unless, as a matter

165 *See* Henry N. Butler & Joshua D. Wright, *Are State Consumer Protection Acts Really Little-FTC Acts?*, 63 FLA. L. REV. 163, 164–65 (2011).
166 *See id.* at 165.
167 *See* Butler & Wright, *supra* note 165, at 166–67.
168 *See id* at 173–75.
169 *See id* at 165.
170 *Id.*
171 *See* Christine Lipsey & Dylan Tuggle, *Little FTC Acts and Statutory Treble Damages – Traps for the Unwary*, A.B.A. JOURNAL, https://apps.americanbar.org/litigation/committees/businesstorts/articles/1109_lipsey.html (last visited Nov. 30, 2016).
172 *Id.*
173 Butler & Wright, *supra* note 165, at 166.
174 Lenore Albert & Michael Thurma, *Unfair and Deceptive Practices: A Comparison of the FTC Act and California's UCL*, 22 NO. 2 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 51, 53 (2013).
175 *Id.*

of law, citizens were not likely to be deceived by the business practice.[176] While not specific to privacy, data breaches have been litigated increasingly under the UCL.[177] Plaintiffs can establish a cause of action by claiming they paid more for the defendants' products than they would have had they known about the defendants' deficient data security measures.[178] This principle could possibly translate into the privacy sphere. Imagine the FTC released a report that they will require more choice, transparency and consumer power in negotiation from gig economy platforms under Section 5 of the FTC Act. States could then use their expansive private right of action and more surmountable pleading standards to provide privacy protection to consumers.

Given the current political climate and repeal of the FCC privacy rules, it is unclear whether the FTC would in fact issue guidance promoting privacy for customers. This makes the state-level regulation even more important, and remains a possibility in the face of federal political fluctuations.

C. *FCC Privacy Regulation of ISPs*

The FCC's former privacy rules applicable to ISPs could serve as a model for the FTC's guidance applicable to sharing economy companies. In 2015, the FCC reclassified broadband ISPs as telecommunications services, allowing for regulation of ISPs as common carriers in the same way the telephone system is regulated.[179] This brought ISPs out of the purview of the FTC, allowing the FCC instead to issue regulations.[180] Just months after the D.C. Circuit upheld the reclassification,[181] the FCC released privacy rules (the "rules") designed to give broadband customers "the tools they need to make informed decisions about how their information is used and shared by their ISPs."[182] These rules contained many policy-driven provisions that could be transferable to an FTC report promoting privacy in the gig economy.

Congress recently issued a resolution to overturn the rules, which

176 *Id.*

177 *See* Stroock & Stroock, & Lavan LLP, 2015 Annual Overview of California's Unfair Competition Law and Consumers Legal Remedies Act (2015).

178 *Id.*

179 *See* Press Release, Fed. Commc'ns Comm'n, FCC Adopts Strong, Sustainable Rules to Protect the Open Internet (Feb. 26, 2015) (on file with author).

180 *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Net Neutrality and Privacy: Don't Fear the Reclassification, Keynote Address at the 2015 TPRC – 43rd Research Conference on Communications, Information, and Internet Policy (Sept. 26, 2015).

181 *See* U.S. Telecom Ass'n v. Fed. Comm. Comm'n, 825 F.3d 674, 689 (D.C. Cir. 2016).

182 Press Release, Fed. Commc'ns Comm'n, FCC Adopts Privacy Rules to Give Broadband Customers Increased Choice, Transparency and Security for their Personal Data (Oct. 27, 2016) (on file with the author).

President Trump approved in April 2017.[183] The Republican-controlled Congress claimed the rules unfairly restricted broadband providers, such as AT&T, while refraining from regulating internet companies such as Facebook or, in theory, Uber.[184] This "repeal without a replacement" allowed broadband providers once again to collect customers' PII and sell to advertisers with little governmental oversight.[185] To combat further privacy encroachment, the FTC should attempt to regulate internet companies using principles from the repealed FCC rules.

Under the rules, which were intended to go into effect late 2017, ISPs had to receive opt-in consent from consumers before sharing sensitive data with third parties.[186] Sensitive data includes geolocation, browsing and app use history, Social Security numbers and the content of communications.[187] ISPs could use and share non-sensitive information, subject to a consumer expectation standard, but had to give customers the ability to opt out of sharing any private information.[188] Email addresses and service tier information fell under this opt-out category.[189] This provided users with significant choice in who can collect or access their personal data.

Moreover, ISPs were required to clearly notify users about what information they collected, how they used and shared it, and also had to identify the types of third parties who would receive any data.[190] This would have likely constrained broad or vague privacy policy language. ISPs could not have used "take-it-or-leave-it" offers leading to adhesion contracts.[191] Stated differently, an ISP could not refuse to provide service to customers who did not consent to the use and sharing of their personal information for commercial purposes.[192] Furthermore, ISPs which wanted to use "de-identified information" not associated with an individual user or device must have sufficiently altered the user's information so that it could not be "reasonably linkable to an individual or device."[193] If they shared de-identified information with third parties for research, promotional, or other purposes, IPSs would have been

183 *See* Steve Lohr, *Trump Completes Repeal of Online Privacy Protections from Obama Era*, N.Y. TIMES (Apr. 3, 2017), https://www.nytimes.com/2017/04/03/technology/trump-repeal-online-privacy-protections.html?mcubz=3.

184 *Id.*

185 *Id.*

186 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64; Lohr, *supra* note 183.

187 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64.

188 *Id.*

189 *Id.*

190 *Id.*

191 *Id.*

192 In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 47 C.F.R. § 64, at 124.

193 *Id.*

required to "contractually prohibit the re-identification of shared information."[194] This would amount to an additional check on encryption, disallowing third parties from attempting to re-identify individuals with the encrypted data. This is not otherwise difficult from a technical perspective, as explained in Part III of this Note. Democratic Commissioner Mignon Clyburn expressed disappointment that mandatory arbitration clauses went untouched by the rules but was hopeful at the time of the rules' release that mandatory arbitration rulemaking would be tasked to the next presidential administration.[195]

Under the current administration, however, the enforcement of privacy rules in any capacity is uncertain. ISPs lobbied against, and House Republicans criticized, the FCC privacy rules, claiming, as discussed above, that ISPs should not be held to stricter privacy standards than websites, which remain under the FTC's jurisdiction.[196] Websites which receive most advertisement money, including Google and Facebook, were untouched by the FCC's rules. They were therefore under no requirement to allow users to opt-out of third party sharing of data. Furthermore, they could still compel users to "take-it-or-leave-it" and benefit monetarily from targeted advertisements.

Gig economy apps were similarly not subject to the FCC rules. Uber continually claims to be an information technology company.[197] This could be considered a valid claim, as it appears its revenue soon will be derived from selling data to third parties, rather than from transportation.[198] For instance, Uber recently partnered with Starwood Hotels, allowing users to link their Uber account to a Starwood Hotels point-based rewards program.[199] Essentially, Uber sells to Starwood all of its users' Uber-related activity, including geolocation and browsing history data.[200] Under the FCC regime, an ISP would have had to allow its customers to affirmatively opt-in to sharing this data with Starwood, while Uber would not. Currently, Uber does choose to require opt-in through an "Allow" or "Deny" interface,[201] but this is a business decision, rather than a legal requirement. As customers become more

194 *Id.* at 47.

195 *See* Jon Brodkin, *FCC Imposes ISP Privacy Rules and Takes Aim at Mandatory Arbitration*, ARSTECHNICA (Oct. 27, 2016), https://arstechnica.com/information-technology/2016/10/isps-will-soon-have-to-ask-you-before-sharing-private-data-with-advertisers/.

196 *See* Jimmy Hoover, *House Republicans Slam FCC's Broadband Privacy Proposal*, LAW 360 (June 2, 2016), https://www.law360.com/articles/802962/house-republicans-slam-fcc-s-broadband-privacy-proposal.

197 Laura Lorenzetti, *Everything to Know about the Uber Class Action Lawsuit*, FORTUNE (Sept. 2, 2015), http://fortune.com/2015/09/02/uber-lawsuit/.

198 Ron Hirson, *Uber: The Big Data Company*, FORBES (Mar. 23, 2015), https://www.forbes.com/sites/ronhirson/2015/03/23/uber-the-big-data-company/#53590c8918c7.

199 *Id.*

200 *Id.*

201 *Id.*

willing to exchange personal data for airline miles or hotel points, the company could choose to remove the opt-in safeguard. Under the rules, ISPs could have become less competitive in the market of selling personal data.

An alternative solution to this imbalance is to regulate privacy of websites and gig economy platforms through FTC guidelines, while enacting congressional legislation allowing the FCC to reinstate similar privacy rules. Instead of relying on the imbalance problem to advance an argument for deregulation, the imbalance could be repurposed as an argument for regulation of websites and, by extension, gig economy apps. The BROWSER Act, discussed *infra* Part V, offers a similar solution, although it is unlikely to pass either House of Congress.

D. *CalOPPA*

An FTC report should also borrow principles from the foremost state-level privacy law in the United States, California's CalOPPA, described briefly in Part I of this Note. CalOPPA, enacted in 2004, requires commercial website operators who collect PII to conspicuously link to a privacy policy on its website.[202] This privacy policy must disclose what type of PII is collected, and any third parties who might access this data.[203] It must, furthermore, contain clauses describing: how users can request changes to PII; how the operator will notify users of privacy policy changes; an effective date of the privacy policy; and disclosure of how the operator responds to users' "Do Not Track" requests.[204] Extension of these transparency requirements to the federal context would streamline privacy policy drafting for gig economy companies, whether they plan to operate in California or not. Moreover, it would provide a baseline of privacy protections for users, demanding more specific disclosure than Section 5 of the FTC Act requires.

E. *GDPR*

EU's new GDPR will significantly affect companies doing business with the European Union.[205] It focuses primarily on data protection measures, but privacy protection is additionally enhanced. For example, under the GDPR, a user's consent to personal data processing must be as easy to withdraw as to give.[206] The platform must receive "explicit" consent from users for sensitive data, and must be

202 *See* California Online Privacy Protection Act of 2003, CAL. BUS. & PROF. §§22575–79 (2004)
203 *Id.*
204 *Id.*
205 *See* Cedric Burton, Laura De Boel, Sarah Cadiot & Sara Hoffman, *WSGR Alert: New EU Data Protection Regulation is Now Enacted*, WSGR (Apr. 14, 2016), http://www.wsgrdataadvisor.com/2016/04/wsgr-alert-new-eu-data-protection-regulation-is-now-enacted/.
206 ALLEN & OVERY, THE EU GENERAL DATA PROTECTION REGULATION (2016).

able to demonstrate that consent was affirmatively given.[207] Any existing consent must meet the new conditions.[208] To determine whether this consent was freely given, the GDPR requires contemplation of the balance of power between the user and the platform.[209] A factfinder must consider fairness factors including whether the performance of the contract is made conditional on the user's consent to personal data collection that exceeds necessity, i.e. an adhesion contract.[210] If this type of provision were instituted in the United States, it would greatly affect gig economy platforms. For instance, Uber's ability to collect contact information from a rider's address book would be limited. Uber must allow customers to use the platform even if they choose not to allow Uber access to their contact list.

The GDPR extensively addresses platform transparency and customer choice. Platforms must provide, and obviously bring to users' attention, the right to object to use of personal data for directed advertising purposes.[211] Fair processing notice requirements are more comprehensive in the GDPR. Platforms must disclose certain rights and information to individual users, including the right to withdraw consent, and the length of time the data will be stored.[212] Processing notice must be clear and easily discernable to users.[213]

F. *Privacy Protection for the Gig Economy (A Model FTC Staff Report Introduction)*

This subsection presents a proposal for a theoretical Staff Report that the FTC could release providing guidance to sharing economy participants.

Consumer choice and transparency with regard to personal data must be balanced with the platform's interest in streamlining transactions. Adequate balance can be a challenge for regulators to achieve. The Commission should actively assess privacy regulation in other contexts and weigh the factors to provide a report on privacy in the gig economy. This report would serve as a guideline for online sharing economy companies to comply with Section 5 of the FTC Act. This Commission report would focus on three prongs: consumer choice, platform transparency, and balance of power between the two parties to the gig economy transaction. Additionally, it should feature a chapter discussing the sharing of data with the government.

The longstanding principle of consumer choice could be clarified

207 *Id.*
208 *Id.*
209 *Id.*
210 *Id.*
211 The EU General Data Protection Regulation, *supra* note 206.
212 *Id.*
213 *Id.*

specifically for the gig economy by this proposed report. To deliver sufficient choice to users, online sharing economy platforms must noticeably provide users with the ability to opt out of sharing any "private" information with third parties. This classification of information would include email addresses, physical addresses and phone numbers. Platforms furthermore should be required to receive affirmative opt-in consent prior to sharing "sensitive" information with third parties. Sensitive information includes geolocation, app use history and communication content. The platform would have to demonstrate that consent was affirmatively given if the FTC were to bring suit under Section 5. This requirement would split the burden between users and platforms. It would allow platforms to seamlessly use personal information required to conduct their transactions without requiring opt-in consent, while simultaneously requiring opt-in from users before sharing sensitive data. Sensitive data is ordinarily not necessary to complete the transaction for which the application was used. The user should also be able to withdraw consent at any time.

To avoid deception under Section 5, platforms should have to maintain transparency about the data they collect from their users. The Commission should require online gig economy platforms to disclose, through a privacy policy, the following: what type of PII they collect; how users can request changes to this collection; how the platform will notify users of changes to the privacy policy; how long data will be stored; and any third parties with whom the platform might share data. This privacy policy should be conspicuously linked to on the main page of the platform's application or website. Platforms furthermore should be obligated to disclose the rights to choices that users have, including the right to withdraw consent.

Currently, an imbalance between the user and platform exists in online contracting in the gig economy. To remedy this disparity, platforms should be unable to condition performance of the contract on the user's consent to personal data collection that exceeds necessity. Gig economy platforms sometimes need an email address or geolocation data to function. However, they should no longer require users to allow their data to be shared with third parties for unrelated commercial research or promotional use. Mandatory arbitration clauses could also factor into an FTC determination of deception under Section 5. If the clause is not sufficiently noticeable and cognizable to the online gig economy user, the FTC should often find deception.

With regard to sharing information with the government, platforms should be obligated to provide certain safeguards for their users. Privacy policies should disclose whether the platform requires a warrant before providing information to law enforcement officials. When providing data to local governments for traffic or other research purposes, the FTC

should require gig economy platforms to de-identify information to avoid association with any individual user or device. They also could contractually prohibit the government from re-identifying the shared information for purposes other than research.

These theoretically proposed regulations would provide safety for users' information, while allowing for a partnership between municipalities and gig economy platforms. This would, in turn, help cities operate more efficiently and effectively, regulating the gig economy itself. The above guidelines should become mandatory for companies who wish to avoid a Section 5 determination of unfair or deceptive trade practices.

V. ALTERNATE SOLUTIONS

Companies typically treat FTC guidelines as rules likely to be enforced through Section 5 and are therefore incentivized to comply.[214] However, they lack legal standing for adjudication in federal civil or criminal court.[215] States could adopt similar guidelines to provide for a private right of action.[216] If states decline to implement such guidelines, however, further alternatives for regulating privacy in the gig economy exist. Congress could enact a statute giving the FTC jurisdiction to create a law in a manner similar to the COPPA structure. Moreover, local governments have jurisdiction to regulate certain aspects of gig economy companies under their transportation or housing codes. This could possibly include regulating privacy with respect to these types of companies.

A. *Congressional Statute*

Despite political predilections of the current Congress, a Congressional statute comparable to COPPA would be an alternative solution to the problem of privacy breaches in the gig economy. Distinguishable from COPPA, however, this Act would amplify privacy protection online to all adult Internet users, including gig economy users. In this situation, Congress would provide the FTC with jurisdiction to write a rule implementing the law.[217] The Congressional statute would state its prohibition on unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about users on the Internet.[218] In other

214 *See* Lipman, *supra* note 38.
215 *Id.*
216 *See* Butler & Wright, *supra* note 165.
217 *See The Children's Online Privacy Protection Act (COPPA): What Parents Should Know*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/kids-privacy-coppa (last visited Dec. 1, 2016).
218 15 U.S.C. § 6501 (1998).

provisions, it would define similar notice, choice and transparency requirements that the guidelines above delineate. The FTC would take action against companies that fail to comply and would issue reports to Congress assessing how companies comply with the law.[219]

This solution is unlikely at present for political reasons.[220] After repealing the FCC privacy rules, Congressional Republicans received significant public backlash.[221] In May of 2017, Representative Marsha Blackburn introduced the Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act of 2017.[222] The BROWSER Act would regulate ISPs and internet edge providers under a regime similar to the FCC privacy rules and would appear to alleviate to the complex problem of regulating internet privacy.[223] In reality, however, Blackburn has been criticized for introducing the bill only to appease constituents, without a genuine intent for it to pass.[224] Politically, both ISPs and internet edge providers oppose the BROWSER Act and therefore it is unlikely to pass through the House.[225]

B. *Local Laws Schema*

Instead, municipalities beyond the national political reach could become regulators. Local government power derives from the "home rule" principle that "local problems can best be solved by those familiar with them and most concerned with them."[226] Thirty–nine states employ Dillon's Rule, in which state legislature controls local government structure, methods of financing and authority to undertake functions.[227] States can, however, confer powers to local government, and traditionally have made local governments responsible for making laws that govern activities permitted on public land and use of infrastructure.[228] Local government furthermore typically is authorized

219 *See id.*

220 *See* Giuseppe Macri, *Republican Online Privacy Bill Struggles to Find Support*, INSIDE SOURCES (June 1, 2017), http://www.insidesources.com/republican-online-privacy-bill-struggles-find-support/.

221 *Id.*

222 *See* Press Release, U.S. Congressman Marsha Blackburn, Blackburn Introduces Bill to Protect Online Privacy, https://blackburn.house.gov/news/documentsingle.aspx?DocumentID=398295 (May 19, 2017) (on file with author).

223 *Id.*

224 *See* Macri, *supra* note 220.

225 *Id.*

226 James L. Magavern, *Fundamental Shifts Have Altered the Role of Local Governments*, 73 N.Y. ST. B. ASS'N 52, 53 (Jan. 2001).

227 *See* Jesse J. Richardson, Jr., Meghan Zimmerman Gough, & Robert Puentes, *Is Home Rule the Answer? Clarifying the Influence of Dillon's Rule on Growth Management*, BROOKINGS (Jan. 1, 2003), https://www.brookings.edu/research/is-home-rule-the-answer-clarifying-the-influence-of-dillons-rule-on-growth-management/.

228 *See Functions of Local Government*, GOOD GOVERNANCE GUIDE, http://www.goodgovernance.org.au/about-good-governance/role-of-local-government/ (last visited Dec. 1, 2016).

to provide a variety of services directly to its residents, including public safety services and economic development services.[229] States have also traditionally delegated general service delivery to local governments.[230] General service delivery includes a range of services, including public health, recreation, transportation, and public libraries.[231] Gig economy platforms often overlap with these services: Lyft provides an alternative to city buses, and Boatbound allows users to rent boats from owners to use recreationally.

Municipalities have authority to regulate aspects of the gig economy that relate to these traditional local roles.[232] For instance, municipalities in Texas are required by state law to regulate taxi transportation service.[233] As Uber and Lyft entered the market in San Antonio in 2014, its City Council adopted amendments to ordinances that provided permitting and other regulations for these transportation network companies.[234] These ordinances regulate safety, requiring vehicle inspections, insurance, and permit qualifications.[235] This translates easily from the city's more traditional role of regulating the use of infrastructure, specifically taxis in this case.

While privacy is not a traditionally local role, local governments might have authority to regulate privacy where it becomes a safety concern for its citizens. Conceptually, local governments could draft ordinances that lay out similar requirements for gig economy companies' disclosure of PII. However, this is a fairly unrealistic alternative at this time, since privacy law has traditionally been codified at the state or federal level.

VI. CONCLUSION

The gig economy will likely continue to flourish as these platforms provide instantaneous service to users and workplace flexibility to contractors. Customers are willing to provide large swaths of PII to these companies. The gig economy platforms can sell the personal data to third parties, as long as they disclose the amounts of data they share in their privacy policies. What is actually done with this data for the most part remains uncertain. However, most gig economy companies fail to protect data against law enforcement agencies with warrant requests; Uber has, in the past, uploaded blog posts describing their use

229 *See What Do Local Governments Do?*, N.Y. DEP'T OF STATE, DIVISION OF LOC. GOV'T SERV., http://www.dos.ny.gov/lg/localgovs.html (last visited Dec. 1, 2016).
230 *See* Functions of Local Government, *supra* note 228.
231 *Id.*
232 *See* Cardozo, Opsahl & Reitman, *supra* note 117.
233 *See* Greater Houston Transp. Co. v. Uber Tech., Inc., 155 F. Supp. 3d 670, 677 (S.D. Tex. 2015).
234 *See* SAN ANTONIO, TEX., CODE OF ORDINANCES ch. 33, art. IX, § 987 (2015).
235 *Id.*

of data for social research, and universities studying discrimination in the gig economy likely receive their data from the companies themselves.

In the past, real-world privacy and security interests were appropriately balanced by the law. People could physically see when they were under surveillance. Now, however, surveillance measures are buried deep within extensive privacy policies. Users have no bargaining power to request that their data not be shared for advertising or research purposes. They must comply with the totality of the company's demands or be denied a convenient service. While the impending political climate remains uncertain for the privacy realm, a report from the FTC could incorporate currently active privacy rules from California, and the EU, as well as the repealed FCC privacy rules and the recently introduced BROWSER Act. This would provide gig economy consumers with more choice, transparency, and stronger bargaining power. While this solution is by no means flawless, it would provide companies and states a strong starting point for implementing fairer and less deceptive standards for personal data collection. As privacy issues materialize in every online context, the gig economy sphere could revolutionize online consumer protection law.

Casey Thomas[*]

[*]J.D., Benjamin N. Cardozo School of Law, 2018. B.S., Texas State University, 2012. I'm grateful to my Cardozo friends & family for their help with this note. "Hey dad. Hi mom."