> “PRIVACY IS NOT AN OPTION, AND IT SHOULDN’T BE THE PRICE WE ACCEPT FOR JUST GETTING ON THE INTERNET.”
>
> – GARY KOVACS
>
> FORMER CHIEF EXECUTIVE OFFICER OF AVG TECHNOLOGIES

SECTION 3

PRIVACY

3. PRIVACY OVERVIEW

“Why do we care?” about privacy and some key concepts to get started.

Create Privacy Principles & Policies – Section 3.1

- Privacy principles and why you should adopt one (3.1.1 – 3.1.2)
- Prominent privacy principles (3.1.3 – 3.1.4)
- Examples of privacy principles (3.1.5)
- Difference between privacy principles & policies (3.1.6)
- Dos and don’ts for privacy principles (3.1.7)

Create Accountability – Section 3.2

- Privacy professionals and why you need them (3.2.1)
- Hold your team internally accountable (3.2.2)
- Establish external accountability (3.2.3)

Evaluate Privacy Risk – Section 3.3

- Embed privacy into your procurement processes (3.3.1)
- Follow best practices and resources on assessing & monitoring privacy risks across activities (3.3.2)
- Overcome the challenges of limited resources and expertise (3.3.3)

Check out the resource repository at the end of the section.

3. PRIVACY

WHY DO WE CARE?

At its core, privacy is a fundamental human right that refers to as an individual's right to determine how their personal information is collected, used, and shared. Difficult to operationalize, privacy is dynamic, multi-faceted, and a highly subjective concept to understand.

Privacy concerns have taken center stage with the surge in data breaches, purposeful and unintentional misuse of personal information, and adoption of surveillance technologies and smart city applications. The continuous evolution of new technological capabilities has been accompanied by increased public scrutiny and awareness. As a result, we see cities and communities being increasingly concerned about the potential privacy risks and liabilities.

The severe public backlash that smart city projects have faced in recent times is a testament to how the relentless pursuit of smart city projects without due consideration of the unintended consequences to resident privacy can lead to privacy events that undercut public trust in municipal leaders and governments. The privacy risks grow exponentially as cities and communities evolve and collect more data on their residents, and use cases support the integration of this information across activities. Therefore, it is wise to place privacy at the forefront as cities and communities mature with regards to both policy and technology adoption.

In this section we provide best practices and guidance on:

1. Establishing Privacy Principles and Policies
2. Creating Accountability for Privacy
3. Evaluating Privacy Risks
4. Privacy Resource Repository for Cities and Connected Communities

KEY DEFINITIONS:[1]

- **Data Minimization** – The idea to collect and retain personal data necessary to inform a decision.
- **Disclosure** – A statement that provides details on how an organization will collect, process, use, and share individual data.
- **Informed Consent** – Unambiguous, specific, and informed indication, by a statement or by a clear affirmative action, that a person is agreeing to provide their personal data as well as grant permission for processing of their personal data as stated in the signed statement.
- **Privacy Event** – The occurrence or potential occurrence of problematic data actions.
- **Personally Identifiable Information (PII)** – Data or any element of data that can be used to establish or trace the identity of the person.
- **Social License** – Ongoing approval or broad social acceptance of a project within the local community and among its stakeholders.

[1] (i) National Institute of Standards and Technology (NIST). (2020, January). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. NIST. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf#page=32; (ii) What is the social license? (2020). SocialLicense.Com. http://socialicense.com/definition.html

3.1. ESTABLISHING PRIVACY PRINCIPLES AND POLICIES

3.1.1 WHAT ARE PRIVACY PRINCIPLES?[2]

Privacy principles are a set of standards or guidelines (binding or non-binding) intended to act as an overarching philosophy for the protection of the personal information of individuals collected, held, and used by government authorities and their stakeholders.

3.1.2 WHY SHOULD CITIES AND COMMUNITIES ADOPT PRIVACY PRINCIPLES?

Documenting and codifying privacy principles can help cities and communities achieve multiple goals:

- **Establish public trust** – The principles can serve as a testimony of a municipality's willingness to take responsibility and act in the best interest of resident privacy and security.
- **Align siloed departments** – The principles can serve as a north star for guiding the implementation of privacy practices across departments that may have a different understanding of privacy.
- **Create a culture of privacy** – The principles are aspirational in nature. They form the basis for everyone to carry out their responsibilities by creating a shared vision for embedding privacy in their daily operations.

3.1.3 WHAT ARE SOME OF THE PROMINENT PRIVACY PRINCIPLES?

There are several privacy principles available that can provide a starting point for coming up with a city or community's privacy principles. The following two sets of principles taken together are comprehensive and representative of the most commonly adopted privacy principles across the public and private sectors.

- **Organization for Economic Cooperation and Development (OECD)'s Fair Information Practice Principles (FIPPs)** - FIPPs were among the first internationally recognized privacy principles that served as privacy guidelines for the public and the private sectors across countries. Since then, the eight specific principles have evolved and have been infused into the privacy framework of several national and state governments around the world.
- **Privacy by Design** – The foundational principles of a framework (see 3.1) that bakes in privacy into an organization's design and operations of the IT system, network, infrastructure, and business practices with seven founding privacy principles.

[2] Clopton, R. (2021). Effective Privacy Management in Local Government. Berkeley Public Policy Journal, Spring, 66–79. https://bppj.berkeley.edu/spring-2021-journal/

FIG 1. FIPPS AND PRIVACY BY DESIGN

FIPPS	PRIVACY BY DESIGN
• Collection Limitation • Data Quality • Purpose Specification • Use Limitation • Security Safeguards • Openness • Individual Participation • Accountability	• Proactive not reactive—preventative not remedial • Privacy as the default setting • Embed privacy into design • Retain full functionality (positive-sum, not zero-sum) • Ensure end-to-end security • Maintain visibility and transparency—keep it open • Respect user privacy—keep it user-centric

Source: Author based on FIPPS and Privacy by Design

3.1.4 WHAT ARE THE KEY CONSIDERATIONS AND COMMON THEMES THAT ARE PRIMARILY ADDRESSED IN PRIVACY PRINCIPLES?[3]

The most common considerations and themes that emerge in the privacy principles adopted by organizations across public, private, and non-profit sectors are as follows:

TABLE 1. COMMONLY ADDRESSED PRIVACY CONCEPTS

PRIVACY CONCEPT	DESCRIPTION
Accountability	Who should be accountable for breaches of responsibility and trust? How should accountability be ensured? What does accountability look like?
Accuracy	How should data be maintained in its most accurate form? Is the information fit for the use to which it will be employed?
Equity	How can the data be collected and analyzed responsibly so that it does not discriminate or mistreat information from vulnerable populations in a biased manner to exploit or harm vulnerable populations directly or indirectly?
Ethics	How can the moral obligation to evaluate the risks to individual privacy of any practice that collects and uses information be upheld?
Informed Consent	How will individuals be informed about how their information will be used and be provided with an option to deny collection or use of data?
Limiting Collection/Retention	How can we ensure that only the specific information required to provide services is being collected and stored only for as long as it is needed?

[3] Clopton, R. (2021). Effective Privacy Management in Local Government. Berkeley Public Policy Journal, Spring, 66–79. https://bppj.berkeley.edu/spring-2021-journal/

PRIVACY CONCEPT	DESCRIPTION
Managing Data/Stewardship	How will the information be protected and stored in a manner that prevents unauthorized access?
Public Record Disclosures	How will we ensure individual privacy when responding to requests for public records while still complying with regulations governing requests?
Review of Systems	How and who will review current and future information systems and evaluate their potential impacts on the privacy of individuals?
Third Party Access	How and who will monitor interactions with third parties, including limiting access to information where possible and requiring third parties to comply with privacy principles?
Transparency	How can we ensure that the public is aware of what information is collected, how it is used, and who may have access?

Source: Modified based on Clopton (2021).

Of these eleven considerations: (i) Accountability, (ii) Informed Consent, (iii) Limiting Collection/ Retention, (iv) Third Party Access and (v) Transparency are among the most common and recurring for principles adopted by local governments.

3.1.5 ARE THERE ANY GOOD EXAMPLES OF CITIES OR COMMUNITIES THAT HAVE ADOPTED THEIR OWN PRIVACY PRINCIPLES?

At least seven local governments have adopted privacy principles in the past five years. Seattle did so in 2015, followed by Kansas City in the same year. Since then, several jurisdictions have adopted privacy principles, including Portland (2019); San Jose (2019); Oakland (2020); Mesa, AZ (n.d.); and New York City (2021).

It is difficult to pick one as the best. To some extent, they are all a work in progress and will need updating over time. However, if you are looking for a starting point, see principles from Seattle, Oakland or Portland. Refer to the resource repository for some more examples of privacy principles and to learn more about how these cities developed and implemented their privacy principles.

QUESTIONS TO CONSIDER

- What public value does your organization want to create through the principles?
- Who should be involved in the process of drafting the principles?
- Who should vet and approve the principles?
- Who will be responsible for implementing the principles?
- How will we communicate the principles to the residents and to the employees?
- Is there organizational support for the principles and the resource necessary to implement?

3.1.6 HOW ARE PRIVACY PRINCIPLES DIFFERENT FROM PRIVACY POLICIES?

Cities and communities may choose to incorporate their privacy principles within their privacy Policies or they may decide to keep them separate. The City of New York has a comprehensive Citywide Privacy Protection Policies and Protocols which provides a detailed description of its privacy practices and policies.

TABLE 2. PRIVACY PRINCIPLES V/S PRIVACY POLICIES

PRIVACY PRINCIPLES	PRIVACY POLICIES
Principles guide values for the entire organization.	Policies are internal statements that governs an organization or entity's handling of personal information. They direct members of the organization who might handle or make decisions regarding the personal information, instructing them on the collection, use, storage and destruction of the data, as well as any specific rights the data subjects may have and may also be referred to as a data protection policy.[5]
They are generally not legally binding and are meant to be aspirational in nature.	They are legally binding.

Source: Author.

3.1.7 WHAT ARE THE DOS AND DON'TS OF CREATING A PRIVACY POLICY?

DOS

- Follow applicable rules and laws - check for local rules that may particularly apply to your jurisdiction.
- Make it easy to opt-out of data collection.
- Make sure that the privacy policies are easily accessible on your website.
- Make sure the privacy policies align with data governance practices.
- Restrict activities to those that support use case.
- Make sure that policies and practices are documented, and sufficient training is provided to understand them.

TIP

Find out about the privacy law(s) in your state using International Association of Privacy Professional (IAPP)'s State Comprehensive - Privacy Law Comparison tracker.

[5] International Association of Privacy Professionals (IAPP). (n.d.). Glossary of Privacy Terms. IAPP. Retrieved April 2021, from https://iapp.org/resources/glossary/#paperwork-reduction-act-2

DON'TS

- Don't use technical or legal jargon.
- Don't miss important clauses. Be very specific and provide details on any exclusions that may apply.
- Don't write long blocks of text.
- Don't use inconsistent policies across departments.
- Don't update privacy policies without notice.
- Don't assume you know what your community expects.

CAUTION: PUBLIC RECORD ACT (PRA), OPEN DATA AND PRIVACY

- PRAs vary from state to state. Some states may favor open data over privacy. This leads to a conflict as open data can have a lot of information being collected that could reveal individual identities or behavioral patterns that can have significant impact on groups and individuals. Furthermore, collection of different datasets can introduce new privacy challenges even if the individual datasets are anonymized.
- This inconsistency from state-to-state leads to gaps in judicial understanding. For instance, date and place may not be considered personally identifiable information (PII) in one state but it can be PII in another state.

QUESTIONS TO CONSIDER

- Who should be involved in the process of drafting the policies?
- How will you ensure that all practices have been disclosed correctly?
- Is the disclosure policy in alignment with Public Records Act (PRA)?
- Who will be responsible for enforcing and updating the policies?
- How will we obtain a clear agreement/ informed consent to privacy policies for residents?
- How will we communicate the privacy policies to the residents?

TIP

Still confused about PII? Refer to this guidance on PII by U.S. Department of Labor.

3.2. CREATING ACCOUNTABILITY FOR PRIVACY

Creating accountability by deploying safeguards both internally and externally is needed for operationalizing privacy principles and policies across all departments of a city or community.

3.2.1 WHAT IS THE ROLE OF PRIVACY PROFESSIONALS IN CREATING ACCOUNTABILITY INTERNALLY?

A number of cities and communities are hiring a dedicated Chief Privacy Officer (CPO) to oversee the privacy and data protection practices. This practice runs parallel to the Privacy Act of 1974 that requires federal agencies to have a privacy officer as well as the private sector practice to appoint a CPO. Having a dedicated CPO is a good practice because: (i) it creates accountability and a clear line of authority by having a dedicated position for privacy; and (ii) it sends a signal that the organization cares about privacy and thus strengthens public trust. If you cannot hire a CPO, consider existing job functions most impacted by privacy risk where the initial privacy approaches can be applied.

3.2.2 WHAT ARE THE KEY CONSIDERATIONS FOR CREATING INTERNAL ACCOUNTABILITY?[6]

- **Awareness and Transparency** – Information silos are commonplace across departments in cities and communities. Early communication and awareness training can help to harmonize privacy practices across departments. This includes engaging with department heads and employees early in the process to get their buy-in on privacy practices.
- **Identifying a Line of Authority** – A top-down approach requires establishing a chain of command to provide a shared vision and disseminate resources to those who are not familiar with the privacy practices. This would also depend on where the office of CPO is housed within the organization. The most common departments for a privacy office are Information Technology (IT), Human Resource (HR), and Legal.
- **Creating a Culture of Privacy** – Privacy should be fostered as a culture and value to conduct the day-to-day operations of the city or community. Creating a culture requires more than appointing a CPO. Cities and communities should nurture privacy champions within each department to facilitate awareness, training, and reinforcement of privacy principles to create a shift in culture and attitude towards privacy practices.

DEFINITION

Accountability is one of FIPPs principles' that pertains to a data controllers (cities and communities) responsibility to comply with measures which gives effect to its privacy principles.

TIP

See how Department of Homeland Security (DHS) describes the authorities and responsibilities of the Chief Privacy Officer here.

QUESTIONS TO CONSIDER

- Which department will house the office of the CPO or a lead privacy professional?
- What will the chain of command look like depending on where the office of CPO is housed?
- What should be the medium (complaint line, email, portal, etc.) for reporting potential privacy risks or concerns?

[6] Flores, A., Sharma, J., Yeung, L., Clopton, R., & Miyano, S. (2020, May). Oakland Resident Data: Understanding What's Collected and Strengthening Privacy. Oakland Privacy Advisory Commission.

- **Training** – The privacy world is constantly evolving which makes training crucial to keep employees abreast with all the changes. Cities and communities should allocate budget for training; however, to get started, they can benefit from the many open-source resources available on privacy. Refer to the resource repository for resources on privacy.

- **Mechanism for Escalation and Red Flagging** – Tied to training is the need for creating a clear mechanism for escalation of potential privacy events. Employees should be trained to identify and report privacy risks and harm. While training will help employees identify potential privacy risks and breaches, having a mechanism for escalation and reporting will bring the matter in front of privacy professionals responsible for ensuring resident privacy.

CAUTION

Privacy risks are different from privacy harms. Risk is related to both the likelihood and impact of a privacy event whereas harm only relates to potential damages resulting from a privacy event.

3.2.3 WHAT ARE THE KEY CONSIDERATIONS FOR CREATING EXTERNAL ACCOUNTABILITY?[7]

- **Privacy Remedy and Redressal** – The vacuum of laws and rules around privacy makes it challenging for cities and communities to tackle remedies for privacy harms. As such, cities and communities should think beyond the legal requirements and proactively consider the consequences of a privacy event. An ombudsperson role is one interesting way to think about complaint lines for citizens to be heard, to make corrections, and access as well as delete their data. To this end, cities and communities should create a channel for residents to directly question the handling of their data. This has been a trend in the private sector, and it shouldn't be too long before people ask local governments (cities and communities) for the same. This goes hand-in-hand with the need for creating an internal escalation mechanism for reporting to ensure a feedback loop is in place to keep a check on privacy events.

- **External Oversight** – Accountability does not necessarily lead to trust when it is purely internal. Therefore, an external oversight is needed to keep a watchful eye. This can be done either through dedicated privacy advisory boards or city councils. This may also include engaging with local academic institutes and independent privacy researchers to conduct privacy evaluation and assessments. Annual reports and/or periodic assessments (triggered by material changes in organization or technology) and making them publicly available can go a long way in establishing transparency and accountability.

QUESTIONS TO CONSIDER

- How can we evaluate scenarios of what happens in case of individual privacy violation?
- How will we inform the residents in case of a breach?
- What corrective actions should be undertaken in case of a privacy event?
- Who will take corrective actions?
- What is at stake in case of a privacy event?

TIP

Refer to this model legislation from Oakland to form your own Privacy Advisory Commission.

[7] Based on interviews with privacy experts.

TABLE 3. EXAMPLE OF STAKEHOLDERS ON A PRIVACY OVERSIGHT BOARD

CHIEF PRIVACY OFFICER (CPO)/ PRIVACY HEAD
Head of the Department leading the project
Representative(s) from a local or regional entity such as non-profits, faith-based organization
Representative(s) from academia
Representative(s) from the communications team
Representative(s) from vendor/private sector player

Source: Author.

3.3. EVALUATING PRIVACY RISK

Cities and communities should proactively assess privacy risks. Cities and communities should undertake risk assessments before as well as after the implementation of a smart city project. This section discusses: (1) how cities and communities should engage with vendors before adopting a smart city application; and (2) how cities and communities can evaluate privacy risks after the deployment of a smart city project.

3.3.1 WHAT CAN CITIES AND COMMUNITIES DO TO EVALUATE TECHNOLOGY SOLUTIONS OFFERED BY VENDORS?

Cities and communities are becoming increasingly dependent on external vendors as they digitize and adopt smart city solutions. City and community leaders should hold the vendors to the same or even higher standards of privacy as they hold themselves.

- Role of Due Diligence – Establish requirements for due diligence for vendor assessments, audits and identify who might have downstream access to data to ensure the data stays in safe hands. Be curious and ask the right questions, not stopping at the first answer, laying out requirements clearly, and being good consumers and skeptics of information making decisions in the public interest. City and community leaders should understand what the technology is, what it's capable of, who it impacts, its limitations and safeguards needed to limit potential harm. Refer to IAPP's privacy vendor list for a directory of companies that can help you protect data, provide services, meet regulatory requirements, respond to breaches, set policies and more.

QUESTIONS TO CONSIDER

- What problem is the organization trying to solve?
- What data needs to be collected?
- Is the data collection justified?
- Can data collection be minimized?
- Who ensures data is in safe hands?
- Does the vendor have experience deploying the proposed solution?
- How will the vendor transfer knowledge to the city or community employees?
- Do you have the social license to implement the technology (such as facial recognition)?

TIP

Refer to the checklist created by the International Association of Privacy Professionals (IAPP) for expedited vendor privacy and security assessment.

[8] Read the foundational principles of Privacy by Design in Section 1.3.

- Privacy by Design – Privacy by design is a popular framework used by the private sector as an efficient and cost-effective way to safeguard privacy[8]. Privacy by design has a lot in common with the principle of minimization. It requires understanding and limiting the collection of data to what is truly needed to accomplish a set of goals. Cities and communities should establish a tangible connection between what is being collected, how it is being collected and how it will be used. Ask your vendor if they comply with principles of privacy by design (see 1.3) or with National Institute of Standards and Technology (NIST)'s privacy framework. Request proof of compliance with the framework, if required. There are two arguments for baking in privacy by design for smart city applications:
  - **Business Rationale for Collecting and Retaining Data** – We have learned from city records management processes that it is costly to hold data. The cost is both in terms of storage as well as the enormous liability tied to the risk of personal data breaches. A caveat here is that there are some laws or rules that may require some departments to retain data for certain periods of time.
  - **Building Better Tools and Developing Better Projects** – Privacy by design allows organizations to consider tradeoffs between potential risks and benefits from data use and address the burning questions regarding privacy upfront. This can save cities and communities a lot of time and resource that they would otherwise spend on building a use case.

TIP

The National Institute of Standards and Technology (NIST)'s Privacy Framework, though designed for the private sector, could be a key steppingstone for many jurisdictions to evaluate where they are, measure how they're doing and evaluate where they want to go.

Privacy by design brings privacy-enhancing technologies and strategic partnerships to the fore. City and community leaders can build trust and earn credibility by working together across public-private partnerships to build systems that are auditable by external researchers. Building systems that are auditable and minimize data collection to what is needed is a powerful way to earn public trust.

3.3.2 HOW CAN CITIES AND COMMUNITIES EVALUATE AND MONITOR PRIVACY RISKS?

Potential privacy events directly affect individuals at the micro-level. The effects that individuals may face vary from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm. As such, these micro-level harms manifest at the macro-level and affect cities and communities in ways of lawsuits, loss of public trust, noncompliance costs, and reputational harms.

QUESTIONS TO CONSIDER

- Who should be involved in the assessment?
- How often are the assessments required?
- Will the assessments be made available publicly?
- Which use cases require comprehensive PIA?

- **Privacy Risk Management** – A cross-organizational set of processes that helps cities and communities understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks.
- **Privacy Risk Assessment** – A sub-process for identifying and evaluating specific privacy risks. In general, privacy risk assessments produce the information that can help cities and communities weigh the risks and benefits of data collection and processing as well as determine the appropriate response or remedy to identified risks. Performing a consistent risk assessment for privacy-facing initiatives allows the staff and community to understand the risks of the project as well as how that compares across projects. The level of detail of the risk assessment interview you use will depend on the privacy culture in place. Higher-level risk assessments are good for early privacy programs.
- **Privacy Impact Assessment (PIA)** – A tool to conduct a systematic risk assessment to address potential privacy risks. DHS provides detailed guidance on the reasons for conducting a PIA as well as guidance on how to conduct a PIA. Documenting PIAs and publishing them are a great way to show that the city or community is proactively taking measures to safeguard individual privacy.

TIP

Refer to this draft template for privacy risk assessment prepared by Future of Privacy Forum

DEFINITION

DHS describes PIA as a decision tool to identify and mitigate privacy risks.

CAUTION: PIAs ARE GREAT BUT...

While PIAs are excellent tools for evaluating privacy risks and communicating them to the public, they are also time consuming and require some level of expertise. For cities and communities that are resource constrained they should decide which technologies or data uses require a comprehensive PIA. This requires differentiating between high and low risk technologies. A risk assessment matrix that evaluates risk on the scale of impact and likelihood may come in handy technologies. may come in handy to identify high risk technologies.

3.3.3 SEVERAL CITIES AND COMMUNITIES HAVE LIMITED RESOURCES AND EXPERTISE TO INDEPENDENTLY EVALUATE TECH CAPABILITIES. HOW CAN CITIES AND CONNECTED COMMUNITIES OVERCOME THIS CHALLENGE?

- **Network Effect and Collaborations** – Cities and communities can benefit from the network effect and collaboratively undertake privacy impact assessments. This includes working with academic experts, consultants (hired as well as pro bono), forming a working group or reaching out to advocacy organizations and leveraging their expertise and experience in civic tech. Resource constrained cities should procure the experience and the expertise from outside, learn from it, institutionalize it and build it in-house over time. In addition, you may benefit from researching other jurisdictions that already have used the technology and experienced feedback on privacy risk management.

  Cities and communities who do not have the resources or expertise to run their own differential privacy algorithm or build their own systems should partner with academic institutions and independent researchers or learn from the experiences of the federal government agencies to build and test use cases.[9]

- **Stepping on the Shoulders of a Giant** – Cities and communities can benefit from the wisdom and experiences of other cities and federal agencies, both domestically and internationally. For instance, DHS publishes PIAs of various technologies. City of Helsinki, Finland has shorter versions of PIA for low-risk technologies.

- **Institutionalizing Knowledge and Decision Making** – Cities and communities can institutionalize knowledge and capacity building by investing time in proper documentation of a use case. Make sure to identify all the features of a project, its potential impacts and risks, mitigation measures and decisions regarding technology. Such practices will go a long way in ensuring consistent and confident decision making across departments. Providing training for employees will also play a big role in codifying knowledge and standardization in decision making.

DEFINITION

Imagine you have two otherwise identical databases, one with your information in it, and one without it. Differential Privacy ensures that the probability that a statistical query will produce a given result is (nearly) the same whether it's conducted on the first or second database.

QUESTIONS TO CONSIDER

- How will the team build relationships with potential stakeholders?
- Which city or federal agency use case aligns most closely with the problem at hand and the jurisdiction?

[9] Differential Privacy definition adapted from Microsoft. (n.d.). Differential Privacy. Retrieved April 2021, from https://www.microsoft.com/en-us/research/publication/differential-privacy/?from=http%3A%2F%2Fresearch.microsoft.com%2Fpubs%2F64346%2Fdwork.pdf

3.4. PRIVACY RESOURCE REPOSITORY FOR CITIES AND COMMUNITIES

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
	UNDERSTANDING PRIVACY		
1	Privacy in the Smart City – Applications, Technologies, Challenges and Solutions	Beginner – Intermediate	Learn more about privacy in the context of smart cities. The paper is a good reference guide to better understand the taxonomies of smart cities, types of privacy, attackers and data sources, and building privacy enhancing technologies.
2	A Taxonomy of Privacy	Beginner	Based on Dan Solove's work, the infographic provides a description of different harms that may arise from breach of privacy. This resource may come in handy for scenario planning or while thinking through the consequences of a potential privacy event.
3	10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade/ Future of Privacy Forum (FPF)	Beginner – Intermediate	This short paper provides information about top 10 privacy risks to look out for and 10 technologies to bake in privacy by design.
4	Differential Privacy Group/ Harvard University Privacy Tools Project	Intermediate – Advanced	Learn more about differential privacy and how it can be used.
5	Course and Educational Material on Differential Privacy/ Harvard University Privacy Tools Project	Intermediate – Advanced	
6	Nothing to Hide: Tools for Talking (and Listening) about Data Privacy for Integrated Data Systems/FPF	Beginner	Refer to Appendix A of the report to understand the basics of privacy (pg. 12), fair information practice principles (pg. 14) and refer to a list of privacy tools and resources (pg. 15-16).
7	Oakland Resident Data: Understanding What's Collected and Strengthening Privacy	All	This is a report prepared by graduate consultants from Berkeley Public Policy for the Privacy Advisory Commission of Oakland. The report provides details on the development and implementation of privacy principles in the Cities of Seattle and Portland. The report concludes with recommendations for the City of Oakland based on lessons learned from the experiences in Seattle and Portland.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		PRIVACY LEGISLATION	
8	Free Global Data Breach Notification Law Library/ Radar First	All	A free library that provides: (i) interactive maps to quickly identify U.S. laws pertaining to US states; (ii) incident risk assessment and data breach reporting requirements – as well as penalties for non-compliance; and (iii) details regarding proposed and recently passed legislation.
9	Security Breach Notification Law/ National Conference of State Legislatures	All	List of legislations across 50 states requiring governments to notify of privacy infringement involving personally identifiable information.
10	Comparison of Proposed U.S. Privacy Legislation/IAPP	All	Comparison of the three proposals for a comprehensive privacy legislation.
11	U.S. State Data Breach List/ IAPP	All	Several state agencies publish lists of reported data breaches in the state. Find the links to the lists here.
		PRIVACY IMPACT ASSESSMENT	
12	Privacy Impact Assessment/ Global Smart Cities Alliance	Beginner – Intermediate	A great resource to understand the fundamentals of PIA. It also provides references and links to a number of PIAs done by local, state, federal as well as international governments.
		PRIVACY PRINCIPLES	
13	U.S. Chamber Privacy Principles	All	10 privacy principles by U.S. Chamber to ensure consumers benefit from responsible use of data.
14	Internet Association Privacy Principles	All	Six principles and policy considerations by the Internet Association to modernize national privacy legislation.
15	The GDPR Principles	All	Read and understand the six GDPR principles. These are primarily inspired from FIPPs.
16	Privacy Principles for Facial Recognition Technology in Commercial Applications, FPF	All	FPF introduced their seven privacy principles to address concerns around personally identifiable information (PII) collected by systems using facial recognition technology.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		OPERATIONALIZING PRIVACY PRINCIPLES	
17	The City of Seattle Privacy Program	All	Provides information about setting up a privacy program, how it will be supported, department obligations, and what the privacy review process will look like.
18	Implementation Guide: City of Oakland Privacy Principles	All	The document provides an explanation of each principle and examples of how cities can operationalize those principles across the different departments.
		MISCELLANEOUS	
19	What Cities Can Learn from the Nation's Only Privacy Commission	All	Lessons learned from Oakland's Privacy Advisory Commission.
20	Best Practices Repository/FPF	All	A repository of privacy best practices and resources for smart city applications ranging from cars, drones to smart grid.
21	A Toolkit Fighting Local Surveillance/ Oakland Privacy	All	A great resource prepared by ACLU of Northern California and Oakland Privacy. This step-by-step guide provides loads of advice on coalition-building, public education, strategy, research, messaging and advocacy and samples of useful documents.

Source. Author.