DATA IN THE ON-DEMAND ECONOMY

Privacy & Security in Government Data Mandates

December 2015

G.S. Hans

Policy Counsel and Director, CDT-SF

cdt

I. Introduction

If you want a luxury car to take you across town to impress a date, you can get it in five minutes. Need a report done at your house urgently? There's an app for that. Looking for a place to stay, but want something different than a hotel? Easy. And of course, if you are willing to give people a ride, repair a broken dishwasher, or make your guest room open to a stranger, you can easily make your service available. The "on-demand" economy is here, and there is unquestionable demand from both those seeking services and those supplying services.

Today, innovative technology companies are entering into new areas of the economy — including travel, transit, utilities, and healthcare — introducing new players into industries that have historically been dominated by a few companies. These developments have been referred to as the sharing economy, the gig economy, or, as in this paper, the on-demand economy.

Many of the sectors these companies are disrupting are often highly regulated, with detailed operating requirements, complex regulations at the state and local level, and extensive oversight by governmental agencies. For technology companies that have historically not operated in highly regulated areas, this presents a host of new challenges; for agencies, the difficulties in regulating companies that are not accustomed to this type of governance are equally as striking.

This new instability has led to many proposals designed to update existing laws and regulations for technology service providers. These proposals frequently mirror the current requirements for companies to provide information to the government about operating procedures. However, because technology companies often have far more personally identifiable information (PII) detailing customers (including, for example, names, addresses, email addresses, IP addresses, location information, and financial information), all of which may be part of a single customer record, a mandate for companies to provide information to the government about operations could, if not narrowly crafted, result in massive transfers of sensitive customer data to the government.

While the government might need some categories of information about individuals for specific reasons, given the massive amount of data generated by on-demand technology companies, data transfers for broad purposes raise a host of privacy and security purposes. The Center for Democracy & Technology (CDT) believes in the need for regulations to both protect consumers and ensure compliance with the law by all companies operating in a specific market. However, such regulations need to be carefully drafted to collect only necessary consumer information for delineated purposes, and must prescribe security standards and retention limits for the data. This paper discusses both the policy concerns surrounding proposals geared toward on-demand technology companies, as well as provides recommendations for how to create regulations that promote governmental goals while preserving consumer privacy — and enabling ongoing innovation.

II. Key Terms and Issues

The core issues that arise when dealing with requests from civil agencies are similar to the issues involved with law enforcement requests, though the calculus may be different in some cases. CDT believes the key questions, based on Fair Information Practice Principles (FIPPs) that policymakers, companies, and citizens should ask are[1]:

- **Legal Basis of Collection:** under what authority is data collected?
- **Duration of Access:** how long are companies required to provide data to agencies? How long is data retained?
- **Scope of Collection:** what categories of data, including sensitive data, are transmitted? Is the data de-identified to any extent?
- **Security of Transmission:** is the data being transmitted in a secure way, using encryption technologies?
- **Secondary Uses:** is the data collected used for other purposes besides its primary purpose?
- **Transparency:** how do governments and companies let individuals know about the frequency, type, and nature of data requests? Do individuals have access to this data?

In this paper, regulatory access is used to refer to agencies' collecting data from companies pursuant to statutory provisions or administrative rules (e.g. for oversight, licensure, or other regulatory actions). It's useful to distinguish this from enforcement actions, where agencies undertake specific investigations of possible violations, respond to complaints from citizens, or otherwise enforce provisions of a statute or rule. Enforcement actions are naturally involve more intrusive, yet more targeted data collection and are outside of the scope of this paper.

III. Case Studies

Two recent proposals demonstrate the issues raised by data sharing in the on-demand economy, and the challenges posed by attempting to pass new regulations.

A. Proposed 2014 New York Taxi and Limousine Commission Regulations

In late 2014, the New York Taxi and Limousine Commission (TLC) proposed revisions to regulations governing cabs and dispatchers.[2] The proposal required dispatchers to send information on the date, time, and location of *all* customer

[1] These questions draw on the organizing framework provided by the Fair Information Practice Principles, baseline information privacy standards which provide a useful lens to analyze these issues. *See, e.g.,* U.S. Department of Homeland Security Privacy Policy Guidance Memorandum, Hugo Teufel III (Dec. 29, 2008), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[2] *See* New York City Taxi and Limousine Commission, Notice of Public Hearing and Opportunity to Comment on Proposed Rules (Sept. 12, 2014), *available at* http://www.nyc.gov/html/tlc/downloads/pdf/proposed_rule_fhv_dispatch_rules.pdf.

pickups to the TLC. Given the sensitivity of location information, this proposal raised a number of privacy and security concerns. It was not confined to specific investigations, but rather mandated the transfer of data *en masse* to the government. The proposal did not detail why it was necessary to change the existing system, which merely allowed the TLC to investigate records when necessary. The shift from allowing access to mandating mass transmission potentially imperiled the privacy of many individuals in the New York area.

Additional concerns were raised due to the possibility of re-identifying TLC data to identify specific individuals and their usage patterns. Just prior to the TLC proposals, a publicly released data set was analyzed and used to determine the usage patterns of specific celebrities.[3] As a result, it's clear that any new program that the TLC instituted that collected data regarding the usage patterns of specific customers would need to be extremely careful in its drafting in order to avoid privacy and security pitfalls.

While the proposal was limited in scope, it would have created a large government database containing records on customer movements. The particular language at issue was as follows:

> *(a) Required Information. A Base Owner must make sure that the following records are collected and transmitted to the Commission in a format, layout, procedure, and frequency prescribed by the Commission:*
>
> *(1) With respect to all dispatched calls:*
>
> *(i) The date, the time, and the location of the Passenger to be picked up*
> *(ii) The Driver's For-Hire License number*
> *(iii) The dispatched Vehicle's License number*
> *(iv) The TLC License number of the For-Hire Base that dispatched the Vehicle*
> *(v) The TLC License number of the For-Hire Base affiliated to the dispatched Vehicle*

By requiring the transmission of data on an unspecified basis (which could be potentially daily, if not more frequently), the proposal would have created a large database containing sensitive location information. The proposed regulations also failed to specify a particular need for the data other than general regulatory supervision. The proposal required only transmitting pick-up location (not drop-off location) to the Commission; however, because it was not clear why the TLC needed this information on an ongoing basis, it was not clear that future amendments wouldn't mandate transmission of yet more information. The lack of an explanation of the need for constant data transmission heightened privacy concerns, as well as

[3] *See* J.K. Trotter, *Public NYC Taxicab Database Lets You See How Celebrities Tip,* Gawker (Oct. 23, 2014), http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546.

fears of future unexpected mandated transfers or sharing with other governmental agencies.

Furthermore, because the proposal did not cabin what data categories would be collected, it opened the door to future expansion of data collection. While the data collected did not identify a particular user, the language of the proposal would not have prevented the TLC from suggesting subsequent changes that would have required the transfer of identifying information on individual customers. The language also failed to account for security in transmission or storage of the data, such as encryption. The prevalence of data breaches underscores the need for explicit language addressing security in data collection laws and policies. Relatedly, the language did not contemplate de-identification measures that the Base Owners should have taken into account prior to transmission to the TLC, or how the TLC planned to address potential open government requests under New York's Freedom of Information Law (FOIL) that could reveal customer information gathered under the regulation.

B. Proposed 2015 Amendment to San Francisco Short-Term Rental Ordinance

In 2014, San Francisco enacted a law governing the use of short-term rentals, attempting to promote responsible housing practices and control skyrocketing rents within the city. The original legislation established that the city's Planning Department would receive information on specific units from individuals who were offering short-term rentals. However, critics observed that the law was ineffective as originally enacted.

Supervisor David Campos suggested various amendments to the law in order to increase its effectiveness.[4] To his credit, some amendments were privacy protective; for example, one revision would have redacted names and addresses in a public database of short-term rentals. However, the proposal failed to describe security standards governing mandated data transfers from companies to the government.

One element of Campos' proposals raised serious issues with the current state of intermediary liability protection under Section 230 of the federal Communications Decency Act. Under existing San Francisco law, a "hosting platform" was defined as "a person or entity that provides a means through which an Owner may offer a Residential Unit for Tourist or Transient Use." However, this definition wasn't limited to sites like Airbnb or VRBO, but could, for example, include social networks like Facebook or Twitter, which could theoretically be used to offer a residential unit for short-term use. The problematic language was as follows:

> *(C) Prior to listing a Residential Unit within the City to be rented for Tourist or Transient Use, a Hosting Platform shall verify with the Planning Department*

[4] City of San Francisco Administrative Code—Short-Term Residential Rentals, File No. 150295, *available at* https://sfgov.legistar.com/View.ashx?M=F&ID=3710408&GUID=BB00F331-0B2F-4A28-AE48-3117B03E854E.

that the Residential Unit is listed on the Registry. A Hosting Platform shall not provide any such listing unless the listing includes a registration number and the Hosting Platform has verified that the Residential Unit is listed on the Registry. Additionally, if a Hosting Platform has information that a Residential Unit has been rented for Tourist or Transient Use for more than 60 days within a calendar year, the Hosting Platform shall immediately remove such listing from its platform.

Under Supervisor Campos' proposal, hosting platforms would have to pre-review any listings, verifying that the listing was part of the city's centralized database and that it had not been rented for more than sixty days within the calendar year. But if an individual posted a public Tweet asking for short-term renters to stay at a San Francisco apartment without including the address, Twitter (which would have had no way of verifying any information before the Tweet was posted), would be in violation of the law, despite the fact that the service wasn't designed to facilitate such short term rentals.

Such a violation would impose a form of intermediary liability under local law, which is expressly precluded by the preemption provisions of Section 230, which preempts similar state and local laws governing intermediary liability. While this may seem like an overly technical point, ensuring that regulations are carefully drafted is necessary to minimize conflicts with superseding federal law. Due to these and other concerns, the proposal was eventually dropped.

IV. Policy Discussion and Recommendations

Whenever governments propose mandates that collect personal data from individuals or companies, concerns inherently arise regarding the scope of such mandates, as well as whether privacy and security measures are sufficiently addressed. Government collection, use, and retention of information relating to individual users (which in some cases may include personally identifiable information) creates challenges for individual privacy. For example, agencies may use information for unpublicized secondary purposes, or could share information with other governmental entities without notice. As we have seen in cases like the Office of Personnel Management (OPM) breach,[5] governmental databases present tempting targets for unauthorized third-party access, creating security risks and imperiling the privacy of all individuals for whom the collecting agency has a record. Given that reality, the collection of data by government agencies should be done only for specific reasons, with clear guidelines for privacy, security, and oversight, created to protect individuals and promote trust.

Multiple stakeholders – governments, companies, and consumer advocates – have interests in this issue. For governments seeking to protect individuals and uphold

[5] *See* David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, N.Y. TIMES (June 4, 2015)*, available at* http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html.

existing regulations, the rapid growth of companies that collect data on individuals pertaining to their daily lives has led to increased interest in understanding the operations of those companies. Some of this interest comes from wholly understandable sources — for example, the need to ensure compliance with existing law or a desire to use company data for public research purposes. However, some regulators may be interested in collecting data from new companies due to the fears of existing firms that their business models may be disrupted. This could lead to a mandate of massive data transfers, creating barriers for newer, tech-focused entrants to enter an established market.

In addition to the regulatory burden, when considering these data transfer mandates companies must also consider the impact of those transfers on their customers' privacy. As such, companies that encounter legislative or regulatory proposals should consider the following issues when determining how to respond:

- **Scope of Collection**: What categories of data are being collected by the government? What changes are being made to the scope of data collection by the legislator or regulator?
- **Secondary Uses**: Are there limitations on the use of data by the agency and its sharing with other entities?
- **Transmission**: Are security standards prescribed, both for transmission and storage, once in government possession?
- **Duration of Access**: What retention limitations are prescribed?
- **Transparency**: What accountability mechanisms (internal or external) are prescribed (e.g. transparency reporting, internal auditing)?
- **Open Government**: How do the regulations contemplate potential freedom of information requests concerning databases containing consumer data?

Proposals that proactively address these issues are likely to be more secure, capable of better protecting privacy and creating useful (and effective) industry oversight.

In addition to the specific recommendations below, facilitating public comment is one long-term method to achieve better outcomes. Consumers are interested in protecting their own privacy; they provide the most effective voices on why a particular proposal might negatively affect them. When proposals are introduced, companies should publicize them. They can work with consumer advocates to draw attention to problematic proposals that fail to protect individual users because of privacy and security concerns. For example, CDT has previously highlighted proposals that fail to include provisions for secure transmission of data; an obvious concern given the possibility of unlawful access and data breach. This has helped raise awareness with policymakers for the unforeseen consequences of broad language. Many proposals originate with state and local agencies and lawmakers, in venues where privacy and civil liberties advocates may not have a strong presence. By publicizing proposals, companies can ensure that advocates have more opportunity to correct problematic elements.

A. Legal Basis and Scope of Collection

When evaluating whether the collection of information is appropriate, the following issues should be considered: statutory/regulatory authority, categories of data, and de-identification measures. As a fundamental matter, agencies should collect data only when authorized by a specific regulation or law. Informal requests for data without an underlying basis, even for ostensibly benign purposes such as de-identified research, should be disfavored, given the lack of oversight for such requests and lack of public transparency. Some companies may have ongoing relationships with agencies that might make such requests relatively easy to fulfill. However, if informal, unauthorized requests become the norm, it will be more difficult for users to gain clarity about how their data is used, or to have confidence that it is protected in a systematic way. Such informal requests have been criticized in other contexts for their lack of formality and appropriate process.[6]

Additionally, the content of data that is transmitted is important to cabin. Companies that collect information from users possess sensitive information, including real names, credit card data, email addresses, and telephone numbers. In the case of ridesharing, smart grid, and short-term rentals, they may also collect home addresses, route patterns, appliance information, and demographic information. As a result, any legislative or regulatory proposal that requests content from companies should be narrow in order to avoid "sweeping up" unnecessary categories of data.

For example, in New Orleans, platforms that allow users to hail cars through smartphones are required to maintain records and provide them to the city.[7] The New Orleans ordinance states:

> *"Every [transportation network company (TNC)] shall keep daily records including all trip requests, complaints, accepted trip requests, daily application sign-in and sign-out logs, vehicle collision reports, service response time reports, reports of crime against TNC drivers and passengers, lost property reports, and TNC vehicle identification information. Such records may be maintained electronically and shall be preserved for a period of not less than two years and be available for examination by the director of safety and permits upon request. Failure to maintain such records or provide them upon request shall be grounds for the suspension and/or revocation of a TNC permit."*

While the retention period of records for two years is far longer than CDT's recommendation of retention for 30-60 days, the data required to be stored does not

---

[6] *See, e.g.,* U.S. Department of Justice, Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records (Jan. 2010), *available at* https://oig.justice.gov/special/s1001r.pdf

[7] Ordinance, City of New Orleans (Feb. 26, 2015), Calendar No. 30,617, *available at* http://cityofno.granicus.com/MetaViewer.php?view_id=3&event_id=509&meta_id=277915.

tie location information to individual accounts — a key protection. Moreover, the data collected clearly demonstrates the city's interest in minimizing accidents, crime, and tracking lost property, rather than collecting a mass of data without a specific purpose.

Any proposal that seeks to collect data should carefully delineate what data categories are necessary for the intended purpose of the proposal, and what categories are not relevant. For example, in the context of ridesharing in order to research usage patterns, it may be relevant to collect information on the number of trips originating in a particular ZIP code. However, there isn't a need for information on individual trips, as aggregated data would be sufficient for the intended purpose. Some agencies are thinking proactively on how to appropriately request data (or enter into voluntary arrangements with companies for data sharing), demonstrating that these relationships need not be adversarial.[8]

Two categories of data deserve special attention. The first is financial data where a breach could lead to identity theft and other severe financial repercussions. Companies routinely collect financial information from customers; however, it is difficult to envision to what ends governmental agencies could apply such data. Therefore, companies should proactively work to remove financial data from records that are transmitted to governmental agencies, as such data could, if breached or misused, cause lasting damage to consumers.

A second category — location data — can also reveal a great deal of information about an individual. Several companies that collect data from consumers (for example, ridesharing or short-term rental companies) have to collect location data in order for their services to operate. As has been well-documented, location data — especially when aggregated over time — can be particularly revealing about an individual's movements and routines.[9] Indeed, it is for this reason that it may be an appealing research corpus for agencies. The challenge for agencies is to ensure that such data retains research value, while protecting individual privacy.

Providing unredacted sensitive financial, location, residential, or demographic data to governmental agencies should *not* be the default. If legislative or regulatory proposals mandate transmission of this data, companies should work to remove or limit the scope. At the very least, any personally identifiable information should be de-identified to the greatest extent possible (for example, through

---

[8] For example, in January 2015, Uber entered into an agreement with the City of Boston to share de-identified data on a quarterly basis, including timestamps for the beginning and end of trips; distance traveled, and ZIP codes of pick-up and dropoff locations. *See* Justin Kintz, Driving Solutions To Build Smarter Cities (Jan. 13, 2015), http://newsroom.uber.com/boston/2015/01/driving-solutions-to-build-smarter-cities/; Douglas MacMillan, *Uber Offers Trip Data to Cities, Starting with Boston*, Wall St. J. Digits (Jan. 13, 2015), http://blogs.wsj.com/digits/2015/01/13/uber-offers-trip-data-to-cities-starting-in-boston/.

[9] *See, e.g.,* Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), *available at* https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

pseudonymization). Removing identifying information is not only privacy protective, but also works to reduce the likelihood of future re-identification.

Companies should therefore de-identify an individual user's location data to the extent possible, while still retaining useful or relevant information for agencies, in advance of transmission. For example, data on an individual's pickup location could be confined to ZIP code location (rather than GPS coordinates), in order to protect user privacy while still providing general geographic information with some specificity. The challenges of de-identification have been well documented; and complete de-identification may not be possible.[10] However, companies are more likely to have access to the latest and most innovative de-identification techniques, and in general have more experience in removing identifying information from data sets than government agencies. They should therefore still attempt to de-identify data while recognizing the limitations of this process.

B. Duration of Access and Security of Transmission

The methods and frequency by which data is transmitted is also an important issue. The number of high-profile data breaches demonstrates the critical nature of data security concerning individual data. Accordingly, proposals that allow government agencies to collect data from companies must prescribe security standards in order to protect the data to the greatest extent possible, both while in transit and while stored.

Additionally, legislative or regulatory proposals should *not* require data transmission on an ongoing basis. Given the volume of data that companies collect on individuals, it is unlikely that any government agency would be able to meaningfully analyze user data unless it was transmitted monthly (or at a longer interval). Real-time or near-real-time transmission could also enable tracking of individual movements (in the context of ridesharing or short term rentals), which companies should oppose given the invasiveness of such tracking. This type of transmission would also make de-identification and other privacy protecting techniques more difficult. One other option would be for companies to set up a "data room" to allow regulatory agencies to view data held by the company for oversight or compliance purposes. This would allow for data inspection without mandating data transmission.

In San Francisco, the short term rental law requires the person who rents ot the space — not the platform — to provide information to the city "upon written request."[11] Rather than require a constant transmission, "the Permanent Resident shall submit a report to the Department on January 1 of each year regarding the number of days the Residential Unit or any portion thereof has been rented as a

[10] *See* Arvind Narayanan & Edward W. Felten, *No Silver Bullet: De-Identification Still Doesn't Work* (July 9, 2014), http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

[11] San Francisco Board of Supervisors, Ordinance No. 218-14, Administrative, Planning Codes — Amending Regulation of Short-Term Residential Rentals and Establishing Fee (File No. 140381), *available at* http://www.sfbos.org/ftp/uploadedfiles/bdsupvrs/ordinances14/o0218-14.pdf.

Short-Term Residential Rental since either initial registration or the last report, whichever is more recent, and any additional information the Department may require to demonstrate compliance with this Chapter." This allows the city to receive information about lawful compliance without mandating that permanent residents or platforms transmit data on an ongoing basis. By limiting the frequency of collection, the potential of tracking individual movements is lessened, as are security risks.

The security perils of constantly transmitting data in real time — or even on a daily or weekly basis — are obvious. Unauthorized individuals may gain access to data as it is transferred, as well as when it is stored. The more frequent the transmission of data, the more likely that such unauthorized access will occur.

Regardless of the frequency of transmission, consumer data should be sent from companies to agencies securely. At the very least, consumer data should be transmitted using an authenticated, encrypted transmission method.[12] The necessity of transferring data with strong security measures has been re-emphasized by the recent series of high profile data breaches that multiple large companies and government agencies have suffered.[13]

Security must also be taken into consideration by regulators when proposing agency collection and storage of data. Government agencies must ensure that any data they collect from companies concerning individuals is given the same security protections as any other form of data, and that such data is retained only for a limited period.

Distressingly, few recent legislative and regulatory proposals discuss security standards for transmission. In Seattle, transportation network companies are required to submit quarterly reports to the city.[14] However, the default option is to send the reports by unencrypted email; the only secure option is to upload data through a Microsoft Sharepoint site. Proposals should specifically state how to securely transfer data to the government, preferably through a system provided by the government that allows for secure file transfers.

---

[12] For example, best practice at the time of writing is to use a strong encryption transport protocol, such as Transport Layer Security (TLS) v1.2. However, in addition to choosing a strong encryption transport protocol, the encrypted protocol must be configured specifically to not use forms of weak encryption. To accomplish this and properly configure a TLS communication to use only good forms of strong encryption, operators should consult a frequently updated reference that describes proper configuration, such as: "SSL/TLS Deployment Best Practices," Qualys SSL Labs, *available at* https://www.ssllabs.com/projects/best-practices/ (last visited October 28, 2015). (Authentication is built into the TLS protocol, using certificates from certificate authorities that are validated at the time of transmission.) Note that TLS is not the only choice for secure transmission and there are other methods that provide similar authenticated encryption, e.g. the Secure File Transfer Protocol.

[13] *See, e.g.,* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), *available at* http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html; Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES (Jan. 10, 2014), *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html

[14] Data Reporting, City of Seattle, http://www.seattle.gov/business-regulations/taxis-for-hires-and-tncs/data-reporting. These breaches affected stored data, rather than data in transmission, but the potential for such attacks exist (such as spoofing or Man in the Middle attacks).

C. Secondary Uses

Privacy and security concerns do not conclude following the transmission and storage of data to governmental agencies. Most obviously, governments should use the data they collect from companies *only* for the purposes specified in legislative or regulatory language. To that end, companies, advocates, and government agencies should work to ensure that any legislative or regulatory proposal contains *specific* language concerning the uses to which data collected from companies will be put. There should *not* be open-ended language allowing governmental agencies to use data for any purpose, or for unspecified purposes. Data use agreements can be one effective method for preemptively circumscribing the limits of what corporate-provided data can be used for by the government – for example, by proactively asserting that data collected by a government agency, like a transit or housing authority, will not be shared with other agencies or law enforcement entities.

In Portland, Oregon, the regulations governing private for-hire transportation stipulate that "Except as otherwise required by law, information submitted to the Administrator under this Section can only be used within the City government. Such information may not be released to the public except in aggregate form."[15] This is a helpful framing of limitations on secondary uses, but could be more explicit in banning the use of data collected by agencies for criminal law enforcement purposes. However, the clear ban on non-aggregated release of information to the public is a strong privacy protective measure to minimize potential re-identification of individuals that may result from improperly broad freedom of information requests.

Given the sensitivity of PII, location data, and financial information, a regime without limitations on secondary uses allows access and application of data in ways that an individual may not realize or approve of. Without appropriate limitations and oversight to ensure compliance with those limitations, user data can be used for unauthorized or illegal purposes; to track individuals or suppress speech; or to deny credit, housing, or benefits. For example, by collecting unique user identifiers (such as email addresses) and location information from ridesharing companies, government agencies could track individual user movements, and potentially share the information with law enforcement entities without use restrictions.

This is of particular concern given the easy replicability of consumer data. Once an agency obtains data from companies, it can be very easy to both reproduce and transmit that data to other governmental agencies, including law enforcement and national security agencies, without a record or rigorous oversight. The Fourth Amendment's protections – which have been repeatedly extended by the Supreme Court to new technologies[16] and large databases[17] – signal the importance of such limitations on government use.

---

[15] City of Portland, Chapter 16.40, Private For-Hire Transportation Regulation, https://www.portlandonline.com/auditor/index.cfm?cce_28593_print=1&c=28593

[16] *See, e.g., Riley v. California*, 573 U.S. ___ (2014).

D. Transparency

Any legislative or regulatory proposal would ideally contain provisions for transparency reporting and auditing on the government. Agencies and companies should detail how frequently the government requests data from companies, and regulations should provide internal government oversight mechanisms that can improve compliance.

Companies can take up the mantle of transparency and auditing through their own responses to regulatory access requests. Companies have used transparency reports to document takedown requests for intellectual property, criminal law enforcement, and national security requests.[18] These reports are vital in illuminating governmental practices in the absence of transparency by law enforcement and security agencies. Companies should issue transparency reports on a periodic basis (ideally quarterly, or more frequently),[19] and detail the origins of a transmission of data; the data fields and volume of data transmitted; whether the data was de-identified, and to what extent; and the security measures employed.

The value proposition for businesses is clear in the context of transparency reporting. First, it communicates to users that the company is upfront regarding how it interacts with law enforcement, increasing user trust in the relationship with the service provider. Second, it shines the light on how often, how frequently, and from what jurisdictions data is being sought, allowing for more effective advocacy.[20]

The value for consumers is equally clear: given that state and local agencies may be creating laws and rules that require companies to turn over data, it can be difficult for an individual consumer to understand just how widespread these practices are. Individuals may not be able to determine which agencies are requesting data (especially given the range of substantive areas and governmental levels involved), and companies, as the recipients of requests, can more easily aggregate them and provide detailed statistics on the frequency, type, and origin of data requests. As the target of such regulations, companies are better placed to provide information on the prevalence of such programs, and therefore, to encourage citizens to advocate for changes to overbroad or poorly managed government access programs.

Finally, government entities can also work to analyze how new programs affect individual privacy. As required by law, the federal government currently conducts

---

[17] *See, e.g., City of Los Angeles v. Patel*, 576 U.S. ___ (2015).

[18] *See, e.g.,* Apple, Report History, http://www.apple.com/privacy/transparency-reports/; Google, Transparency Report, https://www.google.com/transparencyreport/.

[19] As users are not equipped to track what state and local jurisdictions are requesting data, and given the quickly changing pace of regulation and legislation on the local level, companies would best serve the transparency cause by releasing reports on a quarterly basis in order to effectively document the current state of state and local involvement in these issues.

[20] *See, e.g.,* Meghan Kelly, *Why the Transparency Report is Necessary in the Fight for Privacy*, VentureBeat (Sept. 12, 2013), http://venturebeat.com/2013/09/12/transparency-reports/.

privacy impact assessments before instituting new forms of data collection.[21] State and local governmental agencies should consider conducting similar assessments. In doing so, they can demonstrate that they have proactively analyzed the effects of new programs on individual privacy, and that they have determined that their interest in company data is for legitimate purposes, that programs follow enacted statutory and regulatory provisions, and that internal oversight is an institutional priority.

The investment in producing transparency reports is non-trivial; however, many major technology companies already produce such reports for criminal law enforcement and national security data requests. By utilizing similar infrastructure, companies could create similar reports for civil agency data requests. Such reports should be updated periodically, and should be publicized by companies in order to draw attention to the existence of such requests, which may not be obvious to individual consumers. Companies should highlight transparency reports through various channels when they are updated, and provide information to individuals when users sign up for a service, and periodic subsequent notifications.

V. Conclusion

The challenges posed by regulating new entrants to existing markets are significant, especially when the entrants are innovative technology companies offering on-demand services. With both consumers and service providers driving these changes, the need for laws and governmental regulations to promote consumer protection is clear. What is equally clear is that such laws and regulations need to be drafted thoughtfully, with consideration given to the privacy and security of consumer data that companies may collect through the course of business. In order to promote public needs, legislators and regulators must assure the public that their data is kept safe through privacy protections and secure transmission.

These recommendations offer guidance for governmental entities and companies when considering specific language proposals; however, new advances both in technology and changing needs from the government may require further examination and deliberation by businesses, regulators, and consumer advocates. Yet the need to protect consumer data and promote privacy and security is constant — no matter what new technologies may develop in the future.

[21] *See, e.g.,* United States Department of Justice Office of Privacy and Civil Liberties, Privacy Impact Assessments: Official Guidance (Mar. 2012), *available at* http://www.justice.gov/opcl/docs/2012-doj-pia-manual.pdf.