

# The Challenge for Cities of Governing Spatial Data Privacy

Feiyang Sun,<sup>1</sup> Jan Whittington<sup>2</sup>

## Introduction

Organizations from both the public and private sector hold large quantities of data, both in static form and real time flow. US governmental organizations increasingly depend on the timely use of data for evidence-based policymaking, thus allowing government data to be viewed as a public resource and the governance of data to influence public interpretations of the role of government in serving the public good. If these datasets were stored and shared more widely within and across organizations, the resulting analytics could be used to improve organizational efficiency and productivity, enable and empower the general public, and produce economic and commercial value. The governance of data is, however, subject to a tension between data sharing and the need to apply both legal and technical means to protect the privacy of individuals represented in the data, as well as the need to address questions about data as property for public and private agents (Whittington et al., 2015; Young et al., 2019). Local governments face technical and organizational barriers to governing data in the public interest, and have recently begun, as exhibited in the City of Seattle, to piece together

---

<sup>1</sup> Feiyang Sun (fs377@uw.edu) is a PhD Candidate from the Interdisciplinary PhD Program in Urban Design and Planning, at the University Washington. His research reflects the role of planning and evaluates critically on the decisions of adopting surveillance technologies in smart cities in order to provide algorithmic as well as institutional solutions to preserve privacy of the public. His dissertation research develops methodologies for the detection and mitigation of re-identification risks of spatial trajectory data in different urban areas and sociodemographic segments.

<sup>2</sup> Dr. Jan Whittington (Corresponding Author: janwhit@uw.edu) is Associate Professor of the Department of Urban Design and Planning, at the University of Washington, Seattle. Her research applies transaction cost economic theory to networked infrastructures, such as transportation, water, and communications systems, to internalize factors historically treated as external to transactions. Her publications include methodologies for the evaluation of online transactions for efficiency, security, and privacy, greenhouse gas mitigation and resilience through capital investment planning, and examination of the efficiency of public-private contractual arrangements for infrastructure. At the University of Washington, she is the Director of the Urban Infrastructure Lab, Associate Director of the Center for Information Assurance and Cybersecurity, and Affiliate Faculty at the Tech Policy Lab.

policies, departmental resources, and implementation strategies for the purpose of effective governance of data.

The lack of such governance structures not only prevents organizations from receiving the full benefits of their data, but also brings a number of costs to organizations and individuals represented in the data. Data sharing is often an essential first step to enable public-private partnerships, as would be needed to provide government oversight of firms operating within the city under permits or as vendors. Without an established set of protocols for sharing and governing data, considerable costs of repeated negotiation and legal disputes emerge for governments and firms (Savage, 2019). Furthermore, the lack of established governance structures for data sharing opens up an unregulated and unmonitored market for data brokers, who may then collect and rejoin released datasets, re-identify data subjects, and sell the resulting artifacts for profit (Federal Trade Commission, 2014). Any economic or social costs that arise from the loss of privacy from public data can be treated as externalities that, by definition, are paid by the general public (i.e., the data subjects), while the benefits are captured by the private data brokers, which creates harms to social equity as well (Savage, 2019).

This paper examines the case of institutional design for urban data governance in the City of Seattle as a collective action problem, referencing three prominent theoretical frameworks for examining institutional change and institutional economics. This work centers on the Governing Knowledge Commons framework (GKC), which is adapted from Elinor Ostrom's the Institutional Analysis and Development (IAD) framework for natural resource commons (Ostrom, 1990) and developed by Frischmann et al. (2014) to study institutional arrangements for overcoming various social dilemmas associated with sharing and producing information, innovation, and creative works (Frischmann et al., 2014). Furthermore, this paper notes the foundational integration of the IAD framework with Oliver Williamson's transaction cost economics (TCE), highlighting the role of transaction costs in understanding the externalities associated with the governance of data (Williamson, 1975, 1985; Whittington and Hoofnagle, 2012; Hoofnagle and Whittington, 2014).

This paper is organized in two sections. The first provides theoretical context for understanding the case of Seattle City smart city governance, including GKC, IAD, and TCE as presented in the privacy literature, which benefits from the concepts of privacy as contextual integrity (Nissenbaum, 2004) and the taxonomy of privacy (Solove, 2006). The second section applies Seattle's governance structure to this theoretical framework, as one case study of several in the GKC series to comparatively analyze institutional change and city governance.

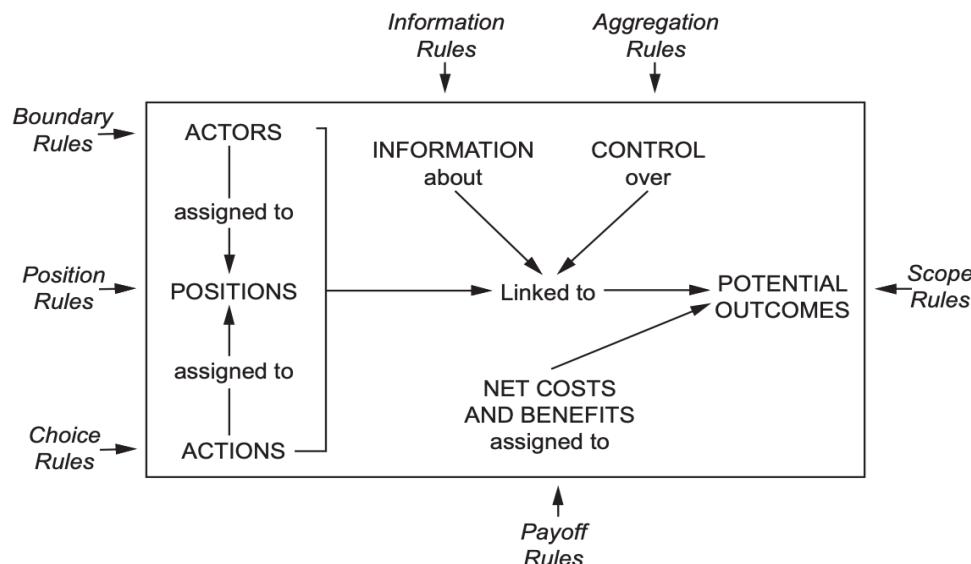
## Theoretical Frameworks for Evaluating City Governance of Privacy

Privacy research recognizes theoretical frameworks from economics (Hoofnagle and Whittington, 2012; Acquisti, 2014), information economics (Choi et al., 2019), and includes the theories developed from within the field (Nissenbaum, 2004; Solove, 2006; Rubinstein, 2018). Some recent advances examine the formation of institutions for governing privacy as part of a

commons (Savage, 2019), with reference to Elinor Ostrom's path breaking institutional economic work (Ostrom, 1990).

Elinor Ostrom's research on the governance of common pool resources provided an empirical and theoretical explanation of institutional change within communities (Ostrom, 1990). Problems governing common pool resources, such as fisheries and groundwater aquifers, offer iconic representations of the tragedy of the commons, found principally in Cournot's model of the non-cooperation in the prisoner's dilemma (Hardin, 1971). Ostrom's contributions to game theory reveal, however, the mechanisms employed to create institutions of self-governance in these settings, providing empirical evidence, more elaborate models, and grounded theories that bear on Nash's (Nash, 1953) theory of cooperation. Frischmann et al. (2014) extends Elinor Ostrom's the IAD framework for natural resource commons (Ostrom, 1990) to study the commons-based knowledge production, or the governing of the knowledge commons.

Adapted to describe institutions governing information, the Knowledge Commons framework simply expands on the concept of resource characteristics to include those other than products of the natural world (Frischmann et al., 2014). Resource characteristics, attributes of the community, and rules-in-use (a reference to path dependence in institutional economics), are influencing factors for actors in "action situations", which give rise to patterns of interaction and feedback loops within the community. Further within Ostrom's concept of IAD (Ostrom, 2011), action situations are given internal structure by recognizing persons in positions meaningful to potential outcomes, who may differ in their information about the situation or authority or ability to control the situation (Figure 1). And of course, the cost and benefits of outcome situations vary, for the community as a whole and for the participants and those they may represent in the action situation. These figures illustrate how, as a framework, Ostrom's IAD and the GKC identify universal elements to consider in the analysis of institutions (Ostrom, 2011, p. 8).



**Figure 1. The Internal Structure of an Action Situation (Ostrom, 2011)**

In general, the IAD and GKC support research on the economics of institutions, as found in transaction cost economics. Transaction cost economics, as described by Ronald Coase (Coase, 1960) and operationalized by Oliver Williamson (Williamson, 1975), provides theoretical and empirical support to the idea that institutions and organizations within well-functioning economies are formed for the purpose of economizing on transaction costs. This theory and associated body of empirical work apply further to comparative analysis of economies (North, 1990), where institutions are the defining source of variation in economic performance. TCE, GKC, and IAD are complementary, as each are elaborating on institutions and their economic performance. Their principal difference may be that GKC and IAD provide a framework for connecting qualitative variables in the formation of institutions to outcomes in the form of costs and benefits to participants, which TCE describes as a transaction in a more typical well-formed market. In contrast, TCE offers research designs for comparatively analyzing the efficiency of institutions in terms of costs, which can answer questions about the relative collective benefits of the institutional changes examined from place to place or over time in GKC and IAD fashion.

Both the GKC and the TCE frameworks have been applied to analyze alternative governance forms for privacy. Sanfillippo et al. (2018) adopted the GKC framework and complemented it with Helen Nissenbaum's "privacy as contextual integrity" approach (Nissenbaum, 2004) and Solove's taxonomy of privacy's diverse meanings (Solove, 2006). Through a meta-analysis of 14 case studies using the GKC or IAD framework, the study demonstrated the usefulness of the GKC framework to systematically explore and structure variance among communities with respect to knowledge resources and participation, obstacles and dilemmas surrounding knowledge formation and flows, objectives of participants, and rules-in-use structuring knowledge and privacy commons. Whittington and Hoofnagle (2012; Hoofnagle and Whittington, 2014) utilized the TCE framework and the concept of asset specificity to explain the hidden privacy cost of the exchange between consumer information and "free" online services. Asset specificity arises in data as individuals may be identified from the data, making data subjects party to transactions that make use of the data or third parties subject to external effects from transactions. Since the exchange between consumers and online firms is not simple and discrete, but rather a continuous transaction with atypical attributes, these exchanges make it very difficult for consumers to determine the value of what they are trading. Even after an individual consumer becomes aware of the cost of privacy loss ex post, it is difficult for that consumer to switch service or withdraw his/her information without a significant cost due to the high asset specificity of personal information. Building upon existing studies using GKC and TCE, this case of governance of information by the City of Seattle offers an application of these theories to municipal data governance for privacy, and an illustration of the potential for research design on the efficiency of institutional change for the purpose of privacy governance.

# The Case Study of the City of Seattle

The City of Seattle has led the nation in the adoption of privacy principles and governance structures since the first appointment of a Chief Privacy Officer in 2015. This was followed by a Surveillance Ordinance and a series of system-wide evaluations of applications, technologies, and data assets, including the contents available as open data and for public records requests. The following sections map the systems and policies of information governance in the City of Seattle to the components of the GKC framework.

This analysis covers several relevant actions as Seattle has expanded and deepened its means and methods for governing privacy in municipal data over the past five years. This brief evolution of policy and its implementation includes the governance of data and the technologies used to collect and process data by the City of Seattle to protect the privacy of city residents, while retaining the utility of data for municipal purposes. The IAD and GKC frameworks exist as a constellation of variables that surround and define these actions. This section first addresses so-called external variables, which are the 1) resource characteristics, 2) attributes of the community, and 3) rules-in-use. This is followed by sections that focus on the action arena, by identifying 4) action situations, 5) actors in positions, 6) rule configurations as they may affect the action under consideration, and 7) patterns of potential outcomes and interactions.

## Resource Characteristics

Cities often face conflicted objectives when it comes to the governance of urban data. On the one hand, they are pushed to provide more public access to the data to better inform decisions, facilitate research, and enhance governance transparency and accountability. On the other hand, they also have the obligation of protecting the privacy of their residents to build and maintain public trust in represented government, the fiduciary responsibility of government with taxpayer funds and the provision of government services for the public good. The goal of the governance of urban data is to balance these two objectives through the management of urban data as a public resource. This section discusses the characteristics of urban data and associated common privacy challenges, noting that the public trust in government is associated with effective governance of data in the public interest and its counterpart, perceptions of lack of trust, can be interpreted as indicators of inefficient or ineffective governance of data in the public interest. However, since the concept of trust in the governance of commons is rather complex and has been discussed extensively in other IAD contexts (Ostrom, 2009), this paper only focuses on the governance of urban data. Data has monetary and governmental value as property, bringing measurable costs and benefits to users and data subjects. In transactions involving personal data, safeguards for privacy are viewed as necessary to reduce the cost to the data subject that may arise from opportunism with guile on the part of any individual or organization possessing such data. In this sense, governance structures safeguarding privacy reduce ex post transaction costs over data that may be used to identify individuals and groups in society.

However, not all transactions of personal data require the same level of safeguard, and implementing the appropriate safeguard requires the evaluation of privacy risks and associated

transaction costs involved in each type of transaction. Safeguards can be construed as alternative governance structures in transaction cost economics (i.e., alternative institutional arrangements), and the idea of economizing is to find the alignment of transactions (with their privacy characteristics) with governance structures (institutional arrangements) to minimize transaction cost to the collection of parties involved, *ex ante* and *ex post*.

In terms of safeguarding personal data for privacy, both Nissenbaum (2004) and Solove (2006) have explored the variability and heterogeneity of privacy expectations. Nissenbaum (2004) has pointed to key parameters of information norms, such as actors, attributes, and transmission principles, to locate context, identify disruptive flows, and determine the constraints on the flow of information. The TCE framework of comparative institutional analysis could be used to empirically examine or implement Nissenbaum's contextual integrity framework in order to find governance structures that fit, i.e., that minimizes *ex post* privacy loss. In other words, the TCE framework is a complementary methodology for understanding the effect and perhaps quantifying the variability of privacy risk and associated harms by examining the relationship between personal data and the bilateral contractual relationship of the transaction through the lens of asset specificity (e.g., trade in personal or identifiable information for another good).

Asset specificity describes the degree to which an asset can be redeployed to alternative uses and by alternative users without sacrifice of productive value (Williamson, 1975). Asset specificity in information is, in this way of thinking, a function of the personal or re-identifiable nature of the data in question (Hoofnagle and Whittington, 2013). Personal information is, in the TCE sense, an asset unique to each consumer and difficult to redeploy. For example, daily routines or habits would often take months or years to change and it is almost impossible to change a person's biological information. When an asset cannot be redeployed without a significant cost, transactions are more likely to form a bilateral dependent relationship *ex post*, even when the contractual relationship starts from perfect competition *ex ante*. Such a bilateral dependent relationship would lock consumers via their personal or re-identifiable information in the transaction, which drastically increases the risk of exploitation by opportunism. The higher asset specificity of a piece of personal information, the more likely a consumer being locked in bilateral dependent trading relations with the firms that obtain this information, and therefore requires higher levels of safeguard.

Previous analysis of Seattle data governance highlights the outsized role of personal identifiable data in city affairs (Whittington et al., 2015). The emergence of location-based services has led to an unprecedented surge in spatiotemporal data sources available to cities and their vendors, and Seattle is no exception. While the new sources offer opportunities to discover subject-level knowledge and expand fields of inquiry, they also allow the re-identification of individuals, thus raising privacy risk by revealing intimate information about persons (Thompson and Warzel, 2019). Location-based and time-stamped data may be analyzed with malicious intent, with serious consequences for the persons identified through the data. This section identifies the common data sources the City of Seattle encounters in daily practice and summarizes the empirical evidence identified in the literature demonstrating the privacy risks of different types of such data.

## Public Records

Although data from public records do not possess the same level of spatiotemporal resolution as data emerged from the new sources, studies have shown that the simplest location or temporal information in the public records can be linked to re-identify people. Golle (2006) examined 2000 census data and found that 63% of the US population can be uniquely identifiable by gender, 5-digit zip code, and estimated date of birth. Even at the county level, 18% of the US population can be identified with the three variables. With the same identifier of gender, zip code, and birth date, Sweeney (2002) linked two public available datasets – the voter registration list and the health insurance data in Massachusetts – and successfully identified the governor of Massachusetts. Acquisti and Gross (2009) used the birth data from the SSA Death Master File (DMF) and observed a correlation between individuals' Social Security numbers and their birth data, which allows statistical inference of private SSNs. The correlation is more significant for the younger cohort between 1989 and 2003, with 61% of records being correctly predicted by their birth data. More recently, Whittington et al. (2015) examined the datasets available from Seattle's open data portal and estimated that nearly all tables in the selected sample can be spatially linked either by spatial coordinates information or by zip code.

## Surveillance Cameras

Surveillance cameras, or closed-circuit television (CCTV) in particular, have long been approved by police forces, governments, local councils, and business owners to maintain safety and security (Ditton, 2000). A plethora of attention to surveillance cameras can be found in urban studies literature. As early as 1996, Jean Hillier documented the course of events in summer 1994 at Burswood Casino where security camera operators abused their access to control equipment by targeting the cameras at women for voyeuristic pleasure. The story caused major public outrage and started a widespread debate on the blurring boundaries between public and private space and activities (Koskela, 2002). More recently, Spiller (2016) discussed his own experiences in the UK of identifying 17 different CCTV cameras and being recorded, and the attempts to access his images through subject access requests. Through the course, the author wrote 37 letters, made 31 phones, and spent £60 making the requests, and faced a number of obstacles in obtaining the footage, including inadequate contact information, misleading or incorrect information, lack of responses, and simple rejection.

Apart from the aforementioned qualitative studies, others have applied a more quantitative approach. Ma et al. (2010) studied how snapshots of traffic intersections can be used as side information to achieve different privacy attacks to a person's mobility traces. The study used both real and simulated mobility trace data and found that ten snapshots can identify the trace of 30% - 50% of the victims. Chen et al. (2017) applied K-means clustering algorithm to a week of license plate recognition data obtained in Shenzhen, China and successfully reduced the data into groups with unique travel time, travel purpose, and spatial travel patterns. Gao et al. (2019) measured the privacy vulnerabilities of license plate recognition data captured by high resolution cameras on highways in Guangzhou, China. The study found that five spatiotemporal records are enough to uniquely identify about 90% of individuals, even when the temporal granularity is set to be half of a day. The study also

proposed two privacy protection methods, a suppression solution and a generalization solution. An entropy measure of information loss is introduced to measure the utility loss caused by each solution.

## Spatial Trajectory Data

Spatial trajectory data is another popular data type. Compared with public records data and data collected by location-based sensors, it has the highest spatiotemporal resolution, which is typically within a time interval of less than a minute. Thus, it also processes the highest privacy risks among all data types. Spatial trajectory data can come in several forms, such as GPS, cell phone signal tower data, or location-based micro-transaction information.

Studies on the privacy risk of spatial trajectory data abound. Terrovitis and Mamoulis (2008) examined the privacy risk of trajectory data using a synthetic dataset with an initial setting of 100 unique addresses, 10,000 trajectories. The number of adversaries who observe information increases gradually and the result shows that with five adversaries (i.e. spatiotemporal data points), over 90% of the individuals can be identified through the dataset. Munizaga and Palma (2012) developed an estimation method for transit alighting and applied it to a week of transit smartcard and GPS data of 36 million observations for Santiago, Chile. The proposed method can build a detailed public transport OD matrix at any desired time-space disaggregation. Montjoye et al. (2013) have shown, in their study of the hourly cell-phone tower tracking of 1.5 million devices by MAC address over 15 months, only four spatial-temporal data points per day are needed to re-identify 95 percent of the owners of those devices. Similarly, Gao et al. (2019) measured the risk of license plate recognition data and found that five spatiotemporal records are enough to uniquely identify about 90% of individuals, even when the temporal granularity is set to be half of a day.

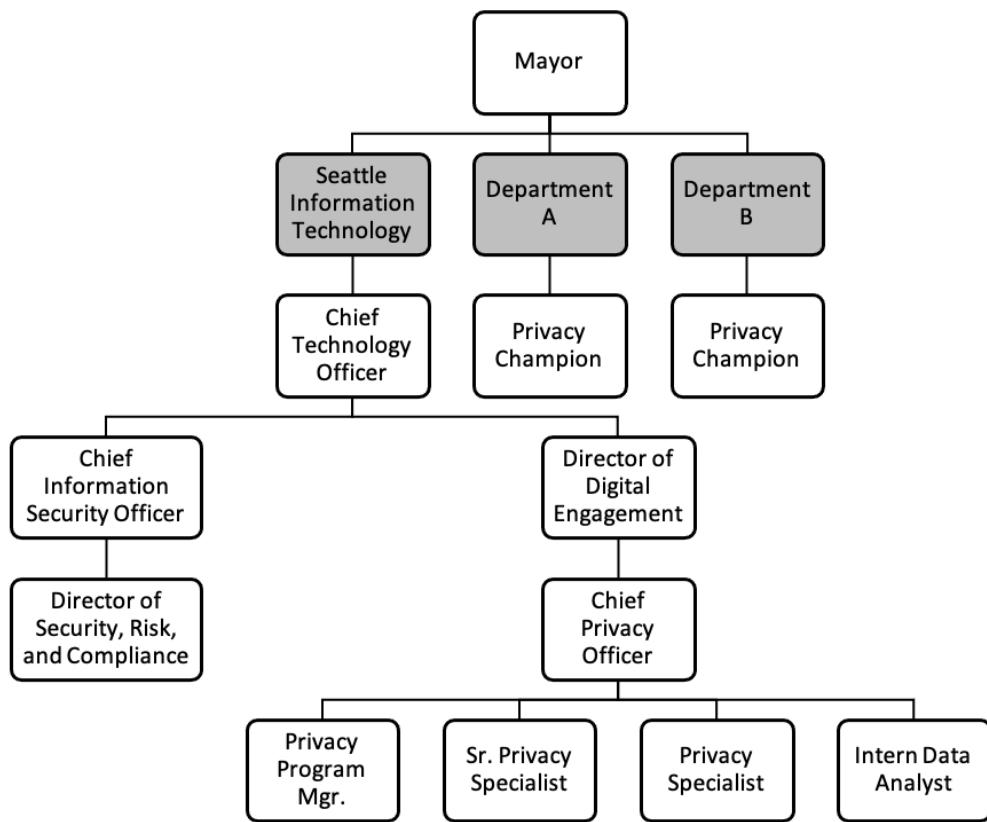
In summary, the public resource under consideration for this paper is data collected, held, and used by the municipality, and many types of municipal data happen to carry the threat of loss of privacy and associated costs to the data subject if released to the public, giving municipalities a compelling rationale for governing municipal data with privacy in mind. In the City of Seattle, events occurring in 2013 and 2014 elevated public concern over privacy to a peak, prompting the City to adopt a fresh perspective on the problem of public surveillance.

## Attributes of the Community

The modern evolution of Seattle's privacy policies and their implementation began in 2013, as the Seattle police began to install surveillance cameras and a mesh network with the capability of tracking wireless devices through downtown. Attentive to the emergence of cameras on city streets, critics of the system were vocal in their concern and opposition, including the Seattle Privacy Coalition, a group formed in March 2013 and incorporated as a non-profit corporation in 2014 to protect citizen privacy from government surveillance programs and intrusive corporate data collection (Seattle Privacy Coalition, 2013). In response to criticism the city deactivated the network, and began a multi-year process to conceive of policies and a governance system for protecting public privacy in municipal data and information technology.

Action on the part of the City was swift. In November of 2014, the City convened a Privacy Advisory Committee composed of academics, practitioners, lawyers and community advocates, which provided advice to City departments as they engaged in a new initiative to explore the role of the municipality with regard to protecting the privacy of its residents. By February of 2015, these efforts resulted in a unanimous vote of the city council to adopt the City's Privacy Principles, referred to by Mayor Murray as "a guide for our work in local government in order to help build and maintain trust with the people we represent" (Murray, 2015). Implementation began right away in 2015, as the City hired a Chief Privacy Officer and initiated policies and procedures associated with the principles, including notice and consent, and minimizing data collection and use, and deleting or de-identifying data according to city data retention schedules. At the same time, the city's approach to data governance for privacy was furthered by the City's participation in a study of internal data governance practices and public perception of privacy risk (Whittington et al. 2015). For example, Whittington et al. (2015) found that while the city's open data initiative was induced by the hope of improving government transparency and accountability, without a comprehensive assessment of latent risks and effective governance structures, it can lead to harms of privacy and social equity to the general public and public employees.

In 2016, the City of Seattle made an ambitious change to its organizational structure by consolidating its IT staff across the Department of IT and other departments into one office, Seattle Information Technology ('Seattle IT') to provide centralized information management and tech support to its 28 departments. Seattle IT hosts its Security, Risk and Compliance division, working in tandem with the privacy program to meet both privacy and security needs. The Privacy Program holds City departments accountable to its privacy principles and has published a Privacy Toolkit for use by each department to assess the privacy implications of the data they collect and use. In 2016-2017, Seattle IT accomplished the feat of training 92% of municipal employees on data privacy and security via an interactive training; this effort achieved high completion rates through internal monitoring, reminders, and customization. Seattle IT's organizational restructuring plays a key role in facilitating administration of the Privacy Program and privacy training. In 2017, managerial performance reviews began to include personnel completion of annual privacy training as a success criteria (Whittington et al., 2018).



**Figure 2. Organization chart of the Privacy Program and related areas (Whittington et al., 2018)**

Figure 2 illustrates the structure of the privacy program and its relationship with other municipal departments in 2018. The Privacy Program oversees privacy issues associated with data used in the other 28 departments in the municipality. The Privacy Program personnel include a Chief Privacy Officer, a Privacy Program Manager, Senior Privacy Specialist, Privacy Specialist, and Data Analyst Intern. It also has indirect reports within each department called ‘Privacy Champions.’ Privacy Champions are volunteers nominated by the directors of each department. They are trained in data privacy, and assist the privacy program personnel in carrying out privacy assessments of datasets intended for Seattle’s Open Data Platform.

The evolution of Seattle’s governance of municipal privacy was given further definition in 2018, when a city ordinance took effect that was touted by the ACLU as the “Nation’s Strongest Regulations for Surveillance Technology” (ACLU Washington, 2017). Seattle had, in 2013 and again in 2016 (Ordinance No. 124142 and 125376), already enacted two ordinances advancing privacy concerns over technologies that may be used for the purpose of surveillance. The latest of these acts (Ordinance No. 125679) offered a significant expansion of the city’s efforts. It deepened the role of municipal governance of privacy in relation to the community by establishing a Community Surveillance Working Group, an advisory body to the city comprised of community members, and a detailed apparatus for communicating to the public about the process and results of city decisions regarding the adoption and use of technologies capable of surveillance.

Altogether, this brief overview of the development of privacy policy and administration at the City of Seattle reinforces the concept of municipal privacy governance as an iterative

process between the municipality and the general public it serves, even as the varied departments and personnel with their roles and responsibilities grow and adapt to the new norms of privacy protection in the governance of municipal data.

## The Action Arena: Action Situations and Actors

The next factor of study in the City of Seattle's institutional environment is the action situation in the action arena; in particular, the action situations for governing privacy in urban data. An action situation is a key conceptual unit of GKC to describe the social space where individuals or actors interact, exchange goods and services, solve problems, dominate one another, or fight (Ostrom, 2011). The identification of an action situation and the resulting patterns and outcomes is essential as most of the description, prediction, analysis, and explanation under the GKC framework take place at this level (Ostrom, 2011; Sanfilippo et al., 2018).

To identify the action situations in this case study, we first apply Varian's (2004) concept of system reliability, common to data security as well as privacy, which argues that system reliability can be treated as a type of public good that depends on the successful function of the weakest link of the system. In other words, any one of many possible actors or action situations can result in a release or distribution of data that results in a loss of privacy: multiple dimensions, actors, and interactions could be identified as weak links in the effort to govern data for privacy and undermine the collective effort of the municipality to preserve citizens' privacy. This paper therefore conceives of the action situation as existing in these multiple contexts.

To further dimensionalize privacy, we also employ Solove's taxonomy of privacy (Solove, 2006) to identify the array of privacy problems and the action situations under consideration. Table 1 presents the privacy dimensions identified in Solove's taxonomy of privacy and the corresponding action situations, actors, and associated privacy concerns. It is worth noticing that under the original taxonomy of privacy there are four dimensions of privacy problems, which are information collection, information processing, information dissemination, and invasion. In this paper we cover the first three dimensions and combine collection and processing as they are often under the same policies.

**Table 1. Privacy Taxonomy and Action Situations**

Privacy Dimension	Action Situations	Actors	Privacy Concerns
Information Collection & Processing	Vendor agreement	Public agency and vendors	Sale of data collected by vendors for public use to third-party data brokers
	Surveillance ordinance	Public agency and special interest groups	Abusive use of data collected by city surveillance technologies

	Privacy impact assessment	Departments within public agency	Personally identifiable or sensitive information
Information Dissemination	Public disclosure request	Public agency and the general public	Request with malicious intent
	Open data release	Public agency and the general public	Data in a single dataset or from multiple joined datasets contain personally identifying or sensitive information

As illustrated in Table 1, public agencies face a variety of action situations under which they may interact with different actors, including private vendors, special interest groups, other departments in the municipality, and the general public. Depending on access to information and control, the same actors may have a different position under different action situations. For example, while public agencies provide monitoring under the action situation of vendor agreement, they are being monitored by the special interest group under the action situation of surveillance ordinance to prevent opportunistic behavior by the public agencies.

## Rules-in-Use

We group rules into federal and state laws and municipal policies. For the action situations, federal and state laws can be viewed as exogenous because they are not influenced by the outcomes of the action situations. In comparison, municipal policies can be endogenous to the action situations since they may be created or amended as an outcome of the action situation.

In the State of Washington, the Public Records Act (RCW 42.56) allows for the clear majority of public agency records to be disclosable in response to a specific request. The City of Seattle estimates that it receives between 200 and 250 public disclosure requests (PDR) each week, over 12,000 per annually. There is careful consideration about what can be disclosed in response to each such request. To comply with the Public Records Act, requested records may only redact or exempt attributes that are explicitly exempted from disclosure under the law, such as the home addresses of city employees, children's information and personal information for individuals receiving some services associated with welfare.

Recognizing the impact of these requests on state and municipal government, in 2017, the Washington State Legislature passed two bills relevant to public disclosure. HB 1595 provides for an agency to charge a per-gigabyte fee for the production of electronic records, whereas costs were previously charged for photocopies and hard drives alone. It also allows agencies to deny requests generated by bots, which are automated software programs that had

been used in the past to send multiple requests for records. HB 1594 requires public records officers to undergo additional training from the Attorney General's Office as to how electronic records must be handled under the law, and initiates a study of how new technologies could facilitate records disclosure, such as a statewide online public records platform. In addition to the Public Records Act, other State and Federal Legislative Activities that have implications for the City are listed in Table 2.

**Table 2. Relevant State and Federal Legislative Activities (Compiled from Privacy Program Annual Report, 2019)**

Legislative Activities	Timeline
<b>State</b>	
The California Consumer Protection Act (CCPA)	Effective in Jan 1, 2020
The Washington Privacy Act (WaPA - SB 6281)	Failed a House vote in 2019; Reintroduced in Jan 13th, 2020
The Use of Facial Recognition Services Bill (SB 6280)	Did not pass out of committee in 2019; Reintroduced in 2020
The Remedies for Misuse of Biometric Data Bill (HB 2363)	Introduced in 2020
The Consumer Protection Requirements for Data Brokers Bill (HB 1503)	Held over in 2019; Reintroduced in 2020
<b>Federal</b>	
Information Transparency and Personal Data Control Act	Reintroduced in 2018
Consumer Online Privacy Rights Act (COPRA)	Introduced in 2019

The rules-in-use at the City of Seattle for governing data for privacy may be categorized according to Solove's taxonomy of privacy, for their purposes in information collection, information processing, and information dissemination.

### Information collection & processing

Information collection and processing occurs as part of the governance of municipal data for privacy through the Data Privacy Review Process, vendor agreements, and the implementation of the Surveillance Ordinance offer insights into the information collection practices of the City.

## Data Privacy Review Process

All projects initiated since 2016 must follow the Data Privacy Review Process. The Data Privacy Review Process has steps which are completed based on whether a program is deemed to have personally identifying or sensitive information. Programs that were in place prior to the creation of this process are referred for a Privacy Review on a case-by-case basis for specific questions, such as a request for Privacy Program personnel to evaluate an existing vendor agreement. In addition, the City has incorporated the privacy review as part of the technology purchasing process. This is intended to identify technologies that meet the surveillance technology ordinance criteria and ensure that they are submitted to Council for review and approval prior to acquisition.

- Step I: Self-Assessment. The first step of the Privacy Review Process is the Self-Assessment. The Self-Assessment is a simple web form that asks the user whether the dataset contains any personal information; it defines personal information as “any information relating to an identified or identifiable individual,” including over 20 data elements, such as name, address, social security number, financial records, or ethnicity. If the user finds that the data does not contain personal information, or meet the definition of surveillance, no further action is needed, and the results of the Self-Assessment are filed for record keeping purposes. If the user indicates that the data does contain personal information, the data proceeds to the Threshold Analysis. The Self-Assessment document is available as a web form to be filled out by the project manager. The output of the analysis is automatically filed on an internal Sharepoint server to document that it has been completed. This record also notes how many of the dataset’s attributes have been reviewed, so in the future if the data is updated or expanded, it may be monitored for further privacy assessments. In 2017, the Privacy Team implemented a case management and automated workflow process to keep a record of the review cases and details, manage response expectations (Service Level Agreements for response time) and track Surveillance and Privacy Impact Assessment requirements.
- Step II: Threshold Analysis. This analysis is used to assess the risk rating associated with the data collected. It requires users to specify if sensitive attributes are collected by the program; for example: names, addresses, drivers’ license number, social security number, birthdate, email, biometric data, sex and/or gender, race, household info, credit card info, financial, health, or the location of persons. It next asks a series of questions about the dataset’s present purpose, data minimization, provision of notice, third-party vendor contract terms, data security, and records retention schedule. The output of the Threshold Analysis is a recommendation to the respondent as to whether a Privacy Impact Assessment will be necessary to evaluate the program. The Threshold Analysis, like the Self-Assessment, is a web form to be filled out by the project manager; it is filed to an internal site in SharePoint as documentation of the answers provided.
- Step III: Privacy Impact Assessment. The third step of the Privacy Review process is a Privacy Impact Assessment (PIA); it is conducted on programs that are using personally identifiable information and have been identified in the Threshold Analysis as representing higher risk. The project manager, privacy champion, or data owner create

an initial draft of the PIA. The PIA asks for detailed information about the program, assessing the contractual terms, security measures, data collected, how data is used, and its retention period. The intent of the PIA is to compare the program to the City's stated commitments in the Privacy Principles, for example, asking whether there is a means for data subjects to opt-into or opt-out of the dataset, or to correct inaccurate information. The Privacy Program Manager or other personnel then take this document and work closely with the project manager or data owner to refine the assessment; this investigative period usually requires a series of in-person meetings between the data owner and privacy program personnel. The content of the PIA depends on the salient qualities of the data collection program under review. The output of a Privacy Impact Assessment is a written report to the project manager documenting the privacy practices in place, and issuing privacy impacting mitigation recommendations where needed. In the long term, the intent of Seattle IT is to release its Privacy Impact Assessments as open data.

#### Vendor Agreement

Whittington et al. (2015) analyzed 18 agreements between the City of Seattle and vendors that handle its data and found a wide variation in the terms governing data privacy, security, and accountability. Third parties are required to meet the same Privacy Principles that City departments are obligated to follow. As a result, the City has drafted model contracts for consulting engagements and third-party data sharing agreements to include appropriate data privacy and security expectations. These are available to all departments considering data-intensive engagements with firms.

#### Surveillance Ordinance

The first City of Seattle Surveillance Ordinance (SMC 14.18) went into effect in 2013. Its purpose was to provide transparency and oversight to the City's increasing acquisition of specific surveillance technologies, such as cameras and drones. With public input, including active lobbying by the American Civil Liberties Union (ACLU), the statute was revised in 2015 to provide Council with the authority to develop an approval process for a broader definition of surveillance technologies. The new focus is on technologies whose primary purpose is to track and analyze the behavior and actions of individuals in a manner that negatively impacts civil liberties. This revised definition applies to all City departments; however, it primarily impacts public safety, transportation and utilities, whose missions both provide needed services and regulate the public's activities.

## Criteria

### Does the technology meet the definition a Surveillance Technology?

**No** Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.

### Do any of the following exclusion criteria apply?

<b>N/A</b>	Technology that is used to collect data where an individual knowingly and voluntarily provides the data.
<b>N/A</b>	Technology that is used to collect data where individuals were presented with a clear and conspicuous opt-out notice.
<b>N/A</b>	Technologies used for everyday office use.
<b>N/A</b>	Body-worn cameras.
<b>N/A</b>	Cameras installed in or on a police vehicle.
<b>N/A</b>	Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations.
<b>N/A</b>	Technology that monitors only City employees in the performance of their City functions

### Do any of the inclusion criteria apply?

<b>N/A</b>	The technology disparately impacts disadvantaged groups.
<b>N/A</b>	There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
<b>N/A</b>	The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
<b>N/A</b>	The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

### Figure 3. Criteria of a Surveillance Technology under Surveillance Ordinance

Figure 3 shows the criteria of a surveillance technology used in the review of surveillance ordinance. The Intelligence Ordinance requires that they be incorporated into the privacy review process. At the review intake stage, a set of questions are used to qualify certain technology acquisitions as surveillance. Surveillance technologies to undergo Council review and ordinance approval for their purchase, deployment or continued use. For certain categories of technology acquisitions, privacy review is required by default at the purchase request stage.

## Information Dissemination

Information dissemination within the scope of governance of privacy occurs mainly through the public disclosure request process and the open data program.

### Public Disclosure Request

In the State of Washington, the Public Records Act (RCW 42.56) allows for the clear majority of public agency records to be disclosable in response to a specific request. The City of Seattle estimates that it receives between 200 and 250 public disclosure requests (PDR) each week, over 12,000 per annually. Each department hires staff to handle. There is careful consideration about what can be disclosed in response to each such request. To comply with the Public Records Act, requested records may only redact or exempt attributes that are explicitly

exempted from disclosure under the law, such as the home addresses of city employees, children's information and personal information for individuals receiving some services associated with welfare. A summary of information exempt from disclosure under the law is available online via the Washington State Legislature. Recognizing the impact of these requests on state and municipal government, in 2017, the Washington State Legislature passed two bills relevant to public disclosure. HB 1595 provides for an agency to charge a per-gigabyte fee for the production of electronic records, whereas costs were previously charged for photocopies and hard drives alone. It also allows agencies to deny requests generated by bots, which are automated software programs that had been used in the past to send multiple requests for records. HB 1594 requires public records officers to undergo additional training from the Attorney General's Office as to how electronic records must be handled under the law, and initiates a study of how new technologies could facilitate records disclosure, such as a statewide online public records platform.

#### Open Data Program

Since 2016, all new data sets pushed onto the Open Data Platform, data.seattle.gov undergo the Data Privacy Review Process as described above. Open data is published through the release process by an Open Data Champion in consultation with the Open Data Manager in Seattle IT, and the data owner. Most prospective open datasets are not about individual people-- for instance, data that would be useful for home buyers such as green building data and which properties use underground gas storage tanks. In these cases, the Privacy Self-Assessment is used to document the fact that the dataset does not contain personally identifiable information. In some cases, datasets that become open data require a thorough Privacy Review and consultation. Two such datasets are from the Police Department; 'officer use of force' and 'officer involved shootings'; both of which document incidents in which police officers used force or discharged weapons. These datasets were released as part of a Transparency and Accountability initiative within the Police Department.

Privacy Program personnel also advise Open Data Champions and the Open Data Program manager not to include "foreign keys" or other attributes in a dataset that could be used to link the dataset with another one. This is a measure to avoid the "mosaic problem", the capability to combine disparate datasets on common attributes, which makes it more likely that the persons represented in anonymized datasets could be re-identified. In a seminal study, Harvard researcher Latanya Sweeney (2000) could uniquely identify 87% of the U.S. population using only three attributes; date of birth, gender, and zip code.

**Table 3. Action Situations and Rule Configurations**

Privacy Dimension	Action Situations	Categories of Rules-in-Use	Descriptions of Rules-in-Use in the Action Situations
Information Collection &	Vendor agreement	<i>Boundary rules</i>	Who has access to the data;

Processing		<i>Position rules</i>	The role of public agencies and the vendor;
		<i>Scope rules</i>	Purposes of data collection;
		<i>Choice rules</i>	Intended uses of data
		<i>Aggregation rules</i>	Control over collected data
		<i>Information rules</i>	Access to the information of data collection and processing
		<i>Payoff rules</i>	Rewards for fulfill the agreement and punishment for violations.
	Surveillance ordinance	<i>Boundary rules</i>	The geographic boundary of the proposed surveillance technology;
		<i>Position rules</i>	The role of public agencies;
		<i>Scope rules</i>	Purposes of data collection;
		<i>Choice rules</i>	Intended uses of data;
		<i>Aggregation rules</i>	Control over collected data;
		<i>Information rules</i>	Access to the information of data collection and processing;
	Privacy impact assessment	<i>Payoff rules</i>	Punishment for violations.
		<i>Boundary rules</i>	The geographic boundary of the proposed project;
		<i>Position rules</i>	The role of public agencies and other involved parties;
		<i>Scope rules</i>	Purposes of data collection;
		<i>Choice rules</i>	Intended uses of data;

		<i>Aggregation rules</i>	Control over collected data;
		<i>Information rules</i>	Required training and access to the information of data collection and processing;
		<i>Payoff rules</i>	Punishment for violations.
Information Dissemination	Public disclosure request	<i>Boundary rules</i>	The requested dataset;
		<i>Position rules</i>	<i>Not applicable</i> ;
		<i>Scope rules</i>	Purposes of data request;
		<i>Choice rules</i>	Intended uses of data request;
		<i>Aggregation rules</i>	<i>Not applicable</i> ;
		<i>Information rules</i>	<i>Not applicable</i> ;
		<i>Payoff rules</i>	Cost of the data request.
	Open data program	<i>Boundary rules</i>	The geographic boundary of the data;
		<i>Position rules</i>	Personnel involved in the privacy impact assessment;
		<i>Scope rules</i>	<i>Not applicable</i> ;
		<i>Choice rules</i>	<i>Not applicable</i> ;
		<i>Aggregation rules</i>	<i>Not applicable</i> ;
		<i>Information rules</i>	<i>Not applicable</i> ;
		<i>Payoff rules</i>	<i>Not applicable</i> ;

Ostrom (2011) classified rules-in-use into seven categories: boundary rules, position rules, scope rules, choice rules, aggregation rules, information rules, and payoff rules. Boundary rules define the number and attributes of the participants. Scope rules identify the potential outcomes that can be affected and the actions linked to specific outcomes. Position rules establish positions in the situation. Choice rules articulate choice sets or actions that actors in each position may, must, or must not take. Aggregation rules define the level of control that an

actor exercises in a position. Information rules delimit an actor's access to information or define what information should be held secret. Payoff rules describe the rewards and punishments as a result of certain actions or outcomes. Table 3 summarizes the categories of rule used in each action situation. Two immediate observations emerge from Table 3. First, compared with other action situations which mostly rely on punishment or cost as deterrents for actions, vendor agreement is a more market-driven governance form that utilizes both punishment and rewards under the payoff rules. Secondly, the public disclosure request and the open data program as alternative forms of information governance may have weaker control over shared information as they have less rules compared with other action situations, and thus they may be more vulnerable to privacy attacks.

## Outcomes and Patterns

This section summarizes the three patterns discernible at this time. Other patterns may emerge as time goes on, or perhaps in relation to additional shifts in technology, internal organizational changes within the municipality, and the municipality's relationship with firms engaged in permitted activities, firms acting as vendors, and city residents.

### Positive Feedback Loop

The original policy and office of privacy set up a feedback loop within the City organizational structure, that reinforced the purpose of the new institutional rules under development and in action. Table 4 below illustrates the institutional feedback loop with the development of the City's privacy program from 2015 to 2019. As the privacy program becomes more mature, the privacy practices, policies, and processes become more institutionalized, emerging from unstructured and reactive practices into more formally defined governance rules and cultural norms of the organizations. Besides the organizational changes, the privacy program has reinforced its technical capacity by adopting new tools, such as the Implemented Privacy Review and Risk Management Tool by OneTrust, the Data and Survey Demographic Data Collection Playbook, and If-Then Planning Tool for IT Project Reviews and extending its scope to integrate systems, such as the credit card purchases that were previously not covered by the review process. The If-Then Planning Tool is a privacy recommendation tool created by Orrick and the City Attorney's Office to identify action items and risks mitigations prior to their privacy review to decrease the privacy review process time (Privacy Office, 2018).

**Table 4. Development of the City of Seattle's Privacy Program (Privacy Office, 2018)**

2015	2017	2018		2019	
First Created	Ad Hoc	Repeatable	Defined	Managed	Optimized
The program was created	Unstructured approach	Privacy is viewed as a	Privacy policies,	Privacy is embedded	Privacy is viewed as a

with six principles to provide guidance and tools for city employees when working with personal information.	where privacy policies, processes, and practices are not sufficiently defined or documented. Privacy management is mostly dependent on initiatives by individuals rather than processes.	compliance exercise and the approach is largely reactive with some guidelines. There is limited central oversight of the privacy policies, processes, and practices, with siloed approaches between units.	processes, and practices are defined, comprehensive to meet business needs, and are consistently implemented throughout. There is a holistic and proactive approach with widespread awareness.	into the design and functionality of business processes and systems and is consistent across the agency. Well-defined governance and oversight structures exist.	strategic initiative with a clear agency culture of continuous improvement. The agency is viewed by stakeholders and the public as a leader in privacy management, introducing innovative initiatives to meet their needs.
--	--	--	--	--	--

A city-wide data privacy and information security training is foundational to the City's Privacy Program. Included with other mandatory training courses for new employees, data privacy is a top priority for City leadership. The training was deployed in late 2016; employees received reminder emails until they had completed the training. As of March 2017, 92% of all 12,000 City of Seattle employees had taken the training (Privacy Office, 2018). Some departments, like Seattle Police, have 98% compliance with the training. As of October, 2017, the training course has been required to be completed annually by all City employees. Completion is tracked through an automated training system and managers will be held accountable for their employees through performance review metrics. The training materials were developed over 6 months via a collaboration with a private partner specializing in online training management systems. After authenticating their ID through an online portal, employees could access a 30-minute interactive training. When personnel did not have access to a computer (e.g., stage hands for events at the Seattle Center), they were sent the key points of the training as a paper document to their homes. Some trainings were customized for the needs of certain personnel, for example, the City Light service fleet who handle unique data types.

## Privacy Governance Consolidation and Scope Expansion

The Privacy Office of the City gradually became a locus of consolidation for the privacy review of data-intensive technologies and activities. This is a sign of maturity of the system of

governance, and may be considered a source of efficiency, even as it can be considered an expansion of the scope of its work across programs appropriate to privacy concerns. This includes reaching back into some of the more challenging tasks that such an office may face, such as the assessment of existing data for potential privacy concerns.

Many of these patterns are evident in organizational changes, or changes in roles and responsibilities noted above. This is also evident, however, in the growth and types of privacy reviews undertaken by this office. Table 5 shows the number of privacy assessments undertaken by the type of privacy review. Overall, contracts with vendors, acquisitions, and IT projects receive the most numbers of assessments. Besides, an increase in the number of assessments for acquisitions and contracts was observed from 2017-2018 to 2018-2019. Whereas there could be multiple factors leading to such an increase, from a transaction cost economics perspective, the observed trend can illustrate the effort of gradually providing more safeguards by the city to these two types of activities since they have higher complexity and privacy risks than others.

**Table 5. Number of Assessments by Type of Privacy Review (Compiled from Privacy Program Annual Report, 2018 - 2019)**

	2017-2018		2018-2019		Total 2017-2019	
	Assessments	Percentage	Assessments	Percentage	Assessments	Percentage
<b>Acquisitions</b>	153	14.87%	229	40.18%	382	23.89%
<b>Contracts</b>	225	21.87%	191	33.51%	416	26.02%
<b>IT Projects</b>	324	31.49%	90	15.79%	414	25.89%
<b>Other</b>	257	24.98%	30	5.26%	287	17.95%
<b>Survey/Form</b>	19	1.85%	19	3.33%	38	2.38%
<b>Open Data</b>	51	4.96%	11	1.93%	62	3.88%
<b>Total</b>	1029	100.00%	570	100%	1599	100.00%

Table 6 shows the number of technologies reviewed by the surveillance ordinance by the city department. It is worth noticing that of all the 912 technologies, only eight of them were determined to be surveillance technology. Table 7 lists the eight technologies. While Seattle City Light (the City's electricity company) and the Information Technology Department have the largest number of technologies reviewed, the Police Department has the most surveillance technologies (six out of eight). The vast difference between the number of reviewed technologies and the number of surveillance technologies shows the use of the surveillance ordinance as not only an assessment tool for a large collection of technologies, but also a screening tool that can dramatically reduce review time by narrowing down to a small selection of technologies for detailed assessments.

**Table 6. Number of Technologies Reviewed by the Surveillance Ordinance (Compiled from Surveillance Technology Acquisition Report, 2017 - 2021)**

Department	2017 Q4	2018 Q1-Q4	2019 Q1-Q4	2020 Q1-Q4	2021 Q1	Total
<b>Seattle City Light</b>	28	40	48	39	8	163
	19.31%	17.47%	17.52%	19.02%	13.56%	17.87%
<b>Information Technology Dept.</b>	45	41	41	28	4	159
	31.03%	17.90%	14.96%	13.66%	6.78%	17.43%
<b>Seattle Police Dept.</b>	14	38	31	21	5	109
	9.66%	16.59%	11.31%	10.24%	8.47%	11.95%
<b>Seattle Public Utility</b>	15	23	27	26	10	101
	10.34%	10.04%	9.85%	12.68%	16.95%	11.07%
<b>Transportation Dept.</b>	5	21	29	19	6	80
	3.45%	9.17%	10.58%	9.27%	10.17%	8.77%
<b>Citywide</b>	0	7	16	16	7	46
	0.00%	3.06%	5.84%	7.80%	11.86%	5.04%
<b>Other</b>	38	59	82	56	19	254
	26.21%	25.76%	29.93%	27.32%	32.20%	27.85%
<b>Total</b>	145	229	274	205	59	912

**Table 7. List of Technologies Determined as Surveillance Technology (Compiled from Surveillance Technology Acquisition Report, 2017 - 2021)**

Department	Reviewed Items	Year	Quarter
<b>Seattle Police Dept.</b>	SmartForce, BulletinWizard for Retail Theft	2017	4
<b>Information Technology Dept.</b>	Seattle IT Visitor Registration System	2017	4
<b>Transportation Dept.</b>	Seattle's Safest Driver Competition Mobile App	2017	4

<b>Seattle Police Dept.</b>	Body-Worn Video Program	2017	4
<b>Seattle Police Dept.</b>	Photo Enforcement Program	2017	4
<b>Seattle Police Dept.</b>	UFED Premium Software Upgrade	2019	2
<b>Seattle Police Dept.</b>	Black Bag Forensic Software	2019	3
<b>Seattle Police Dept.</b>	Seattle Justice Center Interview Room Camera Replacement	2021	1

### City and Public Interaction and Public Attitude Change

The work of the City has elicited increasing interest and participation from the community as it has delved into matters of community concern, such as the uses of technology by the police force and department of transportation, which raise concerns about civil liberties. Table 8 shows the number of public meetings held by the different departments or groups from 2018 - 2020. Prior to 2019, the public meetings were only used for public comments on the surveillance technologies and were held by the department that was responsible for the introduction of the new technology. In 2019, regular monthly meetings were held by the Surveillance Advisory Working Group, which includes members from both the public and private sectors, academia, and communities. Besides meetings on newly acquired surveillance technologies, there were also public meetings designed to raise the awareness of information privacy among the public, such as the Data Privacy Day and public workshops delivered in the Seattle Public Library.

**Table 8. Number of Public Meetings Held by Departments or Groups from 2018 - 2020 (Compiled from the City's Event Calendar)**

<b>Departments or Groups</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
Police Dept.	3	0	0
Transportation Dept.	2	0	0
Fire Dept.	2	0	0
Surveillance Advisory Working Group	0	10	3
Seattle Privacy Office	0	1	2
Information Technology Department	0	0	2

To explore the attitudinal change towards privacy among the general public, we examined the 2013 and 2018 Technology Access and Adoption Surveys of the City of Seattle. The surveys were conducted by the City of Seattle Department of Information Technology to learn residents' use of and attitude toward information and communication technology, such as computer and the Internet, cable TV, and mobile phones. Table 9 presents the number of respondents with and without privacy concerns over high-speed internet stratified by age and income groups. Overall, only 32% of respondents expressed privacy concerns in 2013 while 70% of the respondents expressed privacy concerns in 2018, which indicates a significant increase in the awareness of privacy among the general public. In terms of demographic differences, baby boomers and the middle-income class (\$25K-\$75K) have the highest percentage of respondents with privacy concerns in both 2013 and 2018. However, millennials (22-37) and the highest income group (\$100K+) have shown most increases in privacy concerns from 2013 to 2018.

**Table 9. Selected Results from the City of Seattle's Technology Access and Adoption Survey, 2013 and 2018**

	2013		2018		
Age	Respondents without Privacy Concern	Respondents with Privacy Concern	Respondents without Privacy Concern	Respondents with Privacy Concern	% Increase of Respondents with Privacy Concern
Millennials (22-37)	625	206	290	504	
	75%	25%	37%	64%	156%
Gen X (38-53)	498	243	416	843	
	67%	33%	33%	67%	104%
Baby Boomers (54-72)	467	325	287	925	
	59%	41%	24%	76%	86%
Income					
<\$25K	205	108	194	385	
	66%	35%	34%	67%	93%
\$25K to <\$50K	195	110	136	357	
	64%	36%	28%	72%	101%

\$50K to <\$75K	244	125	121	348	
	66%	34%	26%	74%	119%
\$75K to <\$100K	233	112	135	295	
	68%	32%	31%	69%	111%
\$100K+	596	220	527	1062	
	73%	27%	33%	67%	148%

In summary, the City's privacy program has seen significant growth with more structured institutional design, expanded scope of work, and more active public engagement. However, since the program has only been established for five years, most of the aforementioned observations are only short-term patterns while the long-term patterns and outcomes still need to be examined in the future.

## Conclusion and Future Research

This paper suggests the extent to which municipal governments, through the case of the City of Seattle, can evolve systems of governance to address the external effects of the technology it deploys, and do so in constructive iterations with the public it serves. The GKC framework provides an organizational mapping tool and a structured narrative that helps to break down the complex interactions and rule configurations within the systems and allows for the comparison between governance systems of urban data and technologies. Through the analysis, this paper found that there are two aspects that are unique to the governance of urban data, which requires a different treatment in the research design compared with studies of conventional natural resources. First, the study of urban data governance requires to cover a broader array of action situations as any one of many possible actors or action situations could be identified as weak links in the effort to govern data for privacy and undermine the collective effort of the municipality to preserve citizens' privacy. Second, it is important to examine urban data governance through a longitudinal perspective due to the rapid change of technology and fast evolution of related laws and policies.

Ostrom (2011) distinguished the concepts between framework, theory, and model. A framework defines the boundary of the studied system and maps each component within the system. Based on the framework, a theory proposes the relationship between the selection of the components and the outcomes of the systems. A model focuses on a more specific issue and tests the hypotheses generated from the theory. This paper demonstrates the effectiveness of the GKC as a framework that maps the systems and policies of information governance for data privacy in the City of Seattle. A potential direction of future research is to build on this paper and further examine the effectiveness and efficiency of alternative forms of governance based on the TCE theory. In particular, one hypothesis from the TCE is that

transactions involving more asset specificity carry increased risk to one or more parties to the transaction and possibly third parties in the case of externalities, which calls for more safeguards and possibly hierarchical governance to minimize ex post transaction costs. In the context of privacy, information with higher privacy risks would thus require stronger rules and enforcement characteristics for their governance, where transaction risks can be either qualitatively measured with the “contextual integrity” approach (Nissenbaum, 2004) or quantitative measured by k-anonymity (Sweeney, 2002) and governance forms can be categorized by the seven categories of rules-in-use (Ostrom, 2011) or incentive intensity, administrative controls, adaptation, and contract law (Williamson, 2000).

## References

- ACLU Washington, 2017. Seattle Adopts Nation’s Strongest Regulations for Surveillance Technology.
- Acquisti, A., 2014. The economics and behavioral economics of privacy. Privacy, big data, and the public good: Frameworks for engagement 1, 76–95.
- Acquisti, A., Gross, R., 2009. Predicting social security numbers from public data. Proceedings of the National academy of sciences 106, 10975–10980.
- Chen, H., Yang, C., Xu, X., 2017. Clustering vehicle temporal and spatial travel behavior using license plate recognition data. Journal of Advanced Transportation 2017.
- Choi, J.P., Jeon, D.-S., Kim, B.-C., 2019. Privacy and personal data collection with information externalities. Journal of Public Economics 173, 113–124.  
<https://doi.org/10.1016/j.jpubeco.2019.02.001>
- Coase, R.H., 1960. The problem of social cost, in: Classic Papers in Natural Resource Economics. Palgrave Macmillan, London, pp. 87–137.
- Coleman, J.S., 1990. Foundations of social theory. Cambridge, MA: Belknap Press of Harvard University Press.
- Commission, F.T., 2014. Data brokers: A call for transparency and accountability. Washington, DC.
- De Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M., Blondel, V.D., 2013. Unique in the crowd: The privacy bounds of human mobility. Scientific reports 3, 1376.
- Ditton, J., 2000. Crime and the city. British Journal of Criminology 40, 692–709.
- Frischmann, B.M., Madison, M.J., Strandburg, K.J., 2014. Governing knowledge commons. Oxford University Press.
- Gao, J., Sun, L., Cai, M., 2019. Quantifying privacy vulnerability of individual mobility traces: A case study of license plate recognition data. Transportation Research Part C: Emerging Technologies 104, 78–94. <https://doi.org/10.1016/j.trc.2019.04.022>
- Golle, P., 2006. Revisiting the uniqueness of simple demographics in the US population, in: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society. pp. 77–80.
- Hardin, R., 1971. Collective action as an agreeable n-prisoners’ dilemma. Behavioral science 16, 472–481.
- Hoofnagle, C.J., Whittington, J., 2013. Free: Accounting for the Costs of the Internet’s Most

- Popular Price. UCLA L. Rev. 61, 606.
- Hoofnagle, C.J., Whittington, J., 2012. Unpacking Privacy's Price. NCL REV. 90, 1327, 1358.
- Koskela, H., 2002. Video surveillance, gender, and the safety of public urban space:" Peeping Tom" goes high tech? Urban Geography 23, 257–278.
- Ma, C.Y., Yau, D.K., Yip, N.K., Rao, N.S., 2010. Privacy vulnerability of published anonymous mobility traces, in: Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking. pp. 185–196.
- Munizaga, M.A., Palma, C., 2012. Estimation of a disaggregate multimodal public transport Origin–Destination matrix from passive smartcard data from Santiago, Chile. Transportation Research Part C: Emerging Technologies 24, 9–18.
- Murray, E., 2015. City Adopts Privacy Principles to Protect the Public.
- Nash, J., 1953. Two-Person Cooperative Games. Econometrica 21, 128–140.  
<https://doi.org/10.2307/1906951>
- Nissenbaum, H., 2004. Privacy as contextual integrity. Wash. L. Rev. 79, 119.
- North, D.C. (Douglass C., 1990. Institutions, institutional change, and economic performance. Cambridge; New York : Cambridge University Press, Cambridge; New York.
- OLSON, M., 1971. The Logic of Collective Action: Public Goods and the Theory of Groups, Second Printing with a New Preface and Appendix. Harvard University Press.  
<https://doi.org/10.2307/j.ctvjsf3ts>
- Ostrom, E., 2011. Background on the Institutional Analysis and Development Framework. Policy Studies Journal 39, 7–27. <https://doi.org/10.1111/j.1541-0072.2010.00394.x>
- Ostrom, E., 2009. Building Trust to Solve Commons Dilemmas: Taking Small Steps to Test an Evolving Theory of Collective Action, in: Levin, S.A. (Ed.), Games, Groups, and the Global Good, Springer Series in Game Theory. Springer, Berlin, Heidelberg, pp. 207–228.  
[https://doi.org/10.1007/978-3-540-85436-4\\_13](https://doi.org/10.1007/978-3-540-85436-4_13)
- Ostrom, E., 1990. Governing the commons : the evolution of institutions for collective action. Cambridge; New York : Cambridge University Press, Cambridge; New York.
- Privacy Office, S.I.T.D., 2018. 2018 Privacy Program Annual Report.
- Rubinstein, I.S., 2018. Privacy Localism. Wash. L. Rev. 93, 1961.
- Sanfilippo, M., Frischmann, B., Standburg, K., 2018. Privacy as commons: Case evaluation through the governing knowledge commons framework. Journal of Information Policy 8, 116–166.
- Savage, C.W., 2019. Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy 22, 68.
- Seattle Privacy Coalition, 2013. Seattle Privacy Coalition Vision. URL  
<https://seattleprivacy.org/about/> (accessed 6.29.21).
- Solove, D.J., 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review 154, 477.  
<https://doi.org/10.2307/40041279>
- Spiller, K., 2016. Experiences of accessing CCTV data: The urban topologies of subject access requests. Urban Studies 53, 2885–2900. <https://doi.org/10.1177/0042098015597640>
- Sweeney, L., 2002. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10, 557–570.
- Sweeney, L., 2000. Uniqueness of simple demographics in the US Population, in LIDAP-WP4.  
<http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html>.

- Terrovitis, M., Mamoulis, N., 2008. Privacy preservation in the publication of trajectories, in: The Ninth International Conference on Mobile Data Management (Mdm 2008). IEEE, pp. 65–72.
- Varian, H., 2004. System reliability and free riding, in: *Economics of Information Security*. Springer, pp. 1–15.
- Whittington, J., Calo, R., Simon, M., Woo, J., Young, M., Schmiedeskamp, P., 2015. Push, pull, and spill: A transdisciplinary case study in municipal open government. *Berkeley Technology Law Journal* 30, 1899–1966.
- Whittington, J., Hoofnagle, C.J., 2011. Unpacking Privacy's Price. *N.C. L. Rev.* 90, 1327.
- Whittington, J., Young, M., Armbruster, G., 2018. Seattle's Data Privacy Program: Policy, Training, Inventory, and Assessment (unpublished).
- Williamson, O.E., 2000. The New Institutional Economics: Taking Stock, Looking Ahead. *Journal of Economic Literature* 38, 595–613.
- Williamson, O.E., 1975. Markets and hierarchies, analysis and antitrust implications : a study in the economics of internal organization. New York : Free Press, New York.
- Young, M., Rodriguez, L., Keller, E., Sun, F., Sa, B., Whittington, J., Howe, B., 2019. Beyond Open vs. Closed: Balancing Individual Privacy and Public Accountability in Data Sharing, in: Proceedings of the Conference on Fairness, Accountability, and Transparency. ACM, pp. 191–200.