Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Data Sharing Between Public and Private Sectors

When Local Governments Seek Information from the Sharing Economy

Discussion Paper | May 2023

CIPL DISCUSSION PAPER:
Data Sharing Between Public and Private Sectors

When Local Governments Seek Information from the Sharing Economy

4 May 2023

I. INTRODUCTION

Governments at the state, county, and municipal levels have become increasingly interested in the treasure troves of local data amassed by the sharing economy. A growing number of localities are requesting (and sometimes mandating) that data collected by sharing-economy businesses—providers of ride-hailing services, short-term rentals, and other peer-based transactions—be shared with the localities themselves for a wide range of governmental purposes.

To be clear, such data-sharing requests are often not in the context of law enforcement or national security matters. Rather, those introducing them describe them as efforts to further the public interest or promote a public good. Sometimes, however, sharing requests are overly broad and not specifically tailored to the purported public interest. And given that these requests are sometimes made binding via local ordinances and regulations, they may conflict with companies' pre-existing contractual or legal compliance obligations. In some circumstances, the public sector may be unfamiliar with private sector privacy and data security obligations, and to the extent that similar duties do not apply to the local government, the public sector may lack systems or controls to address generally recognized data protection principles.

To mitigate these concerns, the Centre for Information Policy Leadership (CIPL)[1] recommends that both the public and private sector adopt demonstrable accountability measures to foster responsible data-sharing practices and beneficial data uses while respecting individuals' privacy rights and businesses' legal obligations. Such measures will foster public trust in any data sharing between public and private sector entities.

II. DATA-SHARING INITIATIVES

Localities frequently adopt data-sharing policies and regulations for the stated purpose of benefiting the community. Promoting safety, ensuring housing affordability, and reducing traffic congestion are among the common rationales presented.[2]

---

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] A mobility initiative by the City of Los Angeles seeks not only to "ensure [that] transportation options are safe," but also to "deliver on the City's goals of socioeconomic and racial equity." See On-Demand Mobility

For example, Atlanta's regulations pertaining to its "Shareable Dockless Mobility Program" are designed in part to help the city "make data-driven decisions prioritizing public safety and accessibility."[3] Regulations in Massachusetts require ride-hailing services to collect and report certain information "in furtherance of the public interest, safety, and convenience."[4] A Seattle ordinance relating to short-term rentals seeks to "preserve the availability of housing for long-term rentals …, reduce the negative effects on affordable housing, and protect the safety and liability of residential neighborhoods."[5]

Other regulations seek data to promote and measure compliance or as a precondition for the issuance of a license. Toronto's vehicles-for-hire regulation cites "licensing enforcement" as the reason why ride-hailing companies must notify customers that their personal information might be disclosed to the city.[6] Auckland's Rental Micromobility Code of Practice requires e-scooter and e-bike rental operators to share mobility data with the city in order to maintain an operating license.[7] Amsterdam requires hosts of Airbnb and Booking.com rentals to inform the city each time they rent their property to ensure that property owners comply with the city's permit requirements.[8]

In response to local ordinances like the one in Amsterdam and hoping to streamline data sharing initiatives across the single market, the European Commission recently introduced a proposal for an EU-wide regulation mandating the sharing of data by short-term rental companies.[9] In particular, Articles 8-12 of that proposal specify that providers of online short-term rental platforms would transmit on a monthly basis activity data per unit, together with the corresponding registration number as provided by the host and the URL of the listing. The transmission would take place via machine-to-machine communications to a Single Digital Entry Point of the Member State where the property is located. Competent authorities would be permitted to access the data only for purposes of monitoring compliance with the registration requirements and implementing rules pertaining to short-term accommodation rental services.

Rules and Guidelines 2021, City of Los Angeles, available at https://ladot.lacity.org/sites/default/files/documents/final-year-two-rules-and-guidelines-updated-sla.pdf.

[3] Administrative Regulations for Shareable Dockless Mobility Device 2021 Annual Permit Holders, City of Atlanta Department of Transportation, (as updated Apr. 5, 2021), Section I, available at https://www.atlantaga.gov/home/showpublisheddocument/50629/637532367525500000.

[4] 220 CMR 274.01.

[5] Seattle City Council, Ordinance 125483, AN ORDINANCE relating to short-term rental uses and bed and breakfast uses, available at http://seattle.legistar.com/View.ashx?M=F&ID=5707711&GUID=E803804A-1110-4EC9-BD41-40EA618EF871.

[6] "A [Private Transportation Company ('PTC')] shall disclose to the public … [n]otification that personal information collected by the PTC may be disclosed to the City for the purposes of licensing enforcement when the passenger obtains transportation services in Toronto." Toronto Municipal Code, Chapter 546, Licensing of Vehicles-For-Hire, §546-118(A)(5), available at http://www.toronto.ca/legdocs/municode/toronto-code-546.pdf.

[7] Micromobility Code of Practice Version 2.0, Auckland Council, available at https://www.aucklandcouncil.govt.nz/licences-regulations/Documents/rental-micromobility-code-of-practice.pdf.

[8] Vakantieverhuur melden (Report holiday rentals), Gemeenet Amsterdam (Township Amsterdam), available at https://www.amsterdam.nl/wonen-leefomgeving/wonen/vakantieverhuur/vakantieverhuur-melden/.

[9] Proposal for a Regulation of the European Parliament and of the Council on data collection and sharing relating to short-term accommodation rental services and amending Regulation (EU) 2018/1724 (STR Regulation), available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2022:571:FIN.

Stephen Larrick,[10] a former research fellow at the Harvard Kennedy School's Belfer Center, has tracked these and other developments on a website[11] that compiles data sharing laws and regulations from local governments. He summarized his findings in a report,[12] noting that prior to 2018 only a handful of local governments had policies requiring sharing economy platforms to share operational data with municipal officials.[13] Since then the emergence of micromobility—in particular, the growth in bikeshare and e-scooters[14]—has prompted cities to require data sharing as a precondition for certain kinds of platforms to operate within their jurisdictions.[15]

Larrick has coined the term "platform urbanism data sharing" ("PUDS") to refer to this growing form of data sharing.[16]

In the U.S., the trend has extended to the state level. For example, a proposed bill in Massachusetts would require third-party delivery services to provide to the commonwealth's transportation division, in a format approved by the division, highly detailed data related to deliveries, including but not limited to the mode of transportation for each delivery, the time spent to pick up the delivery order, and the total number of minutes parked while picking up orders.[17]

In an effort to support fair and competitive digital markets, data sharing initiatives have moved beyond the business-to-government (B2G) context to include business-to-business (B2B) data sharing practices as well.[18] The EU Data Act,[19] for example, would provide the means for end users of connected devices to have their data shared with third parties such as aftermarket service providers. It would also create the means for public sector access to private sector data in exceptional situations, such as public health emergencies or natural or human-induced disasters.[20]

While EU-wide initiatives attempt to account for pre-existing obligations that attach to data, local data sharing requests rarely do. Often, local regulations do not address consumer privacy rights, business obligations related to those rights, or even the local government's own obligations after data is shared.

---

10 Stephen Larrick, 2021-22 Fellow, Technology and Public Purpose Project, Harvard Kennedy School, Belfer Center for Science and International Affairs, available at https://www.belfercenter.org/person/stephen-larrick.

11 Platform Urbanism Data Sharing (PUDS) Policy Hub, available at https://sites.google.com/view/datasharingpolicyhub/.

12 Stephen Larrick, *Towards Urban Data Commons? On The Origins and Significance of Platform Data Sharing Mandates*, May 2022, available at https://www.belfercenter.org/publication/towards-urban-data-commons-origins-and-significance-platform-data-sharing-mandates.

13 *Id.*, page viii.

14 Jeff Price, et al., *Micromobility: A Travel Mode Innovation*, Public Roads Magazine, Spring 2021, U.S. Department of Transportation Federal Highway Administration, available at https://highways.dot.gov/public-roads/spring-2021/02.

15 *Supra*, note 11.

16 Platform Urbanism Data Sharing Policy, About / FAQ, available at https://sites.google.com/view/datasharingpolicyhub/home/about.

17 Massachusetts Bill H.3372 (filed Jan. 20, 2023), available at https://malegislature.gov/Bills/193/H3372.

18 A proposed law in Georgia, for example, would require third-party food delivery platforms to provide certain information (including consumer name and contact information) to food service establishments participating in online orders. HB 225 (filed Feb. 2, 2023), posted at https://www.legis.ga.gov/legislation/63979.

19 Data Act: Commission proposes measures for a fair and innovative data economy (Feb. 23, 2022) available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113. A proposed amendment to the EU Data Act reportedly includes a provision ensuring that public authorities may demand access only to non-personal data held by businesses. See *Super-sized amendment to EU Data Act voted through by parliament's industry committee*, MLex (Feb. 9, 2023), available at https://content.mlex.com/#/content/1448187.

20 Data Act, Ch. V, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN.

Such regulations can create legal uncertainty for businesses when data sharing requests conflict with companies' ongoing data protection obligations.

Local legislators and council members need to be aware of the complexities of data protection and data security laws; they must also realize that the data they are seeking may already be subject to legal constraints. Basic data protection principles (such as data minimization and purpose limitation), as well as anonymization, pseudonymization, and other data security practices must be addressed.

Some local governments have already taken privacy and data security considerations into account, such as Austin, Texas. There, micromobility regulations require licensees of e-scooters and bikes to be responsible for "implementing and submitting to the Director [of the Austin Transportation Department] a privacy policy that safeguards users' information, including personal, financial, and travel information."[21] They also prohibit licensees from requiring customers to reveal location data while using the service or to share their data with third parties.[22] The regulations further direct licensees to share data with the Director "in a manner that protects individual user privacy."[23]

As a general measure to help operationalize sound data protection practices, local governments should consider the adoption of accountability-based frameworks. Organizational accountability promotes the implementation of effective privacy and data management programs, which are vital to any organization, private or public, collecting and processing data, especially personal data. To the extent local governments are unfamiliar with good data management practices, an accountability framework will help them clarify the purposes and goals of a given data sharing initiative and place guardrails around their uses of that data. Businesses otherwise hesitant to share data are more likely to comply with non-mandatory government requests if the government is holding itself to at least the same principles adopted by the private sector.

Responsible businesses have increasingly adopted accountability frameworks to operationalize legal requirements. CIPL's Accountability Framework[24] includes seven key elements that every comprehensive data governance and use program should address. See Figure 1 below. One key element – risk assessment – ensures that organizations identify the potential harms to individuals that may result from their envisioned data uses to facilitate the adoption of appropriate protective measures to minimize those risks. Implementing such a comprehensive accountability framework also facilitates compliance with existing privacy laws, which may vary from jurisdiction to jurisdiction, and enables entities to demonstrate their compliance upon request.

---

21 Austin Transportation Department, Director Rules for Deployment and Operation of Shared Small Vehicle Mobility Systems, Section 7 – Privacy, Data Reporting and Sharing, subsection A, available at https://austintexas.gov/sites/default/files/files/Transportation/Dockless_Final_Accepted_Searchable.pdf.

22 *Id.*, subsections B and C.

23 *Id.*, subsection H.

24 See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.

Figure 1. The CIPL Accountability Framework

Source: CIPL

III. ACCOUNTABLE DATA SHARING PRACTICES

To help public entities (and private organizations) comply with best practices related to data privacy and security, CIPL encourages not only the adoption of comprehensive accountability programs such as the CIPL Accountability Framework, but also the adoption of certain specific accountability considerations and practices relevant to the data sharing context that can be used by entities—both public and private—regardless of size or level of sophistication.

1| Clearly define and document purposes of data use

Each proposed collection of private sector data must define clear objectives to set the boundaries of what can and should be done with the data and for what purposes. The proposed purposes should be supported by evidence that the data requested actually addresses a particular legitimate need. Private entities should be informed of these purposes to help facilitate the sharing of relevant data sets as well as any transparency requirements they may be subject to.

Where businesses are subject to limitations on how they may use data—whether by law, contract, or commitments made in their privacy policies—these limitations may impede their ability to engage in non-mandated data sharing with government agencies. Local governments should anticipate such concerns and have in place a mechanism or protocol for businesses to raise these matters and resolve potential conflicts over data sharing obligations.

One particular concern in the B2G data sharing context is the possibility of onward transfers of data. Businesses may object to situations where local governments are resharing the data with third parties such as law enforcement (as it could circumvent rights businesses may otherwise exercise) or competitors (as it could reveal or give insight about confidential business practices). If the government intends to reshare the data with others, the government should identify the intended recipients and specify the purposes for any downstream sharing. The government should also require downstream recipients to execute a confidentiality or data protection agreement to restrict any processing to uses

that are consistent with the purpose of the original collection and to prevent further downstream sharing.

Another concern is the privacy risk associated with making "de-identified" data publicly available.[25] De-identified data is not synonymous with anonymized data. Because de-identified data can be reidentified, governments that require sharing of such data may unwittingly facilitate efforts to "reconnect the dots," thereby violating individuals' underlying privacy rights.

2| Proportionality test

The volume, manner, and duration of data processing should be relevant, necessary, and proportionate to the desired objectives. Public entities should be able to answer and document the following considerations:

- Can we achieve the same objectives by using aggregated or fully anonymized data that does not identify individuals?
- Where personal data is not aggregated or fully anonymized, can we achieve the same objectives with less data or fewer categories of data?
- Is the proposed data processing a proportionate response to the goal we are trying to achieve? If not, what do we need to change and do to make it proportionate?

Local governments should understand and recognize that private entities' willingness and ability to share data may be constrained by their own purpose limitation and data minimization obligations or by the lack of a legal basis to share information. As mentioned above, governments should enable a procedure or process whereby businesses can raise and resolve potential conflicts with pre-existing data sharing obligations.

3| Legal basis

Both government entities and private organizations should have a specific legal basis for processing personal data. Government bodies normally rely on a statutory duty, but they may also reach out to private businesses in the absence of a regulation or ordinance. In many jurisdictions, companies must specify a legal basis for disclosure of personal data (such as legitimate interest, public interest, or consent under the EU GDPR), so governments should be ready to specify the legal grounds on which companies can base their disclosure.

4| Privacy and data impact assessment

Just as private sector organizations are required to do by certain laws, local governments should assess the level of risk associated with the processing or sharing of data and the potential impact on the rights and freedoms of individuals for each use. Risk may be higher if a government initiative involves the collection and use of health, geolocation, or other types of data deemed sensitive in certain contexts. In such cases, specific mitigation measures should be put in place to address the heightened risk. The assessment should also include an evaluation of the benefits of the data use, the risks of not using the data, as well as the impact of any residual risk after implementing all available mitigations if the data is used as planned. To the extent that certain uses of data can lead to disparate impacts and

[25] See, for example, Connecticut SB 1180 (January Session 2023), which would require the Labor Commissioner to make "redacted versions" of data containing personally and identifiable information "available on the Labor Department's Internet web site for analysis by the public." Bill text available at https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2023&bill_num=1180.

outcomes on marginalized and disadvantaged communities, the assessment should factor in those considerations as well.

5| Transparency

In many jurisdictions, private sector organizations are already obligated to provide notices to their customers explaining how and why their data is being processed, shared, and used. Government agencies should be subject to comparable notice requirements. Government transparency would also include a description of controls implemented to address any data privacy risks and other information to foster trust, such as where to address questions and requests to exercise data protection rights.

6| Robust and continued data security

Security is one of the cornerstones of data privacy. Security measures must be assessed and, if necessary, enhanced to avoid unauthorized access to data, especially geolocation information and other types of data that could be contextually sensitive.

Consequently, any transmission of data from the private sector to the governmental agency and any further use of that data must be accompanied with appropriate data security measures to prevent loss, destruction, and unauthorized access. Both public and private entities are responsible for data security with respect to their own processing activities, as well as for any breaches that may occur.[26] Where a data breach occurs at a governmental agency—and where the breach includes data that was shared by a private entity—there are few if any measures of redress against the agency to offset any liability the private entity might face in the B2B or B2C context, e.g., the damages from customers or end users whose data may have been included in the data set that was requested from the governmental agency.

7| Data retention and use limitation

Data processing undertaken in the context of a local government initiative should be conducted under clearly limited time frames. Once the purpose of processing is fulfilled, it is best practice to destroy the data unless potential future uses are safe and likely to be consistent with previously made transparency disclosures; not simply stored for undefined future objectives unrelated to the original purpose.

Equally, depending on local laws, private sector organizations may be under the obligation to set data retention periods linked to their own business needs. Laws in many jurisdictions do not allow data to be kept indefinitely simply because it may be requested at some future date by a local government.

8| Roles, responsibilities, and training

All staff, contractors, and third parties working on the initiatives and projects for which the data was shared must be clear on their roles and responsibilities in delivering accountability measures and ensuring privacy protections. Local governments must provide role-based training and set expectations for acceptable behaviors.

---

[26] Mandiant's "M-Trends 2023" Special Report noted that 25% of Mandiant investigations in 2022 pertained to government-related organizations—compared to just 9% in the previous year—making the public sector the most targeted sector. Mandiant attributed the increase to its work done in Ukraine. See Michael Hill, "Businesses detect cyberattacks faster despite increasingly sophisticated adversaries," Apr. 18, 2023, CSO Online, available at https://www.csoonline.com/article/3693575/businesses-detect-cyberattacks-faster-despite-increasingly-sophisticated-adversaries.html.

9| Data sharing agreements and protocols

Government entities should be aware of the relevant rights, obligations, and controls relating to data use, including any limitations on further transfers of the data. It is likely that data sharing protocols will be necessary to document respective roles and responsibilities of both. The protocols must include oversight and review mechanisms to report concerns and ensure that all parties act in accordance with agreed uses.

10| Trust, but verify

Local governments should conduct assessments and audits to verify that they are implementing the requirements, controls, and accountability measures specified in the data sharing initiative and in any third party agreements.

11| Internal oversight and external validation

The more complex and high risk the data use/sharing is, the greater the need to ensure internal oversight by and clear accountability of senior leadership within the public sector. Dedicated data ethics boards, privacy advisory boards, or data use advisory councils could provide an additional layer of accountability and could be used as a multi-stakeholder forum to discuss new and risky initiatives.[27]

12| Regulatory engagement and validation

Localities should be prepared to demonstrate accountability measures and seek feedback on their initiatives from data protection and enforcement authorities as well as from the private sector organizations supplying the data. This can be either in the planning phases, or post-facto, on request or in the case of a complaint or another issue. Constructive engagement is especially crucial when sharing information deemed contextually sensitive. By discussing and navigating relevant challenges together, all parties can achieve responsible outcomes that satisfy expectations and generate public trust.

Equally, some private sector organisations may conduct their own consultations with data protection and enforcement authorities, in advance of any data sharing request.

13| Privacy-by-design through technical measures

Local governments should consider technical measures to promote privacy-by-design in new data-driven initiatives. For example, the use of Privacy Enhancing Technologies and Privacy Preserving Technologies can play an extremely important role in mitigating privacy risks while enabling beneficial data uses and data-driven decision making.[28] While the best model will vary by context, these technologies have broad potential to enable privacy-compliant data analytics. Governments should welcome industries' use of such technologies—as well as their willingness to supply anonymized or aggregated data sets—since such practices may relieve the government's burden to employ supplemental privacy-compliant measures on their own.

---

[27] The City of Oakland was the first U.S. city to establish a Privacy Advisory Commission to look at city policies through a privacy lens. See "What Cities Can Learn from the Nation's Only Privacy Commission," Governing.com, 21 February 2020, available at https://www.governing.com/next/what-cities-can-learn-from-the-nations-only-privacy-commission.html.

[28] One local government has tested the use of such technologies in the context of election security. See "Wisconsin Partners with Microsoft and VotingWorks for Pilot Test of New Voting Technology," Wisconsin Elections Commission, Feb. 17, 2020, available at https://elections.wi.gov/news/wisconsin-partners-microsoft-and-votingworks-pilot-test-new-voting-technology.

IV. CONCLUSION

In sum, localities must recognize and respect the legal, ethical, and accountability-based obligations that attach to data when requesting or requiring the private sector to share such data. They must be mindful of data privacy and data security obligations already prescribed for the private sector—especially limitations on further data sharing—and they must be ready to implement and maintain similar privacy and data security protocols to enable receipt and responsible use of that data. Moreover, local governments must be judicious and prudent in their demands for data. They must be ready to embrace accountability principles and implement robust policies, procedures, and tools that promote responsible data practices. Indeed, accountability is essential to ensure lawful data sharing and business and public trust and support for such requests. By working together and being able to demonstrate accountability, private sector organizations and local governments can together advance the public's confidence in data-driven initiatives that seek to improve their communities.