Implementation Guidance: City of Oakland Privacy Principles

This document accompanies the City of Oakland's Privacy Principles (the "**Principles**"). It provides guidance on the implementation of the Principles, including a discussion of the foundation and scope of each principle, as well as examples to illustrate how the City might apply each Principle in its day-to-day operations.

The goals of the Principles are threefold. First, the Principles serve as a values statement establishing how the City protects Oaklanders' privacy and security. Second, the Principles will help guide the development of future privacy policies for the City. Third, the Principles are intended to harmonize the way different City departments think about privacy when approaching a new technology or a new issue with data collection.

The Principles open with a preamble that establishes the purpose and tone of the Principles. The Principles themselves are organized into seven different categories: (1) Equity; (2) Collection and Retention; (3) Management of Personal Information; (4) Third Party Relationships; (5) Public Records Disclosures; (6) Transparency; and (7) Accountability. This guidance document contains separate sections for each Principle, explaining its purpose and foundation, as well as providing examples of how each Principle applies to specific situations. The examples are intended to illustrate how City departments would take the Principles into account, rather than to dictate the result that consideration of the Principles would require.

DESIGN AND USE EQUITABLE PRIVACY PRACTICES

Community safety and access to city services should not come at the expense of any Oaklander's right to privacy. We recognize that our collection and use of personal information has disadvantaged marginalized communities at different periods during Oakland's history. We aim to avert future inequities by collecting information in ways that do not discriminate against any Oaklander or Oakland community. When possible, we will offer clearly communicated alternatives to the collection of personal information at the time of collection.

I. Purpose and Goals of the Equity Principle

The Equity Principle guides the City of Oakland's commitment to collect and use personal information equitably across communities and groups in the course of providing city services. The Principle acknowledges that at different points in Oakland's history, marginalized communities have faced disproportionate surveillance or other intrusions into their privacy.[1] It also recognizes the importance of respecting Oaklanders' choices in whether and how their personal information is collected and used by the City. As the Principle explains, "[the City will] aim to avert future inequities by collecting information in ways that do not discriminate against any Oaklander or Oakland community." Therefore, the City will not collect information in unfair ways that target specific communities or neighborhoods, or overlook—and thereby risk perpetuating—past discrimination.[2] The City already takes steps to prevent the unfair targeting of certain groups by following the state's sanctuary law, the California Values Act, which prevents local law enforcement from aiding federal agencies in deportations.[3]

Equal protection under the law is ensured at the federal, state, and local levels. The Fourteenth Amendment of the United States Constitution guarantees the equal protection of all persons under the law.[4] The California Constitution contains its own equivalent equal protection clause, which states that a "person may not be deprived of life, liberty, or property without due process of law or denied equal protection of the laws."[5]

---

[1] *See* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 Wash. L. Rev. 1595, 1617–18 (2016) (describing how the Black Panther Party became a target of the FBI's COINTELPRO surveillance investigation in the 1960s).

[2] The City of Oakland defines fairness to mean "that identity—such as race, ethnicity, gender, age, disability, sexual orientation or expression—has no detrimental effect on the distribution of resources, opportunities and outcomes for our City's residents." City of Oakland, *Oakland Equity Indicators: Measuring Change Toward Greater Equity in Oakland* at 8 (2018) [hereinafter "*Equity Indicators Report*"], https://s3-us-west-1.amazonaws.com/beta.oaklandca.gov/pdfs/2018-Equity-Indicators-Full-Report.pdf.

[3] Cal. Gov. Code § 7284–7284.12 (effective Jan. 1, 2018).

[4] U.S. Const. amend. XIV, § 1.

[5] Cal. Const. art. I, § 7.

The City of Oakland's own commitment to equity is illustrated by its pioneering partnership with the City University of New York's Institute for State and Local Governance to develop an Equity Indicators tool.[6] The Department of Race and Equity developed the Oakland Equity Indicators Report in order to help City staff "make data-driven decisions about programs and policies to . . . ensure people have equitable access to opportunities and services that we administer or deliver, directly or by contract."[7] The City of Oakland distinguishes equality—"giving everyone the same thing, regardless of outcomes"—from equity, which means "ensuring that people have access to the same opportunities or services[.]"[8] The City also fosters equity through its "Equal Access to Services" ordinance, which establishes standards and procedures to help Oaklanders with limited proficiency in English can access city services and programs.[9]

The Equity Principle brings the same values that animate these efforts to the City's protection of residents' privacy interests.

II. Examples Illustrating the Equity Principle in Practice

Example #1: Education and Chronic Absenteeism

The Oakland Unified School District ("**OUSD**") wants to measure the percentage of students who are chronically absent. Studies have shown that chronic absenteeism significantly affects a child's ability to succeed in school and therefore influences a child's access to later opportunities and success.

Since the purpose of the measurement is not to enforce truancy laws against any student or their parents, OUSD does not collect names or other personal information. Therefore, OUSD decides to collect only the demographic data associated with students whose attendance rate is 90% or less (missing 18 or more days in a 180-day school year), regardless of whether the absences are excused or unexcused. Following the Equity Principle's guidance, OUSD also gives parents the choice to opt-out of collection of racial or other demographic information.

Example #2: Department of Transportation and Mobile Automated License Plate Readers

The Department of Transportation ("**DOT**") wishes to employ vehicle-mounted Automated License Plate Readers ("**ALPR**") in order to manage and enforce parking violations. Before getting approval from the City Council to fund the acquisition, DOT presents an Anticipated Impact Report and Use Policy for the Privacy Advisory Commission ("**PAC**") to review and make a recommendation to the City Council.

---

[6]. *Equity Indicators Report* at 8.
[7]. *Id.* at 12
[8] City of Oakland, *Learn More about the Department of Race and Equity*, *available at* https://www.oaklandca.gov/resources/race-matters (last visited Apr. 26, 2019).
[9] Oakland, Cal., Ordinance 12324 § 2.30.030.

DOT is aware of the community concern about having ALPR on at all times while the vehicle is moving through marginalized communities. With that concern in mind, DOT decides that it will turn on ALPR only when patrolling the areas in which parking violations occur, which are largely commercial districts and neighborhoods with Resident Permit Parking areas. To further address the concern, DOT provides anonymized data to the Department of Race and Equity to audit and help determine whether the collection is having a disparate impact.

Example #3: Libraries and Surveillance Cameras

The Oakland Public Library receives extra funding and a mandate to install surveillance cameras at several of its branches. The Library considers installing the new cameras in the branches with the highest number of incidents. However, it recognizes that this metric will predominantly affect marginalized communities.

The Library wants to proactively address how cameras affect the branches' visitors, so it reaches out to PAC with its concerns. At the same time, library branches institute a comment box policy so patrons can submit their thoughts on the use of surveillance cameras in each branch anonymously. Only after considering both the insight from PAC and the collective patron feedback does the Oakland Public Library determine whether and where to place the new cameras.

LIMIT COLLECTION AND RETENTION OF PERSONAL INFORMATION

We believe that we should collect and store personal information only when and for as long as is justified to directly serve the specific purpose for which it is collected, such as to protect Oaklanders' safety, health, or access to city services. We will continue our practice of reaching out to Oaklanders for their views on the information we collect and how we use it. We also will look for new opportunities for outreach.

I. Purpose and Goals of the Collection and Retention Principle

Considering the privacy implications of collecting personal information before the collection begins helps prevent privacy violations. And thoughtful retention is just as relevant to protecting individual privacy as collection. The Collection and Retention Principle affirms the City of Oakland's commitment to limit its collection of personal information, collecting only what is needed in order to provide a city service and only for as long as required. By stating that personal information will be collected "only when and for as long as is justified," the Principle helps ensure that personal information will not be used in unintended or unexpected ways. This approach prevents the City from misusing "sleeping data," which includes stored or unused data that is digitized and then repurposed for an unforeseen use. The Principle also reflects the importance of outreach to the democratic process: residents should be able to voice concerns both before and after information is collected.

This Principle guides data collection and retention within the boundaries of existing law. The State Records Management Act directs the California Secretary of State to establish and administer a records management program, which includes the retention and disposal of state records.[10] Section 12275 of the Act provides that "[a] record shall not be destroyed or otherwise disposed of by an agency of the state, unless . . . the record has no further administrative, legal, or fiscal value and . . . the record is inappropriate for preservation in the State Archives."[11] Under the Act, government agencies must establish and maintain a records retention schedule.[12] The schedule must detail what records the agency will keep, how the records will be managed, and how the agency will legally dispose of non-permanent records.[13] At the local level, cities must retain any record that is less than two years old.[14] However, records of "routine video monitoring" may be destroyed after one year and recordings of telephone and radio communications may be destroyed after 100 days with approval from city council and the written consent of the

[10] Cal. Gov. Code §§ 12270–79.
[11] Cal. Gov. Code § 12275.
[12] Cal. Gov. Code § 12274.
[13] *Id.*
[14] Cal. Gov. Code § 34090.

city attorney.[15] Duplicates less than two years old may be destroyed if they are no longer required.[16]

II. Examples Illustrating the Collection and Retention Principle in Practice

Example #1: Fire Department and Body Heat Cameras

The Oakland Fire Department wants to add body-worn cameras to firefighter uniforms in order to aid in search and rescue. Because the Fire Department wants to use the body-worn cameras to help search and rescue operations, it determines that the cameras do not need to record live footage, which would record images of the immediate surroundings and any persons within the camera view. Instead, the Fire Department decides that cameras that record only heat signatures are sufficient to help firefighters find and rescue Oaklanders who may be trapped in a fire.

The Fire Department introduces the heat signature cameras in its search and rescue operations. All recordings are retained according to the department's retention schedule and then destroyed.

Example #2: Libraries Collecting Less Patron Data

The Oakland Public Library collects the name, date of birth, address, gender, phone number, and other personal information from patrons when applying for a library card. Whenever a patron checks out a book, that book is tied to the patron information associated with that patron's account.

The Library decides to redouble its efforts to foster community and move away from generating revenue from lending activities. As a result, fine collection for overdue books becomes less of a priority. Additionally, in view of the USA PATRIOT Act's provision granting law enforcement access to patron records in certain circumstances,[17] the Library decides to limit its collection of information so as not to be subject to requests from agencies, knowing that the information could be used to target vulnerable patrons. The Library decides to collect only first and last names, for which a patron may use an alias, and dates of birth. A patron is not required to provide an address or phone number but may choose to do so. Thus, when a patron checks out a physical book, it is tied only to the information associated with the patron's library card.

Example #3: Public Health and Childhood Asthma

The Department of Race and Equity wants to measure the rates of asthma-related emergency visits to hospitals in the Oakland area in order to determine racial disparities in the incidence of

[15] Cal. Gov. Code § 34090.6.
[16] Cal. Gov. Code § 34090.7.
[17] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, § 215 (2001).

asthma in children for the Equity Indicators Report. Childhood asthma has been linked to poor housing conditions, and the Department wishes to explore that connection in its report.

Cognizant of the privacy and safety concerns associated with a child's personal information, the Department of Race and Equity decides to collect only the race and residential data for asthma-related emergency room visits for children under five years of age. Rather than collecting each child's name and address, the Department decides to collect only zip codes and census block data, which is sufficient to determine the housing conditions of neighborhoods. The Department also puts in place a retention schedule for eventual deletion of the information.

MANAGE PERSONAL INFORMATION WITH DILIGENCE

The personal information of Oaklanders should be treated with respect. We handle all personal information in our custody with care, regardless of how or by whom it was collected. To maintain the security of our systems, we review and regularly update software and applications that interact with Oaklanders' personal information. Further, we recognize that deletion, encryption, minimization, and anonymization can reduce misuse of personal information. We aim to make effective use of these tools and practices. Additionally, we combine personal information gathered from different departments only when we must.

I. Purpose and Goals of the Management of Personal Information Principle

The Management Principle affirms the City of Oakland's commitment to protect the privacy of residents' personal information once that information has been collected by the City. Responsible data management helps the City build trust: The City can provide better services to Oaklanders if Oaklanders feel more secure in the handling of information shared with the City. To that effect, the Management Principle covers the storage, security, and accessibility of personal information of Oakland residents with a specific focus on information security practices. How the information is collected is irrelevant to these practices, which come into play once information becomes part of the City's records. Additionally, the Management Principle limits aggregation of personal information across different City departments to those instances where aggregation is necessary for the City to provide services.

Minimization, encryption, anonymization, and deletion are identified in the Management Principle because these are best practices for information management. Data minimization is the act of following a purpose-specific approach to collecting data and gathering only the data necessary to provide city services. Encryption is the process of encoding data to prevents access by unauthorized individuals. Anonymization is the process by which personal data is obscured to inhibit deriving from data the identity of the individual who provided it. Deletion is the act of deleting any information that is not necessary for the City to provide services to residents.

The newly enacted California Consumer Privacy Act ("**CCPA**") gives California consumers the right to demand that business delete personal information collected from that consumer.[18] It also provides a list of measures to protect personal information, including pseudonymization and deidentification.[19] Collectively, these provisions show the importance of technological safeguards to protect individual privacy. The Management Principle similarly identifies available measures to protect Oakland residents' personal information that the City collects and stores.

---

[18] *See* California Consumer Privacy Act of 2018, L. 2018 ch. 55 (A.B. No. 375), codified at Cal. Civ. Code § 1798.100 *et seq.*, § 1798.105(a) [hereinafter **"CCPA"**]. The CCPA is currently undergoing amendment and becomes operative January 1, 2020.

[19] *See* CCPA §§ 1798.100, 1798.140, 1798.145.

The Principle's direction to "make effective use" of these measures implies that use of those measures, and others, will evolve over time.

II. Examples Illustrating the Management Principle in Practice

Example #1: City Clerk's EMT Records

An employee at the City Clerk's Office received an automated notice from Alameda County regarding an Oakland resident's use of Emergency Medical Technician (**"EMT"**) services. The Oakland resident had suffered a heart attack and another Oakland park visitor had called emergency services, which routed to the County EMT hotline. The County hotline dispatched an ambulance to the scene. Because of the healthcare implications, the paramedics on duty collected a substantial amount of health information about the patient, including the patient's name, date of birth, medical history, current medications, insurance information, and emergency contacts.

Because all the information collected is personal information, privacy concerns about the safety and security interests of Oakland residents are implicated. In order to best protect the privacy of the individual who suffered the heart attack and of the individual who placed the call to emergency services, the employee at the City Clerk's Office followed Oakland City policy and shredded all the personal information included in the notice.

Example #2: Primary Languages and ICE

To improve classroom outcomes, administrators at several schools in the Oakland Unified School District (**"OUSD"**) want to conduct a survey about primary languages spoken in the home of students enrolled in Head Start programs. The administrators create a survey working group made up of teachers from different schools within the Oakland community. Despite the fact that Oakland has passed a Sanctuary City Ordinance that prevents the City's departments and officials from turning over immigration information to Immigration and Customs Enforcement ("**ICE"**), the group is concerned that this survey data can be used by other federal law enforcement agencies to collaborate with ICE and target neighborhoods for immigration enforcement.

To respond to this concern, the working group proactively anonymizes the results and removes personal information that can be used to reverse-engineer identities from the information collected. Additionally, since this will be a multi-school survey, the group codes the results such that individuals not involved in the administration of the survey will not be able to determine data for specific schools without OUSD's involvement and approval. Finally, school administrators verify that the server storing the survey data has been updated with the latest security patches.

Example #3: Public Works Volunteer Program Application Process

An employee at the Department of Public Works has been tasked with creating a volunteer program that provides opportunities to help beautify Oakland neighborhoods and clear city drains. The Department of Public Works wants to make this Adopt-a-Drain Program accessible to all Oaklanders in order to create a database of potential volunteers for future projects. To create the

volunteer database, the Department of Public Works has to collect substantial amounts of personal information about the applicants, some of which is highly sensitive.

Recognizing the importance of ensuring the privacy and security of individuals applying to be volunteers, the Department of Public Works collaborates with the IT Department from an early stage to design a secure application system for the Adopt-a-Drain Program. The application system is regularly updated and protected from being accessed by unauthorized parties. The Department also informs all potential applicants about this new, protective application portal on the application website.

EXTEND PRIVACY PROTECTIONS TO OUR RELATIONSHIPS WITH THIRD PARTIES

Our responsibility to protect Oaklanders' privacy extends to our work with vendors and partners. Accordingly, we share personal information with third parties only when necessary to provide city services, and only when doing so is consistent with these Principles. When the law permits, we will disclose the identity of parties with whom we share personal information.

I. Purpose and Goals of the Third-Party Relationships Principle

In the course of providing city services, the City sometimes must exchange personal information with third parties. The Third-Party Relationships Principle extends the City's commitment to protect Oaklanders' privacy to parties that work with the City. The City engages with a range of vendors and partners that fall into two broad categories: City entities and non-City entities. The City will share personal information with these third parties—whether City or non-City entities—only to the extent necessary to provide city services, and to the extent that this sharing adheres to all of the other Principles and applicable laws.

The first category of third-party relationships describes relationships between entities within the City. In general, this category refers to instances in which two or more City departments enter into partnerships involving the exchange of personal information in order to provide city services to residents. These intra-city relationships typically are not governed by a contract and do not involve the exchange of money for goods or services.

The second category of third-party relationships describes relationships between the City and non-City entities. This category is much broader and encompasses the City's relationships with both public and private parties. The City may partner with other public entities outside of Oakland, including departments and agencies in other cities, or at the state, county, or federal levels. The City also enters into contractual, paid relationships with private non-City entities. For example, the City regularly issues requests for proposals from private vendors, who have the opportunity to bid on public projects ranging from the provision of new law enforcement technology to sidewalk repairs and park maintenance.

The City must abide by a variety of contracting policies and legislation when entering into an agreement that might involve information sharing with a third party.[20] Further, Oakland's Sur-

[20] City of Oakland, Contracting Policies and Legislation, https://www.oaklandca.gov/resources/contracting-policies-and-legislation/ (last visited Apr. 1, 2019). For example, in 2001, the City passed an ordinance preventing city contractors under contracts of at least $25,000 from discriminating in the provision of benefits between employees with spouses and employees with domestic partners. *See* Oakland, Cal., Mun. Code § 2.32.010–2.32.110.

veillance Technology Ordinance ("**Surveillance Ordinance**") contains provisions applicable to certain types of third-party information sharing.[21] In general, City Council approval is required whenever the City wishes to enter into a contract with a non-City entity to use surveillance technology, which includes approval for data sharing agreements.[22] The Surveillance Ordinance also requires the City to produce an impact report for each technology it wishes to acquire, including a discussion of potential third party dependencies in handling and storing information generated by the technology.[23] Similarly, the Surveillance Ordinance requires the city to draft a surveillance use policy for each technology it wishes to acquire, which must include a discussion of a policy for third-party data sharing with both City and non-City entities.[24] Lastly, once the City begins to use a particular surveillance technology, the Surveillance Ordinance requires an annual surveillance report, including a discussion of what data was collected and shared with outside entities during use of the technology.[25]

II. Examples Illustrating the Third-Party Relationships Principle in Practice

Example #1: Information Sharing with FEMA After a Wildfire

A major wildfire recently broke out in the Oakland Hills and caused widespread damage. The Oakland Fire Department coordinated with other local and state departments on fire relief efforts, but the extent of damage necessitates federal assistance once the fire is extinguished. The City of Oakland begins conversations with the Federal Emergency Management Agency ("**FEMA**") about receiving federal funding for its disaster recovery efforts. In order to qualify for a grant, the City must provide FEMA with certain information about the number of homes and families impacted, including addresses of these homes and the names of known occupants.

In compiling this file for FEMA, the City gathers only the minimum information necessary to receive the funding. In so doing, it redacts any personal information—such as household income and citizenship status—not relevant to the impact assessment FEMA will need to conduct.

Example #2: Data Sharing Agreement with ALPR Vendor

The City of Oakland, through the Oakland Police Department ("**OPD**"), begins contract negotiations with LicenseCam, a vendor of Automatic License Plate Recognition ("**ALPR**") technology. As part of the contract, LicenseCam requests that the City provide monthly success metrics quantifying how frequently the ALPR technology has helped OPD locate a person of interest. LicenseCam also requests that the City provide the raw data—including images of license plates, makes and models of cars, and names of car registrants—to corroborate these statistics.

---

[21] *See* Oakland, Cal., Mun. Code § 9.64.010–9.64.070.
[22] Oakland, Cal., Mun. Code § 9.64.030(1)(D).
[23] Oakland, Cal., Mun. Code § 9.64.010(6)(I).
[24] Oakland, Cal., Mun. Code § 9.64.010(7)(H).
[25] Oakland, Cal., Mun. Code § 9.64.010(1)(B).

This data sharing agreement is put up for review before the Oakland Privacy Advisory Commission ("**PAC**") in advance of a vote by the City Council. Based upon feedback from PAC, the City modifies the data sharing agreement to state that OPD agrees to disclose the monthly hit rates of LicenseCam, but does not agree to share the information underlying these statistics. OPD reaches this policy decision by concluding that sharing personal information with LicenseCam is not necessary to provide law enforcement services to Oakland residents.

Example #3: Data Sharing Between City Departments

There has been a massive uptick in car break-ins throughout the City of Oakland, particularly in large parking lots adjacent to BART stations, libraries, and event spaces. In an effort to address the situation, OPD requests CCTV video footage from a list of City Departments and divisions known to operate CCTV cameras, including the Department of Transportation, the Oakland Public Library, and the Oakland-Alameda County Coliseum Authority.

Since OPD wishes to gather only the information necessary to resolve the current uptick in car break-ins, it makes clear in its requests to other City entities its commitment to use this video footage only in connection with that specific objective. It also makes a commitment to purge the aggregated video footage per OPD's approved retention schedule.

SAFEGUARD INDIVIDUAL PRIVACY IN PUBLIC RECORD DISCLOSURES

Open government and respect for privacy go hand-in-hand. Providing relevant information to interested parties about our services and governance is essential to democratic participation and civic engagement. We will protect Oaklanders' individual privacy interests and the City's information security interests while still preserving the fundamental objective of the California Public Records Act to require transparency.

I. Purpose and Goals of the Public Records Principle

The Public Records Principle affirms the City of Oakland's commitment to take specific steps to safeguard its residents' privacy when complying with public records requests, and to consider whether and how it will comply with requests where the disclosure could include personal information. While the California Public Records Act ("**CPRA**")[26] already includes privacy and security protections, many of these exemptions are invoked at the discretion of the agency or government entity receiving the request. This Principle helps guide the exercise of that discretion. As the Principle explains, "[o]pen government and respect for privacy go hand-in-hand." The City recognizes its residents' strong and sometimes competing interests in transparency and personal privacy and security, and it is committed to weighing these interests carefully when complying with CPRA requests.

In considering whether the public interest weighs in favor of disclosure, the City will keep top of mind its commitment to foster "democratic participation and civic engagement" through transparency. These words convey the strong interest in disclosing information relevant to matters of public debate or interest. On the other hand, in situations where the City determines the public interest in privacy and security requires redaction of an individual's personal information prior to disclosure of a record, the City will redact in a manner that fully protects the information identified as sensitive. The City will use care in making decisions about redactions where the information requested may not amount to "personal information" in isolation, but may rise to the level of "personal information" if aggregated with other public records.

California enacted the CPRA to implement Californians' fundamental right to access information concerning the conduct of the People's business.[27] While the state passed the law with increased transparency in mind, it also took note of the privacy and security implications that come with increased transparency. In fact, the statute references privacy in its opening sentence: "In enacting this chapter, the Legislature, *mindful of the right of individuals to privacy*, finds and declares that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."[28]

---

[26] Cal. Gov't. Code §§ 6250–76.48

[27] Cal. Gov't. Code § 6250.

[28] Cal. Gov't. Code § 6250 (emphasis added).

Multiple provisions of the CPRA include privacy-related exemptions that give agencies discretion to either not disclose certain information or limit the information disclosed. When exercising its discretion to exempt information from disclosure on the ground that disclosure would constitute an unwarranted invasion of privacy, the agency must weigh the public interest in disclosure against the public interest in privacy and security.[29] The Public Records Principle is intended to guide that exercise of discretion in a way that best furthers twin objectives of transparency and privacy.

II. Examples Illustrating the Public Records Principle in Practice

Example #1: Redacting Documents Responsive to Broad Public Records Requests

A resident submits a CPRA request seeking all emails sent and received by the City in 2018 discussing use of Oakland Paratransit Services. The City receives this request, completes the requisite search, and compiles a file of all relevant emails. However, the file the City compiles contains a set of emails between employees in the Department of Human Services discussing specific residents and their travel routines. The emails contain the full names of many users of paratransit services.

While the City understands the importance of disclosing the records requested, it also considers the privacy implications of disclosing this small subset of emails containing sensitive personnel information about potentially vulnerable residents. In weighing disclosure against privacy, the City determines it must withhold the names and location information of paratransit users.

Example #2: Maintaining Privacy During Law Enforcement Investigations

A reporter submits a CPRA request to the Oakland Police Department seeking any video footage it has of a recent incident in West Oakland that resulted in a police officer discharging his firearm after being called to the scene to investigate an alleged altercation. The City locates the relevant Police Department body camera footage, but upon reviewing it, realizes the altercation in question took place next door to the West Oakland Planned Parenthood. Because of the angle of the camera, it caught footage not only of the altercation, but also of people walking in and out of the Planned Parenthood behind the scene of the dispute.

Since the altercation resulted in the discharge of a firearm by a police officer, it rose to the level of a "critical incident" per the CPRA, giving the City the discretion to determine whether or not to use redaction technology to protect the identities of certain individuals in the recording.[30] Given that those seeking care at a Planned Parenthood facility have a reasonable expectation of privacy, and given that the visitors to Planned Parenthood had no relation to the altercation in question, the City decides it will blur out the faces of those people unrelated to the altercation.

---

[29] California Attorney General's Office, *Summary of the California Public Records Act 2004*, at 7, http://ag.ca.gov/publications/summary_public_records_act.pdf (last visited Apr. 26, 2019).
[30] Cal. Gov't Code § 6254(f)(4)(B)(i)–(ii).

The City leaves all other parts of the footage intact and discloses the partially redacted video recording to the reporter.

Example #3: Promoting Security through Disclosure

The City recently launched a new interface for submitting job applications to the City. Unfortunately, it just discovered a major security vulnerability that would allow an attacker to bypass authentication and access sensitive personnel files maintained on a related webpage by the Human Resources Management Department. The vulnerability could take weeks to patch, and it currently remains exploitable. Meanwhile, a curious IT professional, submits a CPRA request to the City of Oakland seeking information about its public website, www.oaklandca.gov, including the new job application interface.

The City locates the relevant records, but realizes they include very recent emails between members of the IT Department discussing the details of the vulnerability. The City Attorney's Office immediately seeks guidance from the IT Department about how to proceed, since it knows this request might pose some privacy and security concerns. Disclosure of these records could put the City at serious risk of malicious hacking. Moreover, exploitation of this particular vulnerability could result in the leaking of very sensitive City personnel information. Accordingly, the IT Department and the City Attorney's Office jointly decide that the City must not disclose specific portions of emails that would allow a malicious actor to exploit the vulnerability until the City can address it.

BE TRANSPARENT AND OPEN

Oaklanders' right to privacy is furthered by the ability to access and understand explanations of why and how we collect, use, manage, and share personal information. To that end, we aim to communicate these explanations to Oakland communities in plain, accessible language on the City of Oakland website. We also aim to communicate this information at a time when it is relevant and useful.

I. Purpose and Goals of the Transparency Principle

The Transparency Principle intends to establish trust between the City of Oakland and its residents by informing them about City privacy practices in a way accessible to them. Increased openness builds trust and facilitates citizen engagement in deliberations on privacy issues. Transparency and openness are ongoing commitments to provide regular information as privacy practices change and adapt in the face of evolving technology.

The Transparency Principle is grounded in various state and municipal laws, including the Ralph M. Brown Act,[31] the Oakland Sunshine Ordinance,[32] the Privacy Advisory Commission ("**PAC**") Ordinance,[33] and the Oakland Surveillance and Community Safety Ordinance (**"Surveillance Ordinance"**).[34] The Brown Act and Sunshine Ordinance's requirements of regular order and public availability of meeting and hearing documents reflect the view shared at the state and local level that transparency and openness are essential to effective democratic governance. The PAC Ordinance and the Surveillance Ordinance similarly make good on the City's commitment to transparency regarding matters of city administration when it comes to the growing role that technology plays in the collection of personal information. Nothing in the Transparency Principle limits the application of these state and municipal laws. Rather, the Transparency Principle intends to communicate to Oaklanders, when possible, the information security practices undertaken by the City to protect individual privacy.

The Transparency Principle also emphasizes the City's commitment to communicate relevant information to all Oakland communities in "plain, accessible language." Plain language increases the clarity of information about privacy practices. "Accessible language" means providing information in multiple languages and in formats useful to the blind and print disabled. The Principle's accessibility provision is grounded in state and local ordinances. The California Civil Rights Act and The Bilingual Services Act are the two main state statutes governing language access services.[35] Both mandate that local agencies provide language access services to individuals with

---

[31] *See* Cal. Gov't Code §§ 54950–63.
[32] *See* Oakland, Cal., Ordinance 11957 (1997); Oakland, Cal., Ordinance 12483 (2003).
[33] *See* Oakland, Cal., Ordinance 13349 § 2(a)–(b).
[34] *See* Oakland, Cal., Oakland Surveillance and Community Safety Ordinance §§ 9.64.010(6)–(7); § 9.64.020; § 9.64.030(3).
[35] *See* Cal. Gov't Code § 11135(a); Cal. Gov't. Code § 7290.

limited proficiency in English. Oakland was the first city in the U.S. to implement a language access ordinance as the "Equal Access to Services Ordinance,"[36] expanding definitions and providing specific guidance to fulfill obligations under the California Bilingual Services Act.[37]

II. Examples Illustrating the Transparency Principle in Practice

Example #1: Homelessness and Housing Units

An employee at the Department of Housing and Community Development wants to help develop more low-income housing projects in Oakland. The project requires her team to gather data and create reports about homelessness in the City. Over the course of the project, the team plans to conduct surveys at various homeless shelters, with the intent to gather residents' personal information including names, dates of birth, employment information, and mental health history. The Department wants to emphasize to potential participants that while the survey is entirely optional, it provides valuable information that can be used to better serve Oakland residents.

The Department proactively informs individuals about purpose of the survey, the information collected, any other departments that may be able to access the information, and the option to not participate. It also posts notices regarding the project both online and in shelters in multiple languages. The notice is simply worded and provided in formats accessible to print disabled residents.

Example #2: Public Works and Rain Barrel Project

An employee for the Oakland Public Works Department wants to build on the success of the last Oakland Rain Barrel Program to better conserve resources and protect the Oakland environment by recycling rainwater. As part of the project, the City is required to survey homes that might have the capability to install rain barrels safely so it can determine a working budget to subsidize the cost. The City plans to collect residents' names, addresses, household size, water usage patterns, and interest in the program in order to determine contract requirements for local installers of the rain barrels.

Recognizing the significant amount of personal information being collected for implementation of the project, the Public Works Department decides to inform Oakland residents about the types of personal information collected in the survey. The City includes this information in flyers about the program, which also includes contact information and link to the Department's webpage, in multiple languages.

[36] *See* Oakland, Cal., Mun. Code § 2.30.
[37] *See* Oakland, Cal., Mun. Code, § 2.30.020(d).

Example #3: Department of Transportation/Oakland Police Department Intersection Danger

A particular neighborhood intersection has been the site of numerous accidents, some of which have been fatal. The Department of Transportation ("**DOT**") and the Oakland Police Department ("**OPD**") confer and decide that installing a traffic camera at that intersection would help reduce the number of accidents. They present their plan to add cameras to the intersection at the monthly PAC meeting, which approves the installation after hearing members of that neighborhood advocate in support of the camera installation. However, some neighborhood advocates are concerned that the camera might also surreptitiously monitor the activity of individuals near the intersection in non-traffic related incidents.

Acknowledging the importance of this concern raised by some members of the community, the departments decide to notify neighborhood residents about the installation of the camera, the purpose and limitations of data analysis, and any additional privacy precautions that the PAC advises such as drawing attention to the cameras themselves with highly visible notices. Since the primary language in this community is not English, the notices posted around the neighborhood are translated into multiple languages. The notice also appears on both the DOT and OPD websites.

BE ACCOUNTABLE TO OAKLANDERS

Trust in our stewardship of personal information requires both that we collect and manage personal information appropriately, and that we create opportunities for active public participation. We publicly review and discuss departmental requests to acquire and use technology that can be used for surveillance purposes. We encourage Oaklanders to share their concerns and views about any system or department that collects and uses their personal information, or has the potential to do so. We also encourage Oaklanders to share their views on our compliance with these Principles.

I. Purpose and Goals of Accountability Principle

The Accountability Principle ensures that the City of Oakland is answerable to its residents when it collects and manages their personal information by proactively seeking input through legislative and administrative bodies such as the Privacy Advisory Commission ("**PAC**") about the City's compliance. The Accountability Principle emphasizes the importance of giving Oakland residents whose privacy interests may be impacted by city policies information about those policies and an opportunity to weigh in on them. The Principle acknowledges that accountability requires more than serving as a passive receptacle for feedback. The goal of the Principle is to lower barriers for civic participation on questions of privacy. By soliciting feedback from a wide and diverse pool of residents, the City can safeguard the privacy and security of all residents, especially marginalized communities who are most affected by inequitable data collection practices and may face barriers to participating in the decisionmaking process.

The Accountability Principle also calls for residents' views on compliance with the Principles themselves. Because of constantly changing technology and the increasing sophistication of residents' conception of their privacy rights, the precise steps the City must take to meet the standards set by the Principles may evolve over time. By asking for feedback on compliance with the Principles, the City can continue to refine its approach to privacy in a democratic and participatory manner.

PAC provides a model for this kind of engagement. Because PAC conducts monthly meetings and uses other public forums to collect and receive public input, Oaklanders have the opportunity to weigh in on any surveillance technology that can collect residents' personal information.[38] PAC also makes publicly available City departments' annual use reports, privacy analyses, and data retention policy recommendations regarding the City's deployment of existing and proposed surveillance equipment and technologies.[39]

---

[38] *See* Oakland, Cal., Ordinance 13,349 § 2(b).

[39] *See* Oakland, Cal., Ordinance 13,349 § 2(e)–(g); Oakland, Cal., Oakland Surveillance and Community Safety Ordinance §§ 9.64.010(6), (7), 9.64.020, 9.64.030(3).

II. Examples Illustrating the Accountability Principle in Practice

Example #1: Parks Department Privacy Training

An Oaklander volunteering at the Lakeview Park Kitchen Garden is surveyed by some Parks, Recreation & Youth Development Department employees as part of a research project. The employees ask for Oakland residents' name, age, district affiliation, and information about what times they go to parks and which parks are closest to their homes. Although the volunteer agrees to participate in the survey, she is concerned about the amount of personal information being collected by the Department.

After finishing her shift at the Kitchen Garden, the volunteer decides to email the Director of the Department to let him know about her concerns with the Department's survey practices and the amount of information collected on her. The Director of the Parks Department, who is aware of the Oakland Privacy Principles, responds to her and also decides to flag the information for the City's Chief Privacy Officer to review compliance with the Privacy Principles. The Privacy Officer reviews the survey practices and communicates to the Department necessary guidance on how to best comply with the Principles. The Parks Department sends a follow-up note to the resident who flagged the concern.

Example #2: Automated License Plate Reader Hearing at PAC

An Oakland resident learns that the Department of Transportation has been using Automated License Plate Readers ("**ALPR**") to enforce parking regulations. She finds the use of ALPR invasive and worries that the same vehicle has captured her information on multiple occasions.

To voice her concerns in a public forum, she decides to attend an upcoming PAC meeting where the Department's use of ALPR is being considered. After hearing PAC's deliberative process and department officials speaking in support of ALPRs, the resident lays out her concerns about how her image and information has been captured by the ALPR repeatedly. Hearing her account, PAC recommends adjusting the angle of the ALPR camera to limit capture of driver images going forward, leading to amendments to the ALPR Surveillance Use Policy.

Example #3: Air Quality Surveys

The Oakland High School Environmental Science Academy team is participating in a community project measuring the disparity in air quality in different areas of Oakland. The team is tasked with collecting health information on the individuals living in areas near the devices. They want to test whether there is a correlation between areas with higher particulate matter in the air and increased incidences of asthma and chronic obstructive pulmonary diseases in the local population groups. This involves surveying local populations about personal information, including names, genders, ages, and medical history. The City is also very interested in the results of the team's research.

Recognizing the sensitive nature of the information collected as well as the City's responsibility to protect Oaklanders' privacy and information security, the City decides to include language to proactively inform all survey participants of the purpose of the data being collected as well as contact information for a privacy officer for the Oakland Unified School District so that participants can give any feedback on any concerns they might have about the data collection or the District's compliance with the Privacy Principles.

CONCLUSION

Collectively, the Privacy Principles create a citywide standard for privacy practices in Oakland. This Guidance document illustrates how City departments should apply the Principles in practice. While the Principles express Oakland's privacy values, the Guidance helps to harmonize the ways different City departments—from the Oakland Police Department to the Department of Public Works to IT—use the Principles to protect Oaklanders' privacy interests in the course of providing city services. This Guidance is a living document and will be updated periodically to respond to changes in information technology and evolving norms and understandings of privacy, information security, and civil liberties.

If you have any questions or concerns about any aspects of the Principles or this accompanying Guidance, we encourage you to reach out to the Oakland Privacy Advisory Commission ("**PAC**") directly or to participate in a monthly PAC meeting to share your insights or seek more information.