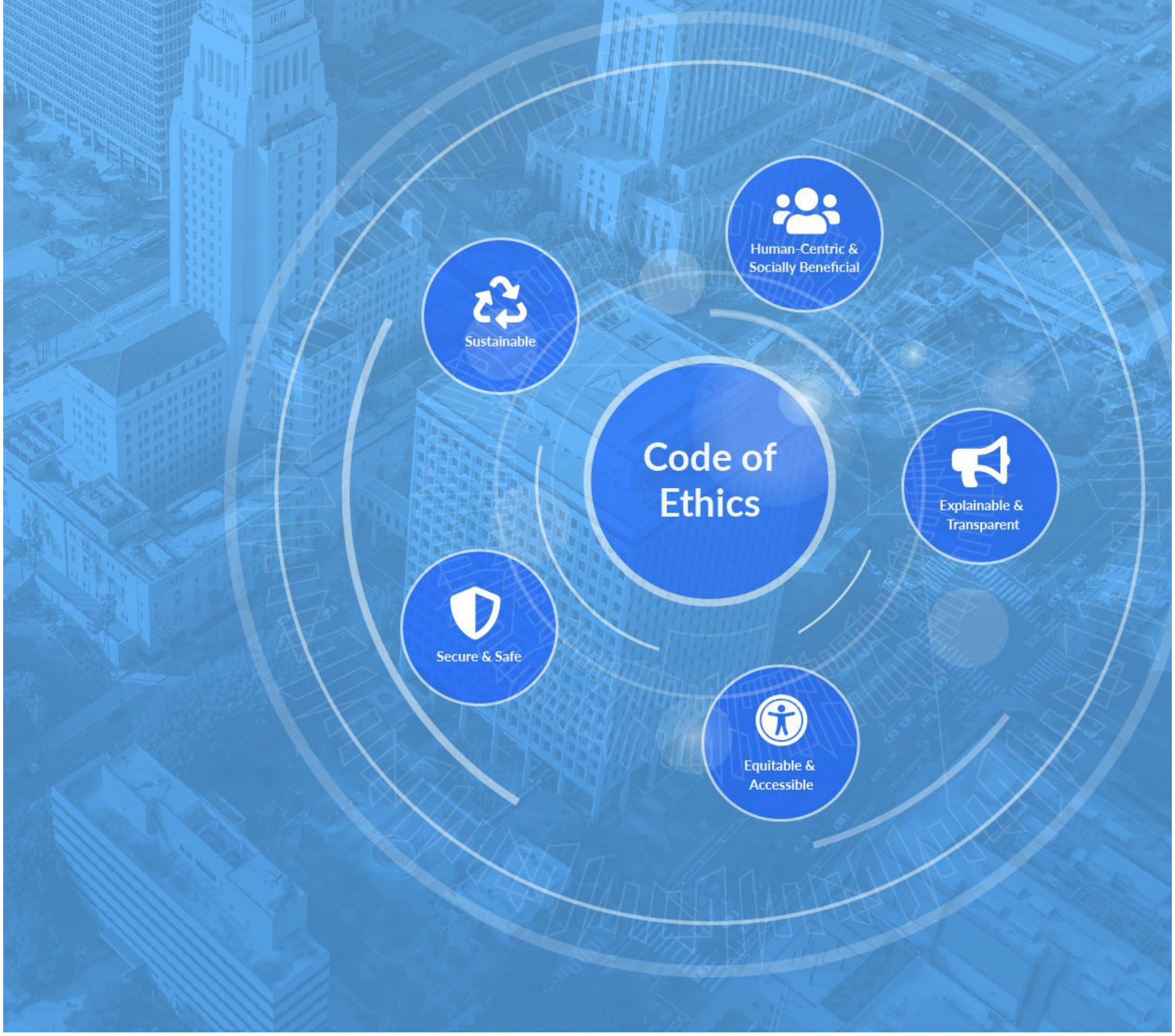
P187

City of Los Angeles Digital Code of Ethics


Code of Ethics
Human-Centric & Socially Beneficial
Sustainable
Explainable & Transparent
Secure & Safe
Equitable & Accessible

P188

ACKNOWLEDGEMENTS

The lead authors of the Digital Code of Ethics were General Manager Ted Ross and Assistant General Manager’s Anthony Moore and Jeanne Holm from the Information Technology Agency (ITA) with contributions in the emerging technologies section from Gartner Inc, Google, Microsoft Corporation, and the University of Southern California (USC). The graphics editors were Balmore Botero and Calvin Lee. Technology leaders from across the City of Los Angeles were instrumental in review and input through the citywide Information Technology Policy Committee (ITPC). The continued commitment to innovation and digital ethics by General Managers at the City of Los Angeles is both an inspiration across Southern California and around the world.

We would like to acknowledge the truly progressive leadership of Mayor Eric Garcetti and our other elected leaders: City Attorney Mike Feuer, Controller Ron Galperin, and City Council, specifically the members of the Information Technology & General Services (ITGS) Committee (Chairman John Lee, Bob Blumenfield, and Monica Rodriguez) who ask the tough questions and expect excellence from City of L.A. technology.

P189

TABLE OF CONTENTS

DIGITAL ETHICS: WHY IT MATTERS

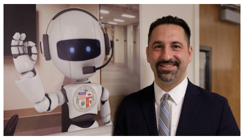
"If the lifeblood of the digital economy is data, its heart is digital trust."
-Price Waterhouse Cooper, The Journey to Digital Trust, 2018

The City of Los Angeles provides critical public safety, economic development, transportation, public works, sanitation, and cultural services to over 4 million residents, 500,000 businesses, and over 48 million annual visitors. Angelenos rely on the 42 L.A. City departments to answer 9-1-1 calls, clean streets, fix potholes, remove graffiti, collect trash, and make it easier to work and play in Los Angeles. For over 230 years, L.A. City government has sought new, innovative ways to improve our growing urban environment and serve the needs of our diverse communities. In the last five years, this mission has been transformed by the Digital Age. 81% of Americans own smartphones, 71% are active on social media, and 70% shop online (Pew Research Group, Dec 2019). In this digital era, Angelenos expect a lot from their L.A. City government. They want easy-to-use, powerful websites and apps to request City services (fixing potholes, removing graffiti, repairing streets, etc) and get the information they need. Responding to these expectations, the City of Los Angeles has been building world-class technology to provide residents, businesses, and visitors with the secure digital services they expect from a leading global city. In fact, these efforts have been recognized, earning the coveted #1 U.S. Digital City award for three straight years, a national Cybersecurity award, a Webby award, and multiple international Smart City awards. However, innovation is no longer enough. As Americans have become increasingly digital, they have also become increasingly distrustful of digital technology. From privacy concerns to data breaches, Americans are concerned that the innovations they use daily will have profoundly negative impacts on their lives. These anxieties have become so prominent that Oxford Dictionary officially added "techlash" (technology backlash) as a word in the English dictionary. As a government that heavily uses technology to serve our more than 4 million Angelenos, the City of Los Angeles understands the importance of digital services that are both ***innovative and ethical***. This is why digital ethics matters at the City of Los Angeles.

Digital ethics is our system of values and standards for the conduct of City of Los Angeles electronic interactions with residents, businesses, and visitors. Drafted by the L.A. City Information Technology Agency and adopted by the citywide Information Technology Policy Committee, this Digital Code of Ethics clearly articulates our ethical standards and policies in the use of technology and data to interact with residents and perform City operations. Without these standards, our government risks alienating the very stakeholders that we serve. It has become imperative that ethical principles and safeguards be identified and put in place to reinforce the public's digital trust. This is more than just compliance with existing laws; this is an update to our social contract in an increasingly digital world.

Since information technology (IT) has become such a predominant tool to engage L.A.'s residents and deliver City services, this Digital Code of Ethics was drafted to provide guidance to all City of Los Angeles departments, including specific standards in the use of emerging technologies (e.g. automation, facial recognition, machine learning). This is done to help deliver assurance to city residents & employees that the City of L.A. values their privacy and takes active measures to prevent unintended ethical consequences. The values and standards expressed in this Digital Code of Ethics are derived directly from resident feedback, community meetings, representatives of business coalitions, meetings with our elected officials, and academic experts in digital ethics. Unlike private sector tech companies, the government is presumed to provide leadership in the responsible and ethical use of modern technology. At the City of Los Angeles, we understand that public trust takes time to build and can be easy to lose. Through the Digital Code of Ethics and other initiatives, the City of Los Angeles is committed to not only building innovative technology solutions, but also maintaining the public's digital trust for years to come.

Ted Ross
General Manager and CIO
City of Los Angeles, Information Technology Agency



P192

City of Los Angeles
DIGITAL BILL OF RIGHTS

Every person who lives in Los Angeles is an “Angeleno”. As an Angeleno, we value your privacy, your freedom, and your equality. Living as an Angeleno in a Digital Age, we at the City of Los Angeles are pledged to recognize the following Digital Bill of Rights as it pertains to the data, computer systems, and technology we administer:

1 **THE RIGHT TO FREE EXPRESSION**
We will not censor your digital voice in our social media or public meetings based on the content of your opinion, viewpoint, or political party.

2 **THE RIGHT TO PRIVACY**
You can have the reasonable expectation that you will not be personally monitored through surveillance, tracked by your location, or have your data shared outside of our government.

3 **THE RIGHT TO EXCLUSIVE OWNERSHIP OF PERSONAL DATA**
Your data is your own. We will not share or sell your personally identifiable information to outside parties without your consent.

4 **THE RIGHT TO GOVERNMENT TRANSPARENCY**
We will use our technology to promote open and accessible government. We will make our public hearings and data open by default.

5 **THE RIGHT TO NO-COST ACCESS TO DIGITAL SERVICES**
We will not charge Angelenos for access to City of Los Angeles websites, mobile apps, portals, City services, or public data.

6

THE RIGHT TO USER ASSISTANCE

City services must be available to all Angelenos, regardless of race, neighborhood, immigration status, age, income, or education-level. We will make our digital services easy-to-use and provide opportunities for user assistance to maximize user experience.

7

THE RIGHT TO ACCESS SERVICES IN YOUR OWN LANGUAGE

The strength of the City of Los Angeles is its diversity. We will make every effort to provide automated or human translation tools to provide digital services in your language of preference.

8

THE RIGHT TO FULL DISCLOSURE

You have the right to understand how and why we collect and use your personal data.

OUR DIGITAL VALUES

"64% of Americans are very/somewhat concerned about how the government uses the data it collects."

-Pew Research Center, "Americans and Privacy Survey", 2019

Every year, technology changes. However, good guiding principles and values for technology do not. Beyond simply complying with federal and state laws, the City of Los Angeles Digital Code of Ethics is based on five fundamental values:

Human-centric & socially beneficial (Value #1)

Our technology and the resulting data is used for the benefit of the people (human-centric) and of our community.

Equitable & Accessible (Value #2)

Our public digital services are optimized for easy access by all of our diverse communities, and our technologies will not be used to discriminate against them. Technology and digital services shall be developed to serve the city's disability community.

Explainable & Transparent (Value #3)

We will never implement technology that we don't understand (no "black boxes") and will make resulting data open by default.

Secure & Safe (Value #4)

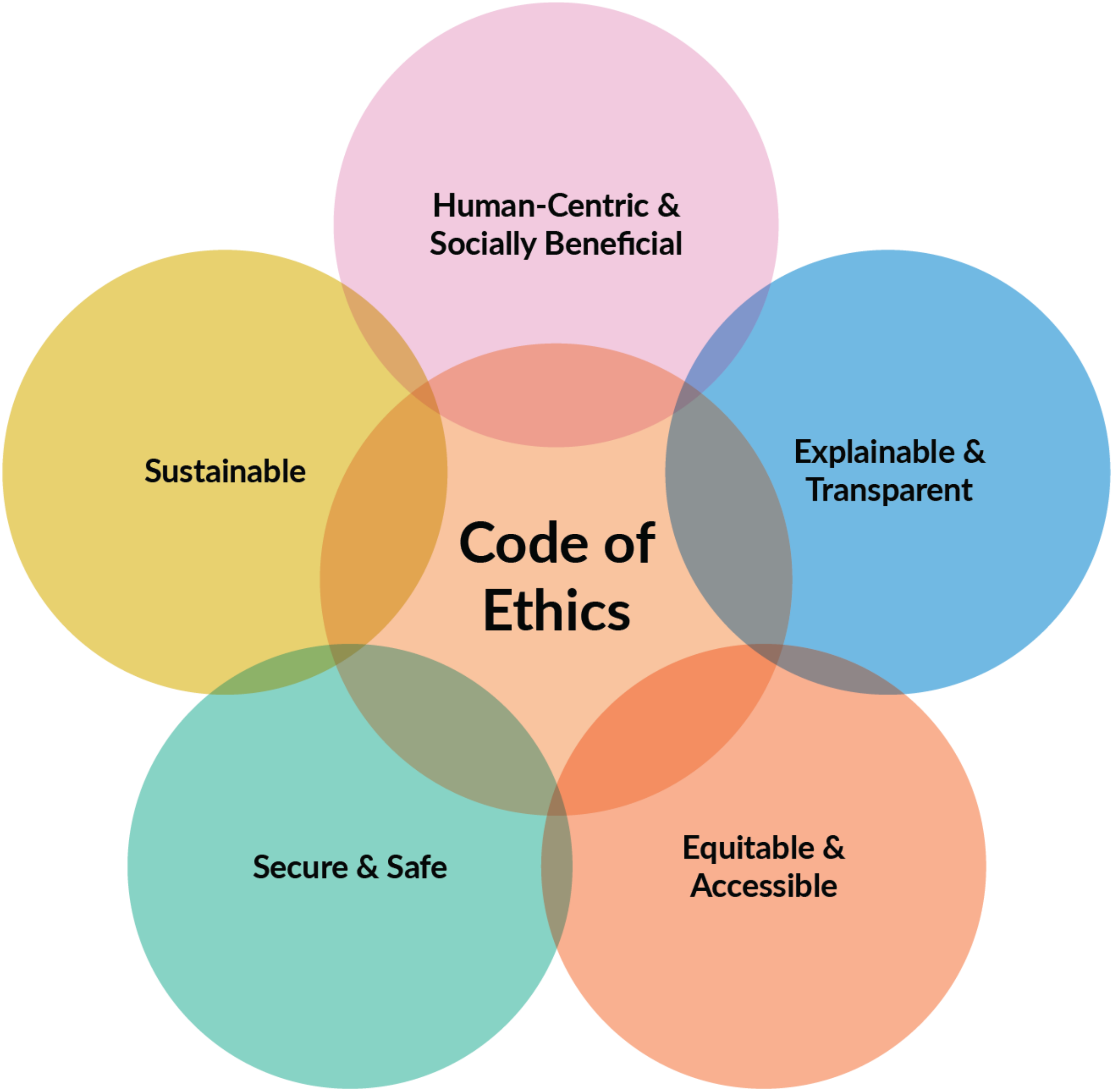
We are stewards of our resident's digital assets and will vigilantly protect the sensitive data entrusted to us (PII, HIPAA, PCI).

Sustainable (Value #5)

Technology impacts our environment and the choices that we make. We prioritize technology that promotes sustainable choices and reduces environmental waste and emissions.

P195

Digital Values are Foundational to Our Code of Ethics



THE ROLES WE PLAY

"No one can whistle a symphony. It takes a whole orchestra to play it."
-H.E. Luccock, American Professor & Author

Digital ethics is not the responsibility of one person or one group of people. We all play an important role.

Below is a summary of digital ethics roles at the City of Los Angeles:

A. **Los Angeles Residents**
   a. Understand their digital rights
   b. Provide informed consent to use of personal data
   c. Contact Councilmember with concerns about technology or data use

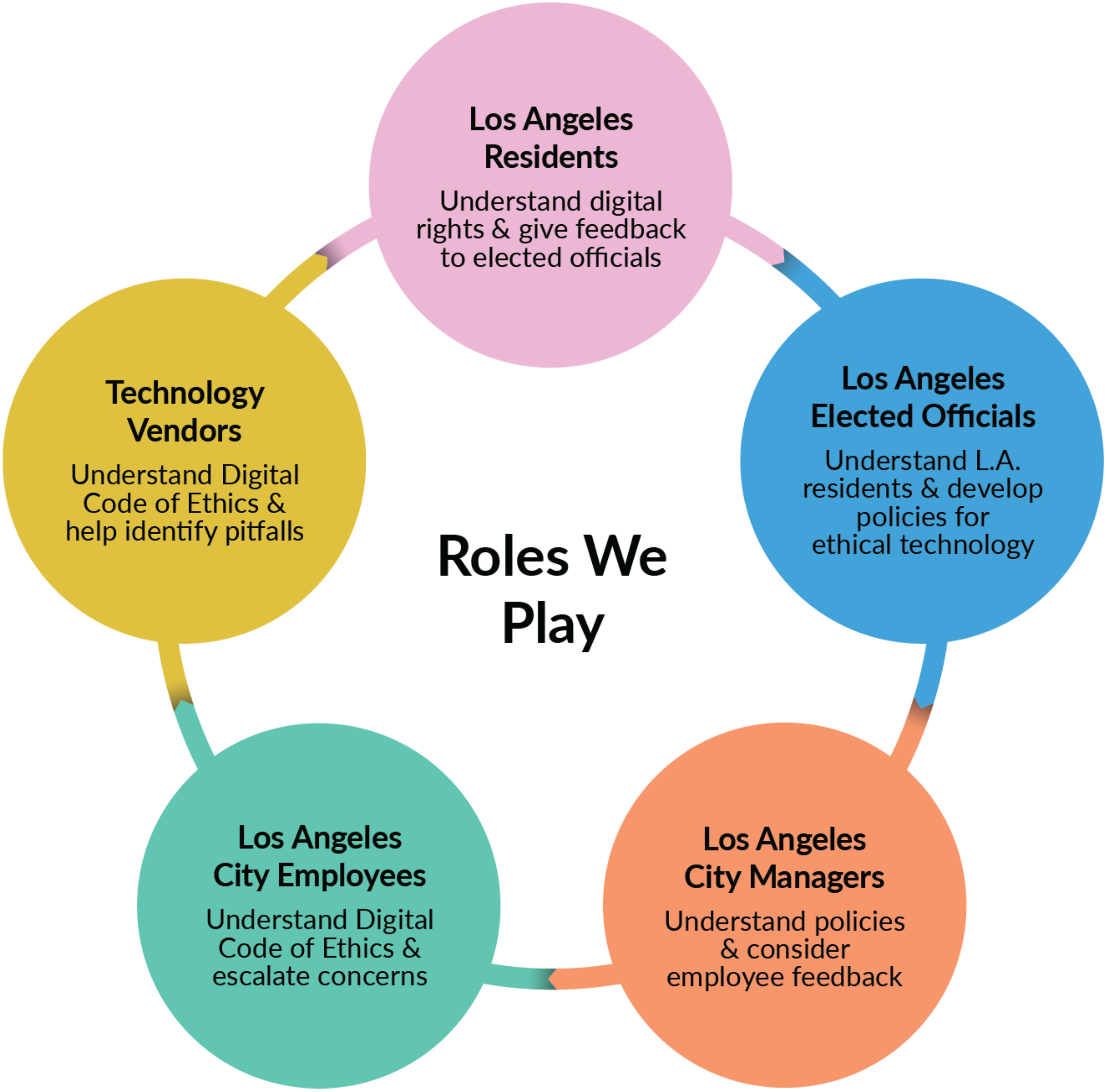
B. **Los Angeles Elected officials**
   a. Develop and enforce policies for ethical use of technology and data
   b. Listen and respond to concerns of L.A. residents and businesses

C. **Los Angeles City Managers**
   a. Evaluate ethical consequences before choosing technology platforms
   b. Establish preventative measures to avoid negative ethical consequences when deploying new technology or data initiatives
   c. Provide feedback opportunities for employees or vendors to raise concerns
   d. Establish safeguards to ensure compliance with L.A. Digital Code of Ethics across your department services

D. **Los Angeles City Employees**
   a. Escalate ethical concerns of new technology or data uses to management, including recommendations for preventative measures and fixes
   b. Identify digital ethics concerns early in technology & data projects
   c. Adhere to L.A. Digital Code of Ethics when performing daily tasks

E. **Technology Vendors**
   a. Assist City managers and employees in identifying ethical concerns when choosing and implementing new technologies
   b. Recommend mitigation strategies to prevent unintended ethical consequences for new technology or upgrades to existing technology
   c. Assist in the build and deployment of ethical technical solutions for L.A. residents

Everyone Plays a Role in City of Los Angeles



Roles We Play

Los Angeles Residents
Understand digital rights & give feedback to elected officials

Los Angeles Elected Officials
Understand L.A. residents & develop policies for ethical technology

Los Angeles City Managers
Understand policies & consider employee feedback

Los Angeles City Employees
Understand Digital Code of Ethics & escalate concerns

Technology Vendors
Understand Digital Code of Ethics & help identify pitfalls

OUR DIGITAL STANDARDS

"Tweet others the way you want to be tweeted."
-Germany Kent, L.A. Journalist & Social Media Expert

More than just values and guiding principles, this Digital Code of Ethics is designed to be a practical guide for City of Los Angeles departments. Building on our five foundational values, the City of Los Angeles technology leaders have identified and agreed on the digital standards below to ensure our technology meets both the innovation and ethical expectations of the public:

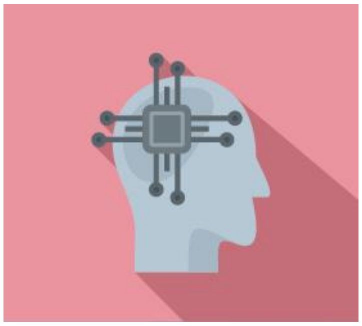
#1	**WE BUILD ETHICAL TECHNOLOGY, NOT JUST INNOVATIVE TECHNOLOGY** While innovative features are important to empower the users of our technology, we also take responsibility in foreseeing ethical problems and misuses of our technology that would overshadow these great features.
#2	**OUR TECHNOLOGY MUST BE BOTH FUNCTIONAL AND EASY TO USE** We value both what a technology can do for the public and how easy it is to use by the public ("user experience"). Ease of use is a core value for our digital services.
#3	**TECHNOLOGY MUST ENABLE OPEN & TRANSPARENT GOVERNMENT** Our technology provides a unique opportunity for 4 million busy Angelenos to participate with, learn about, and get necessary services from their government. From easy-to-access government data on our open data portal (Data.LACity.org) to body worn cameras used by the L.A.P.D., we believe technology provides unparalleled insight into government activities that are paid for by the public.
#4	**TECHNOLOGY MUST INCREASE ACCESSIBILITY FOR L.A. COMMUNITIES** Websites, apps, and digital portals provide unprecedented access to government services. Whether using a smartphone, laptop, or kiosk, our technology is built with all of our communities in mind, regardless of race, language, gender, neighborhood, education level, disability, etc.

P199

#5	**TECHNOLOGY MUST BE BUILT FOR THE PRESENT & THE FUTURE** We make technology investments using proven platforms that are cost effective, scalable for future demand, and based on a competitive purchasing process.
#6	**WE WILL NOT SHARE OR SELL YOUR PERSONAL DATA** The data we gather is exclusively used for improving public services. We will not share or sell your personally identifiable information to outside parties without your consent. In addition, we see ourselves as digital stewards of your data and will secure it according to our Information Security Policy.
#7	**WE WILL NOT DIGITALLY TRACK, STORE, OR SHARE YOUR LOCATION** Where you have been is fundamental to your privacy. Location data will not be tracked or stored, unless it is required by a lawful warrant or essential to providing a service, and then it is anonymized with no stored history. An example of this is the ShakeAlert app, which uses current location of anonymized users to warn of a coming earthquake (with location history continuously being deleted).
#8	**OUR TECHNOLOGY WILL NOT BE USED FOR SURVEILLANCE** The apps, websites, and portals that we provide to the public will never be instruments for unauthorized spying or surveillance activities.
#9	**WE SEEK TO HIRE A TECHNOLOGY WORKFORCE AS DIVERSE AS L.A.** We believe one of the best methods to prevent racial, gender, and neighborhood bias in our technology is to have a diverse technology workforce. We actively recruit a diverse workforce within the limits of existing human resource laws.
#10	**WE INVEST IN OUR COMMUNITIES TO REDUCE THE DIGITAL DIVIDE** All Angelenos need the skills and tools to compete in the digital economy, including access to the Internet, digital literacy training, and access to computing devices.

Artificial Intelligence & Machine Learning

What is Artificial Intelligence and Machine Learning?



Artificial Intelligence (AI) is the science of making things smart. Machine learning (ML) is a subset of AI, where computers learn and recognize patterns from examples (i.e., data), rather than being programmed with specific rules. While the theory behind AI-based approaches has existed for decades, its application and use has become much more accessible with the availability of computing and data management at a large scale. Apple Siri and Google Home use AI to understand speech, identify what you are asking for, and then provide you with a response. Pandora uses AI to propose additional songs you may like based on listening patterns and Google Nest uses AI to examine your patterns to adjust your thermostat and turn on/off your smart devices. AI is increasingly used for government solutions, from leveraging AI-enabled computer vision to detecting potholes to using AI-enabled language translation tools to make government information more accessible to non-English speakers. While possibly a transformational tool for improving government operations and the lives of Angelenos, there are potential pitfalls with this technology that must be addressed to ensure positive benefits for the public.

Potential Issues with Using Artificial Intelligence (AI)

Harnessed appropriately, AI can deliver great benefits for governments and society writ large. But, like other digital tools, it is critical that the technology is developed and deployed responsibly and in ways that build public trust. As a discipline of computer science, AI development must follow general best practices for software and IT systems. At the same time, AI can pose special challenges and requires that special attention be paid to: 1) fairness 2) explainability.

Fairness: Though it can be tempting for some to think of computer algorithms as infallible and objective, AI models are susceptible to unfair biases implicit in the data, as well as the design choices made by the humans that build them. Because humans are ultimately responsible for finding, organizing, and labeling that data, there are multiple ways in which bias can be introduced into the AI model. For example, historical volumes of text—often used to train machine learning models that deal with natural language processing or translation—can perpetuate harmful stereotypes if left uncorrected. Seminal work by Bolukbasi et al (https://papers.nips.cc/paper/6228-man-is-to-computer-programmer-as-woman-is-to-homemaker-debiasing-word-embeddings.pdf) demonstrated how easily statistical language models can "learn" outdated assumptions about gender, such as "doctor" being "male" and "nurse" being "female." Of course, if the City of Los Angeles used a chatbot running on AI that communicated to the public based on these outdated assumptions, it would lead to public offense, reduce accessibility, and harm the digital trust between the government and those we serve. Similar issues, known as embedded biases, have been demonstrated with respect to race as well, which would be unacceptable if part of a City service (https://researchportal.bath.ac.uk/en/publications/semantics-derived-automatically-from-language-corpora-necessarily).

Additionally, beyond forms of bias that can creep into the development of a model, there are also potential biases that arise from how end users interact with a model. Automation bias, for example, is a tendency to favor results of automated systems over human judgement, which can lead to overreliance and misuse of an AI system. It's essential therefore to consider how the outputs of AI models are presented and understood within City of Los Angeles processes and decisions, in addition to how the underlying model is trained.

Explainability: Explainability is the concept that AI systems can be explained by the humans that use them. Explainability is essential to understand and trust the outputs of AI systems. These issues apply to humans as well as AI systems since it is not always easy for a person to provide a satisfactory explanation of their own decisions. For example, it can be difficult for an oncologist to quantify all the reasons why they think a patient's cancer may have recurred—they may have an intuition, leading them to order follow-up tests for more definitive results. In contrast, an AI system can list a variety of information that went into its prediction: biomarker levels and corresponding scans from 100 different patients over the past 10 years, but have a hard time communicating how it combined all that data to produce a specific prediction. While the logic of traditional software can be laid bare with a line-by-line examination of the source code, a neural network is a dense web of connections shaped by exposure to thousands or even millions of training examples.

L.A. City Standards for Using Artificial Intelligence

For the City of Los Angeles, Artificial Intelligence offers transformational opportunities to improve our services and better engage our residents and businesses. The following are key standards in the use of Artificial Intelligence or Machine Learning:

1. **Design AI models using concrete goals for fairness and inclusion of diverse communities**. Consider whose views and which types of data are represented and what outcomes this application will generate for different users and communities.
2. **Use representative datasets to train and test models**. Assess fairness in datasets, which includes identifying representation and corresponding limitations, as well as identifying prejudicial or discriminatory correlations between features, labels, and groups. Visualization, clustering, and data annotations can help with this assessment.

3. **Check the system for unfair biases**. Organize a pool of trusted, diverse testers who can adversarially test the system, and incorporate a variety of adversarial inputs into unit tests to identify who may experience unexpected adverse impacts.
4. **Analyze performance**. Develop metrics to evaluate performance across different subgroups, and consider whether a system's false positive rate varies.
5. **Plan out how to ensure explainability before, during, and after the design and training of an AI model**. Determine what degree of explainability a system needs, and whether it is possible to analyze the training and testing data, as anomalous behavior can often be explained by quality issues or gaps in data.
6. **Treat explainability as a core part of the user experience**. Iterate with users in the development cycle to test and refine assumptions about user needs and goals. Design the user experience so that users build useful mental models of the AI system.
7. **Design the AI model to be explainable**. Use the smallest set of inputs necessary and simplest model possible to meet your performance goals.
8. **Choose metrics to reflect the end-goal and the end-task**. Metrics should address the particular benefits and risks of the application in question. For example, a fire alarm system would need to have high recall, even if that means the occasional false alarm.
9. **Communicate explanations to model users**. Provide explanations that are understandable and appropriate for the user. Model cards (https://modelcards.withgoogle.com/about) can help organize ML essential facts in a structured way.
10. **Test repeatedly and follow software engineering best testing practices**. Conduct rigorous unit tests to test each component of the system in isolation and iterative user testing to incorporate a diverse set of users' needs in the development cycles.

Additional Considerations and Resources

While fairness and explainability are the most common ethical considerations when deploying AI systems, they are not the only ones. Important questions around privacy, safety, security, and other more domain-specific considerations arise as governments find ways to use AI. Google's AI Principles were established for this purpose (https://ai.google/principles/). In addition, the following resources provide a deeper view into these areas, which can be tailored to the needs of AI uses at the City of Los Angeles:

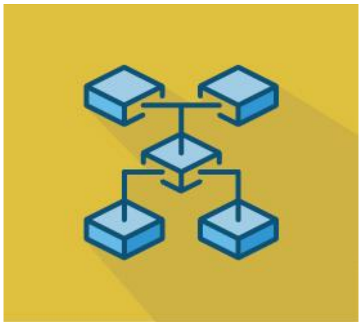
- Responsible AI Practices (https://ai.google/responsibilities/responsible-ai-practices/)
- Inclusive ML Guide (https://cloud.google.com/inclusive-ml/)
- ML Crash Course (https://developers.google.com/machine-learning/crash-course)

The Artificial Intelligence & Machine Learning topic above was prepared by the City of Los Angeles Information Technology Agency in collaboration with Chris Hein, Head of Customer Engineering for Public Sector at Google, where his goal is to help public sector organizations become more efficient and effective in furthering their mission using best in breed technologies and methodologies (https://www.linkedin.com/in/christopherhein).

Blockchain

What is Blockchain?

Blockchain technology provides a distributed ledger that presents users with an immutable and consistently-ordered version of data in the form of digitally signed transactions. Blockchain-based distributed ledgers can enable ecosystems of organizations including industry, nonprofits and government agencies to work together to share in the communication, storage, and processing of data in a decentralized yet trustworthy manner. The decentralized model allows for all of the nodes (computers) on the network to contain the complete ledger of transactions. The result of decentralization is that the hacking of the blockchain is virtually impossible. It is for this reason that blockchain can be extremely useful for functions such as voting and financial transactions. Bitcoin is a cryptocurrency with no central bank, but uses decentralized blockchain technology to account for money transfers and payments. Spotify uses blockchain to correlate music artists with their songs and licensing agreements. De Beers uses blockchain to securely and independently track diamonds from mine to jeweller (to reduce fraudulent sales of conflict diamonds). Though originally designed for cryptocurrencies and banking applications, the uses of distributed ledger technology are much broader, encompassing use cases such as property ownership records (home deeds), transparency of government actions, decentralized identity management (digitally confirming you are who say), and tracking of goods (supply chain).



Potential Issues with Using Blockchain

When using blockchain, special attention must be paid to potential issues that can arise from: 1) using it without a compelling reason (relevance), 2) using features not technologically mature, 3) not properly securing the blockchain platform, 4) excessive energy consumption, 5) exposing confidential data, and/or 6) incorrectness of data.

Not Establishing Relevance: Blockchain is not always the solution to every problem involving data storage and sharing. Consider evaluating alternative technologies and establish a clear justification for using blockchain.

Lack of Maturity: As the underlying technology is still maturing, early blockchain adopters run the risk of being locked into systems that are hard to scale or upgrade. Proper testing and adoption of more mature features and capabilities to mitigate this risk is needed.

Securing Trust: The underlying distributed platform must be as secure as possible, particularly with respect to the parties involved in maintaining and validating the ledger.

Environmental Impact: Proof of Work, used in early protocols, can incur high energy costs.

Maintaining Confidentiality: Confidential, privacy-sensitive data should not be exposed on a ledger. This should be clearly evaluated and mitigated during design and testing.

Guaranteeing Correctness: While blockchain technologies can ensure that data in the ledger is immutable, they cannot always guarantee the correctness of the data. Other application controls must be in place to guarantee the correctness of data.

L.A. City Standards for Using Blockchain

For the City of Los Angeles, blockchain affords a unique opportunity to transform government processes through simultaneous improvement in transparency, privacy, and accuracy. The following are key standards in the use of blockchain.

1. **Examine alternatives before using blockchain**. Carefully compare blockchain with alternative, even centralized, technology solutions to see if it is truly a good fit for the problem being addressed.
2. **Be honest and accommodate for current technology limitations**. Seek solutions based on open and widely adopted standards that are easy to upgrade and scale over time as the technology matures; avoid vendor lock-in.
3. **Thoroughly plan for both current and expanded blockchain decisionmaking**. Be mindful of the governance process adopted by the underlying platform including how validators are chosen, how users are authorized for their roles, and how open it is.
4. **Consider environmental impact and carbon offsets if selecting blockchain solutions**.
5. **Protect confidential data.** Have a clear policy about what data is entered on a public ledger; ensure confidential data is suitably encrypted. Ensure that private keys are kept secure.
6. **Implement policies and system controls to ensure that data entered on a blockchain ledger is truthful and correct**.

The Blockchain topic above was prepared by the City of Los Angeles Information Technology Agency in collaboration with Bhaskar Krishnamachari, Professor of Electrical and Computer Engineering at the University of Southern California. Professor Krishnamachari has co-authored more than 300 articles and 3 books focused on wireless networks, the internet of things, and distributed systems. He is a recipient of the National Science Foundation CAREER award, the ASEE Terman Award, and has been featured on MIT Technology Review's TR35 list, as well as Popular Science's “Brilliant 10” (https://www.linkedin.com/in/bhaskar-krishnamachari/).

Data & Predictive Analytics

What is Data Analytics?

Data analytics is the science of analyzing data to understand trends and patterns. Predictive analytics is a specialized form of analytics that assesses current and historical trends to make predictions about future events. Netflix uses data analysis to write algorithms that suggest movies for you to watch based on your past watch history. Major League Baseball uses data analytics to evaluate player performance and recruit new talent as evidenced in the movie Moneyball. Data analytics at the City of Los Angeles departments is the examination of data to understand the impacts of City services, departmental programs, or public policies. While data analytics is a crucial element of "data driven government" and improving services for the public, it can also be misused, resulting in unintended negative consequences for L.A.'s communities.

Data analytics can be performed in two forms. First, a "report" based on longitudinal data across a period of time. A report represents findings regarding what has happened and often includes recommendations for changes to policies or systems. Second, a "dashboard" delivered in real-time, providing automated decision making systems (ADS). Both types of data analysis require careful thought, attention to detail and a reliance on the City's ethical values to bring useful conclusions.

Potential Issues with Data Analytics Projects

For data analytics, special attention must be paid to: 1) data issues and 2) analysis issues.

Data Issues: All data has bias. Data from City systems inherently contain novel biases. By acting as a "digital exhaust" of city administrative programs, the data automatically encodes a bias from the city program itself. To ensure ethical and accurate results, data analysts must identify and quantify how the data is biased, avoiding statements like "the data says x". Data can also contain implicit bias (attitudes that affect us unconsciously). For example, 311 graffiti complaints are a misrepresentation of actual graffiti across Los Angeles as some communities use 311 to report graffiti much more than others.

Analysis Issues: When making policy recommendations, bias must be presented properly to decision makers (i.e. these results skew this direction and here's why). Secondly, data scientists must not yield to the pressure to make results conform to an expected result. Thirdly, limits of the analysis must be clearly communicated. As Danah Boyd writes in *Engaging the Ethics of Data Science in Practice,* "*Technical actors are often far more sophisticated than critics at understanding the limits of their analysis.*" Stakeholders should be informed of the hard earned context learned by the data analyst during the analysis. Fourth, departments must be able to audit and explain dashboards and Automated

Decision Making Systems (ADS). An automated result must have underlying knowledge of how it is derived, used, and what biases may exist. Fifth, visualizations can unintentionally misrepresent results. Data visualizations must abide by common standards.

L.A. City Standards for Data Analysis

As L.A.'s elected leaders and the public increasingly rely on "data driven" government to inform policies, ethical and accurate data analysis is of premium importance. The following are key standards for data analysis at the City of Los Angeles:

1. **Data analysis projects must be reproducible (traceable from data to conclusion)**. Famous "Excel Error that Changed the World" was discovered by University of Mass. students trying to reproduce Harvard economists' results.
2. **Data analysis results must be anonymized (no Personally Identifiable Information) and aggregated to protect privacy**. However, aggregation must not hide critical insight into racial or demographical impacts.
3. **Data must be securely stored with least privilege access by data analysts**.
4. **Data analysts must not use data for purposes other than what was authorized by the data provider**. Furthermore, analysts should not attempt reidentification.
5. **Data analysis projects must use the City of L.A. Code and Methodology Review Checklist to avoid common mistakes and biases**. This is especially important where results could affect services or funding for disadvantaged L.A. communities (https://github.com/CityOfLosAngeles/best-practices).
6. **Automated Decision Making Systems (ADS) and dashboards must be interpretable**. Inputs and outputs must be documented with understanding of how the data is transformed, used, and known influences on the model (no black boxes).
7. **ZIP code must not be used as a unit of aggregation**. Aggregation by ZIP code masked the Flint Water Crisis. Instead, use census tracts or LA Neighborhoods.
8. **Data analysis results must be transparent**. While some datasets should be kept private, reports, analysis, and code should be open for inspection and questions.

Additional Resources

- Data Science Best Practices (https://cityoflosangeles.github.io/best-practices/)
- Ethics of Data Science (https://dl.acm.org/doi/pdf/10.1145/3144172?download=true)
- The WSJ Guide to Information Graphics (*can be purchased on Amazon.com*)
- The Grammar of Graphics (*can be purchased on Amazon.com*)

The Data Analysis Standards above were prepared by Hunter Owens, Technical Lead of the Data Science & Predictive Analytics Team at the City of Los Angeles Information Technology Agency. Before working for the City of L.A., Hunter worked at Obama for America and the Center for Data Science & Public Policy.

Digital Assistants & Chatbots

What are Digital Assistants & Chatbots?

Digital assistants and chatbots ("bots") are software that understands natural language voice commands and provides information or completes tasks for the user. Common examples are Microsoft Cortana, Amazon Alexa, Apple Siri, and Google Home. These digital assistants can take dictation, read messages aloud, setup appointments, schedule meetings, set reminders, and more. Powered by conversational artificial intelligence (AI), these tools are increasingly used by companies to offer new services to customers, reduce call hold times, and expand service hours. At the City of Los Angeles, our Chip the Chatbot has *answered over 133,000 resident questions* through LACity.org, the LABAVN.org business portal, LAPD Recruitment, and other websites. While automated digital assistants can improve equitable access to City services and customer service, they also have the potential to undermine public trust and negatively affect our residents.

Potential Issues with Digital Assistants & Chatbots

In order for Los Angeles residents and businesses to benefit from the City of Los Angeles' digital assistants and chatbots, we must ensure we address any potential issues that can arise from: 1) not properly identifying themselves as a bot 2) being unknowledgeable or unreliable 3) showing cultural bias or disrespect.

Bots Misidentifying Themselves: Humans make the understandable connection that when they are communicating with someone, they are communicating with another human. The technological development of digital assistants and chatbots can pose a sociological challenge when the human observes too many commonalities between the bot and another human (aka the "uncanny valley"). This is readily addressed by the bot clearly identifying itself as a technology tool there to help the human and not as another person.

Bots That Are Unknowledgeable or Unreliable: We've all experienced the frustration of a phone tree that makes it impossible to get to a person who can help us or answer our question. A bot that cannot answer your questions conveys the same frustrating feeling. Bots need to be pre-loaded with a substantial amount of answers BEFORE being made available to the public. Secondly, a knowledgeable bot will be frustrating if answers are unpredictable or unreliable. A well trained digital assistant must consistently answer questions from the public.

Bots That Are Disrespectful of Racial or Cultural Differences: As bots often have human-like personas, it is especially important that they interact respectfully and safely with the public. The possibility that AI-based systems can perpetuate existing societal biases, or introduce new biases, is a top concern in the scientific community. Bots must include cultural considerations, built-in safeguards, and protocols to handle the diversity of our community.

L.A. City Standards for Digital Assistants & Chatbots

At the City of Los Angeles, digital assistants and chatbots offer the promise of improved customer service options for L.A.'s residents, businesses, and visitors. The following are key standards for the effective use of bots at the City of Los Angeles:

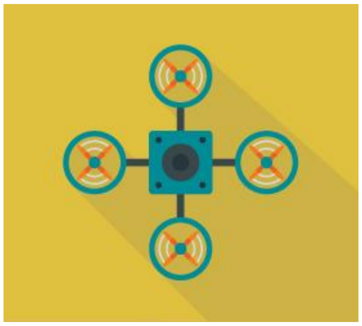
1. **Before developing a digital assistant or chatbot, clearly define its purpose, target audience, and value it will bring (aka mission)**. Understanding this mission is essential during the design, build, and maintenance of the bot.
2. **Be fully transparent to the public that they are using a bot and acknowledge any limitations.** This builds public trust.
3. **When initiating the conversation with a bot, be sure to clearly establish how the bot can help and any limitations up front.**
4. **Ensure your bot complies with ADA Section 508 accessibility standards.**
5. **To avoid offensive speech, program your bot to ensure it limits the "surface area" for norms violations.** For example, a bot whose purpose is to answer business permitting questions should never engage on topics of race, gender, religion, etc. If necessary, deploy a two-way filtering mechanism with a customizable threshold of tolerance to control what your bot takes in from users and says in response to prevent malicious users from re-training your bot.
6. **Ensure diversity in your bot development team.** A diverse development team is the first step in ensuring the bot addresses cultural differences.
7. **Systematically assess data used for bot training.** Assess bot training data to ensure it has appropriate representativeness and quality, taking steps to understand the lineage and relevant attributes of training data. Consider use of bias detection tools to ensure your bot treats all people fairly.
8. **Provide opportunities for the user to bypass the digital assistant and access a real human being.** This respects the public's individual preferences.
9. **Periodically review analytics about bot accuracy and reliability**. If bot accuracy is less than 51%, take steps to improve or else remove the bot from public use. Sentiment analysis tools and user feedback mechanisms are also valuable.

The Digital Assistant & Chatbot Standards above were prepared by the City of Los Angeles Information Technology Agency in collaboration with Microsoft Corporation through the writings of Lili Cheng, Corporate Vice President and Distinguished Engineer. Lili manages the Microsoft AI and Research division, responsible for the Microsoft AI developer platform.

Drones & Remotely Piloted Aircraft

What are Drones & Remotely Piloted Aircraft?

A drone or remotely piloted aircraft is a small, flying robotic device that is remotely controlled by a human operator or flies autonomously through software-controlled flight plans using embedded computer systems, onboard sensors, and GPS. Most of us have observed a hobbyist flying a remote controlled drone at the park or beach. Filmmakers have used quad copters (four propellers) with cameras to get exciting aerial shots for movies. Companies, like Amazon, have been testing the use of large flying drones to deliver packages to customers. While remote controlled aircraft are nothing new, drones have become much more sophisticated in their capabilities (software-controlled flight, cameras, GPS, battery power, and relatively low cost) and are becoming powerful tools for getting situational awareness or avoiding the need for humans to do a dirty or dangerous job, such as inspecting structures or utilities. Increasingly, drones are being used at the City of Los Angeles for firefighting, search and rescue, and utility inspection. However, automated aerial vehicles can raise ethical concerns about privacy and the data that drones can obtain and store. As drones are under the control and influence of the humans that use them, our Digital Code of Ethics includes potential ethical issues and the standards we apply at the City of Los Angeles.



Potential Issues with Using Drones

When using drones, special attention must be paid to potential issues that can arise from: 1) using drones only for unauthorized and unethical purposes 2) conflicts with other aircraft 3) insecure data collection and storage of images or video.

Using Drones For Unethical Purposes: The average resident feels an invasion of privacy when a drone hovers above their home, regardless of whether it is owned by another resident or the government. California State law (AB 856 // 2015) prohibits “entering the airspace of an individual in order to capture an image or recording of that individual engaging in a private, personal or familial activity without permission.” While there is a compelling commercial usage for drones at the City of Los Angeles, video and images must never be collected or stored of individuals engaging in a private, personal, or family activity at their home. Likewise, City of Los Angeles usage of drones must be for clear, compelling, and public uses.

Conflicts with Other Aircraft: Drones are not the only things in the sky. One major issue has been the use of drones in conflict with pilots of aircraft in occupied airspace. In Washington for example, a news helicopter was covering a fire when a drone started flying a few feet away from the helicopter. The FAA now receives over 100 complaints per month. It is critical for City of Los Angeles drone usage to abide by existing laws as it relates to uncontrolled airspace (Class G) and controlled airspaces.

Insecure Storage of Drone Data and Video: Drones provide a unique vantage point and often capture sensitive video and images. If a drone gathers data for its commercial purpose, then it must be securely captured and stored by the City department using the drone in compliance with the City of Los Angeles Information Security Policy.

L.A. City Standards for Using Drones

For the City of Los Angeles, drones are an effective way to coordinate resources for public safety (e.g. fighting a fire) and to perform dirty or dangerous work instead of a human. The following are key standards in the use of drones.

1. **Ensure ethical drone purposes before buying one**. Before acquiring a drone, establish compelling commercial purposes for it that will not violate State or Federal law. Ensure these purposes are clearly understood and adhered to by drone pilots.
2. **Train drone pilots and maintain equipment**. Establish proper training curriculum for pilots and maintenance regimen for all drones to prevent drone failure in which injury or damage can result.
3. **Perform required FAA drone registration and apply markings on all drones in service**.
4. **Abide by FAA airspace regulations**. Be sure to abide by all FAA drone airspace regulations and gain authorizations when required (e.g. below 400 feet in uncontrolled Class G airspace).
5. **Keep drones within visual line of sight when in use**.
6. **Delete inappropriate footage immediately.** If inappropriate footage of residents is obtained by a City of Los Angeles drone, especially if in the airspace of their home or property, it must be deleted immediately.
7. **Drones must be secured from hacking**. Ensure the drone has encrypted communications, default passwords are changed to long passwords, and chain of custody is established to ensure sensitive drone data is stored securely. This is necessary to avoid “maldrone” hacking attempts or data breaches.

The Drone and Remotely Piloted Aircraft topic above was prepared by Ted Ross, CIO of the City of Los Angeles and General Manager of the Information Technology Agency (ITA). Ted has over 23 years of private and public sector technology experience, has been featured in Fortune Magazine, The Wall Street Journal, and The Economist, and has earned various awards, including Top 25 Doer & Dreamer and CIO of the Year according to LA Business Journal. Ted has been an avid UAV enthusiast since the 1980s, starting with radio-controlled sailplanes (https://www.linkedin.com/in/ted-ross-643a616a).

P211

Facial Recognition

What is Facial Recognition Technology?

Facial recognition technology is the software and systems used to detect, analyze and compare facial features in order to identify unique individuals. Most of us have used facial recognition technology to unlock our Apple or Android smartphone by simply looking at the screen. Facebook and Google use facial recognition to identify and tag people in your photos, so you can easily search and find photos of your friends. has been used in a variety of ways. At the City of Los Angeles, any usage of facial recognition raises serious concerns around privacy and racial profiling, requiring approval by the Office of the City Attorney. This technology has become viable as the quality of facial recognition results has evolved over the past 60 years through the use of increasingly sophisticated statistical models, such as “deep neural networks” which have proven to outperform human facial recognition in certain cases. Technology even allows mobile face recognition through drones and smart glasses. At this time, performance is imperfect, proving to be variable and potentially prone to error.

Potential Issues with Facial Recognition Technology

For facial recognition, special attention must be paid to potential issues that can arise from: 1) the way the technology is deployed and 2) inherent system features.

Deployment Issues: Facial recognition databases contain personally identifiable information (PII) about individuals. For acceptable usage, this information is sensitive and must be highly secured from data leakage or allow unauthorized access. Secondly, facial recognition is often cross-referenced with known “watchlist” databases that may be erroneous themselves, causing false positives in the results. Third, facial recognition has shown bias against people of color. The globally-recognized National Institute of Standards (NIST) conducted studies in 2019 and found empirical evidence that Asian and African-Americans were up to 100 times more likely to be misidentified than Causasian subjects, with Native Americans having the highest false positive rate of all ethnicities.

Fourth, some facial recognition uses may be indiscriminately and passively on, thus identifying children (minors) and vulnerable individuals and then inappropriately storing data about them and, by default, their movements. The collection of this data is highly inappropriate and unjustified in most cases. Fifth, regulations for facial recognition are rapidly evolving. Even a justifiable and ethical usage of facial recognition must adhere to federal, state, and local ordinances.

System Feature Issues: Model performance is dependent upon the quality and quantity of training data. If training data is not representative of the population, it will skew results and generate false matches, especially for particular ethnicities, and may not be able to handle occlusion adequately. Secondly, all systems are prone to error, especially as lighting conditions, movement, distance from the subject, and occlusion erode performance. Facial recognition errors, no matter how unlikely, must be accounted for and accommodated with any facial recognition system.

L.A. City Standards for Facial Recognition Technology

At the City of Los Angeles, the usage of facial recognition is prone to privacy issues and racial profiling, requiring an extremely compelling justification and greater safeguards than other emerging technologies in these standards. The following are key standards for the use of facial recognition at the City of Los Angeles:

1. **The use of a facial recognition system must first be approved by the City of Los Angeles City Attorney Office to ensure adherence to current laws and ethical usage**. Requests must detail scope, justification, and data protection impact assessment (describe collection, use, and deletion of personally identifiable data).
2. **Facial recognition systems must be thoroughly tested**. Tests must involve real world conditions with the results evaluated against performance benchmarks (industry reports, NIST evaluations, etc) before being relied upon.
3. **Facial recognition systems must be evaluated for the specific, authorized usage**. Facial recognition systems on the market exhibit performance idiosyncrasies with differing strengths and weaknesses that must be accounted for.
4. **Before soliciting for a facial recognition system, specific use case requirements must be detailed and the chosen product must meet those requirements**. Unethical vendors have spoofed good results through altered conditions. In addition, highly tailored systems are often unnecessary, opting instead for proven, standardized technology platforms.
5. **Alternative biometric or traditional solutions must be considered first**. Facial recognition may be expensive, unreliable, and not necessary for desired outcome.
6. **Facial recognition systems should be clearly identified via signage and other public notifications using conditions of entry, terms of employment, etc.**
7. **Facial recognition systems must be audited every two years**. This is necessary to confirm proper collection, prevent expanded scope, maintain accuracy levels across different races, deletion of PII, data security, safeguards for minors, etc.
8. **Facial recognition systems must adhere to City's Information Security Policy**.

The Facial Recognition Standards above were prepared by the City of Los Angeles Information Technology Agency in collaboration with Nick Ingelbrecht, Senior Research Director with Gartner Inc. (https://www.gartner.com/analyst/18260).

Healthcare & Personally Identifiable Information (PII)

What is Healthcare & PII?

Healthcare data is information and data which relate to the physical/mental health of an individual or the provision of health services to that individual. This data includes your blood type, existing medical conditions, medical procedures you have had, medications you are using, blood pressure, etc. Healthcare data is a very sensitive form of personally identifiable information (PII), which is information that permits the identity of an individual to be reasonably inferred. If maliciously or accidentally revealed, health data can result in many harmful actions, such as embarrassment, discrimination, impersonation, and even blackmail. While some City of Los Angeles departments (e.g. L.A. Fire Department paramedics) have specific needs to gather healthcare and PII data, other City departments must avoid gathering and storing this information. Under the Health Insurance Portability and Accountability Act (HIPAA), health information is privileged and cannot be shared without consent, unless for the safety and welfare of others.

Anonymized healthcare data can be beneficially used in biomedical and health research for preventive, diagnostic and therapeutic public benefits. At the City of Los Angeles, analysis of employee health data has revealed workplace safety issues that were resolved for the safety of employees. Anonymized resident health data has been used by universities to reveal public health issues, environmental hazards, and influence urban plans. However, there are many serious potential issues that must be addressed.

Potential Issues with Storing Healthcare & PII Data

When storing health data or PII (or considering the analysis of health data), special attention must be paid to potential issues that can arise from 1) limits of de-identification 2) added pressures on consent procedures 3) transferability of health data to other domains 4) risks associated with analytics 5) meaningfulness of consent:

Limits of De-Identification: Health data may be re-identifiable, even when substantial identifiable information has been removed. This may result in insufficient privacy protection for individuals in the data set. New opportunities for data linkage and the integration of different data sets (e.g. social networking, internet searches, web postings, medical devices, wearables, or smartphone apps) can make re-identification possible.

Added Pressures on Consent Procedures: When data is collected and stored for future use, it is difficult to anticipate future uses and therefore difficult to ensure fully informed and specific consent from the individual. Secondary and subsequent data use should be more transparent, and allow people to consent (or withdraw consent) for both anticipated and unanticipated future uses.

Transferability of Health Data to Other Domains (and Vice Versa): Data sets can be used to make health-relevant inferences pertaining to individuals. Thus, data that was not collected for health-relevant purposes can unethically be used in a health-relevant way.

Risks Associated With Predictive Analytics & Inferences: Individuals don't have insight on how their own data is used to make inferences or predictions about them. If there is a negative impact to them, even if inaccurate data is used, there are no easy options available to them to rectify the harm/error or seek redress.

Meaningfulness of Consent When Required for Services: Consent, authorization, or permission for data release is less meaningful when patients have little choice — such as emergency ambulance services, mandatory health insurance, drug prescription subsidies, or use of health-related social networks, smartphone apps, wearables, and monitors.

L.A. City Standards for Using Health Data or PII

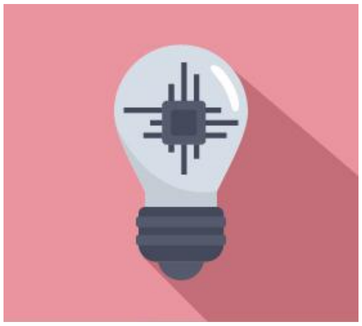
For the City of Los Angeles, healthcare data and PII (if ethically obtained and secured) is essential for some services (e.g. ambulances) and potentially beneficial for identifying public health issues. To avoid ethical issues, the following are key standards:

1. **Do not gather or store any L.A. resident healthcare data and PII, unless essential to your department's responsibilities (e.g. L.A. Fire Department).**
2. **Respect the obligation to protect an individual's privacy.** Understand the rules and laws regarding personal data including Personally Identifiable Information (PII) and Protected Health Information (PHI).
3. **Use the minimum personal data necessary to achieve the desired outcomes**.
4. **Unless under emergency circumstances, allow individuals the opportunity to determine whether or how their personal data may be collected, used, or share** This should include providing consent and methods to control use/access to their data.
5. **Always use data for the purpose in which it was collected and consented for**.
6. **Do not share health data or PII with other agencies, unless understood and consented by the individual**. Then, anonymize and restrict access to the shared data using the City of Los Angeles Data Sharing Agreement.

The Healthcare Data & Personally Identifiable Information (PII) topic above was prepared by Timothy Lee, Chief Information Security Officer, and Madeline Dia, Information Security Governance Manager, at the City of Los Angeles Information Technology Agency. Tim and Madeline bring over 40 years of combined experience in data security and technology management.

Internet of Things (IoT) & Sensors

What is the Internet of Things (IoT)?



According to Oxford Dictionary, the Internet of Things (IoT) is “the interconnection, via the Internet, of computing devices that are embedded in everyday objects, enabling them to send and receive data.” While not one specific device or technology, the Internet of Things (aka the Internet of Everything) is the digital connection between electronic devices (computers, sensors, cameras, smartphones, home appliances, and other networked devices) that enables tremendous new capabilities between internet-connected devices and the humans around them. This includes “smart” light bulbs that can be controlled by your smartphone and Fitbit watches that track your daily step count. Ring doorbells that track when a package was delivered and send photos of your visitors are IoT devices. Parking meters that allow use of credit card and automatically notify the City when they are broken are also IoT devices. These sensors are generating unprecedented amounts of data and posing unprecedented challenges around security, privacy, and sustainability. In 2018, the world had over 7 Billion IoT connected devices. In 2019, this increased to over 22.6 Billion devices, with 127 new IoT devices connecting to the Internet every second. As the City of Los Angeles increasingly uses sensors and connected devices to improve our urban landscape and gather important information about water usage, traffic, pollution, and noise, the ethics around IoT becomes an important set of standards.

Potential Issues with the Internet of Things (IoT)

When implementing and using IoT sensors, special attention must be paid to potential issues that arise from: 1) physical safety; 2) informed consent; 3) privacy; 4) information and device security; 5) congestion of IoT devices.

Physical Safety: IoT allows for increased automation and “action-at-a-distance”, allowing the digital world to affect the physical one. For example, an IoT connected automobile is able to identify that the owner is approaching the vehicle, sense the temperature, turn itself on, and change the thermostat to a cozy 72 degrees. Across a city, you can imagine the tremendous benefits of a living, adjusting “Smart City” that alters traffic and lighting for the benefit of the public. If hacked and maladjusted, this could impact the physical safety of its occupants, so substantial controls are needed to ensure physical safety when using IoT.

Informed Consent: Informed consent is when someone impacted by technology has clear understanding and agreement to the use of the technology, along with the implications and consequences of the use. With an increasing number and integration of public and private IoT devices, it becomes much more difficult to gain informed consent, often devolving into “implied consent”. Getting to informed consent with IoT devices is important in the collection of any personal information.

Privacy: The increasing array of IoT sensors must be careful of the privacy rights of City of Los Angeles residents. First of all, IoT data must abide by the City’s privacy standards on what can be collected. For example, noise or pollution monitoring data is acceptable in a neighborhood, while audio recordings of a resident is not. Secondly, IoT data must not invade privacy in how the data is used. For example, a well known merchandising store analyzed and profiled client purchasing habits and inappropriately sent a pregnancy related mailer to a teenage girl whose family was unaware. The average American viewed this as an invasion of privacy.

Information & Device Security: IoT technology can provide security concerns due to the fact that it can be physically accessible to a hacker, is often constantly in communication with its network, and is typically a low cost device that infrequently receives security patches. This requires security of the data collected by the IoT device, the communication channel, and the device itself. These security concerns were demonstrated in 2016 when the Mirai malware controlled a large number of IoT devices and used them to commit a “distributed denial of service (DDoS)” cyber attack. The City of Los Angeles cannot allow government devices to be data breached or converted into a zombie bot that assists in damaging the property of others.

Congestion by IoT Devices: With the proliferation of IoT sensors, City of Los Angeles departments must collaborate to install multi-purpose devices wherever possible to prevent congestion of sensors and devices in the urban landscape. Through appropriate coordination, devices can perform multiple purposes making them easier to secure, more cost effective, and reduce unsightly congestion of digital devices in public.

L.A. City Standards for IoT & Sensors

For the City of Los Angeles, the Internet of Things provides tremendous benefits for monitoring conditions in our urban landscape (traffic, pollution, public safety, excessive noise, etc) and providing real time feedback/response to improve quality of life for L.A.’s residents. The following are key standards in the use of IoT and sensors:

1. **Acquire IoT devices in coordination with other City Departments through the IT Policy Committee.** Single purpose IoT devices will be expensive, difficult to secure, and create unsightly congestion in L.A.’s streets. City Departments preparing to implement IoT devices must first communicate and coordinate with other departments using an agenda item in the City’s Information Technology Policy Committee (ITPC).
2. **Analyze the type of data you will capture and establish appropriate levels of security using Information Security Policy**. Assess the type of data being

collected by the IoT sensor, classify using the City of L.A. Information Security Policy, and institute the appropriate level of security. The following are considerations to secure devices (based on the sensitivity of data collected):

   a. Periodic patching of device operating system and software
   b. Implement encryption at rest and in transit
   c. Place sensors on secure communication networks (e.g. cellular).
   d. Hide and anonymize IoT identifiers. Ensure that IoT sensor identifiers are hidden and anonymized to prevent collection analysis by hackers.
   e. Manage encryption keys to prevent unauthorized decryption of devices.
   f. Secure boot technology to ensure only known software can run on device.
   g. Use of hardware-rooted trust chains to prevent low-level software attacks.
   h. Use software that identifies compromised or malfunctioning devices so they can be repaired or removed.

3. **Establish security for systems that interconnect with your IoT**. An IoT device operates in concert with other connected devices (using an attack vector to compromise the device). Establish a network diagram of interconnected IoT devices with permissions between each other. Implement security for all connected devices at the level required by the most sensitive devices (i.e. secure them all at the level required for the most security sensitive device).

4. **Do not place IoT sensors directly onto City network**. By nature, IoT is often in the public and potentially accessible by the public. It is forbidden to connect an IoT device directly onto the City of Los Angeles network, allowing a potential threat vector for hackers to access the internal City network. Connectivity needs to be provided through separate communications vehicle (e.g. ISP, cellular, etc).

5. **Limit access of IoT sensors to the public.** IoT sensors are often in the public domain, which requires efforts to limit physical access using locked cases, elevation on light poles, hiding from sight, etc.

6. **Share data with other City departments and open data portal.** Mayor Eric Garcetti's Executive Directive #3, states: "To promote transparency and accountability, the City of Los Angeles (“City”) will make publicly available raw data in easy-to-find and accessible formats… made freely available for use by the public, subject only to valid privacy, confidentiality, security, and other legal restrictions." Unless it is subject to the restrictions listed above, IoT data needs to be added to the Data.LACity.org open data portal.

The IoT Standards above were prepared by Joyce Edson, Executive Officer, of the City of Los Angeles Information Technology Agency. Joyce has over 33 years of enterprise IT and management experience and is a founding member of the Intelligent IoT Integration (I3) consortium with the University of Southern California (USC) and 90 other member organizations (https://www.linkedin.com/in/joyce-edson-468b855/).

Social Networks & Media

What are Social Networks & Media?

More than 4.5 billion people around the world use the Internet, of which, 3.8 billion people are a part of an online, social network using a social media platform (DataReportal, 2020). More than 72% of Americans use social media (Pew Research, 2019). That is 238 million Americans interacting with each other, with businesses, and with government entities at all levels. Social Media is interactive computer-mediated technologies dedicated to facilitating community-based input, interaction, content-sharing, content-creation, and collaboration. These channels include social networking sites, weblogs (blogs, vlogs, or microblogs), podcasts, online chat sites, and forums. Examples include Facebook, Youtube, Twitter, Tumblr, LinkedIn, Instagram, Snapchat, and TiKTok. For the City of Los Angeles, social media and social networks can transform the ways in which our government, our City departments, and our elected officials relate to the public. These powerful sets of tools can be highly beneficial by allowing constituents easy, engaging, and immediate access to government information or services. However, as with any publicly shared medium there are risks and ethical issues that must be addressed.

Potential Issues with Social Networks & Media

When using social media, special attention must be paid to potential issues that arise from: 1) maintaining transparency; 2) impartiality in messaging and branding; 3) censorship; 4) active engagement with public; 5) privacy concerns with social media monitoring tools.

Maintaining Transparency: Governments hold positions of power. Access to government is a fundamental right for every L.A. resident. In social media, openness and transparency are driving principles when communicating with the public. Letting residents see and hear an unfiltered side of government service is genuine and typically a best practice approach.

Impartiality in Messaging: Social media coordinators must remain impartial when sharing official messaging and be authentic in representing the brand, voice, and goals of their government organization when communicating with and engaging target audiences (residents, businesses, visitors, and other stakeholders). To be authentic is to be accurate, clear, concise, and responsible in communications, regardless of personal opinions.

Censorship: City employees who coordinate or manage a City social media account are stewards of interactive, public forums. Public forums managed by government and elected officials are subject to First Amendment civil liberties and may not discriminate against or censor the viewpoints of private speakers.

Active Engagement with Public: By its nature, social media is bi-directional communication that should be engaging. Social media coordinators are tasked with engaging the public, especially during times of emergency, disaster or public health crises.

Privacy Concerns with Social Media Monitoring Tools: Social media monitoring or listening tools analyze public discussions on social media. These tools provide insight into public sentiment, access to real-time feedback, allow timely contribution to open conversations, and provide the ability to respond to public questions. However, while not private, some social media users may be put off by stepping into their conversation. Please consider tone and stakeholder comfort if using a social media monitoring tool to engage the public.

L.A. City Standards for Social Networking & Social Media

At the City of Los Angeles, social media provides transformational opportunities to listen to and engage our public. To do so ethically, the following are key standards for the use of social networks and social media at the City of Los Angeles:

1. **City social media messages must be on mission, accurate, and respectful**. Employees and elected officials are responsible for ensuring social media content is relevant to their organization's mission, professionally presented, accurate, and respectful of L.A.'s diverse communities. Messages with bad grammar or unfactual should be removed immediately to maintain public trust.
2. **City social media must be unbiased and impartial**. As taxpayer-funded City officials, our social media accounts must remain unbiased about prioritizing one political agenda over another, whether in local or national politics. Messaging should instead guide residents to engaging their elected officials and government directly.
3. **City social media cannot censor the public**. City social media cannot violate the First Amendment and must allow speech in public forums as protected, with narrow exceptions such as threats, fighting words, or incitement to imminent lawless action (https://www.abajournal.com/magazine/article/social-clashes-digital-free-speech).
4. **City social media must understand their department's or elected official's voice and brand**. Consistency is important, especially when multiple people manage an account. Messaging should also be vetted, verified, and credible.
5. **L.A. City government social media platforms must not participate in data surveillance or sharing with third-parties**. Additionally, use of social media monitoring must include feedback loops from the public.
6. **Use the City of Los Angeles Social Media Policy for guidance**. The City policy provides procedures and standards for use of social media and tools.

The Social Media topic above was prepared by Mariana Ferraro, Social Media Director at the City of Los Angeles Info Tech Agency. Mariana has 24 years of experience in broadcast production & communications, including over 40 supervising producer credits.

Virtual and Augmented Reality

What is Virtual or Augmented Reality?

Virtual reality (VR) is "an artificial environment which is experienced through sensory stimuli (such as sights and sounds) provided by a computer and in which one's actions partially determine what happens in the environment" (Webster's Dictionary). VR is associated with a headset (Oculus, HTC, Samsung, etc) that blocks out the real world around you while substituting it with a computer generated reality that allows for our interaction in one form or another. While commonly associated with the gaming industry, VR has many applications, including at the City of Los Angeles for promoting tourism, highlighting the L.A. River, and recruitment of potential City employees. While related, Augmented Reality (AR) is "an enhanced version of reality created by the use of technology to overlay digital information on an image of something being viewed through a device (such as a smartphone camera)." While VR is a complete environment that replaces reality, AR only enhances what we see by adding digital elements. One of the most recognizable AR apps was Pokemon Go, which used built-in GPS, camera, and screen in the smartphone to allow users to digitally catch and train Pokemon characters in real-life locations. At the City of Los Angeles, AR has been used to train employees in complex job tasks (e.g. L.A. Fire Department headset repair) and test technical employees for job aptitude. If you have ever used your computer to imagine what colors or furniture would look best in your home or used your smartphone to see how different clothes would look on you, then you are no stranger to AR.

Potential Issues with Virtual Reality (VR) & Augmented Reality (AR)

While virtual and augmented reality can be powerful technologies, special attention must be paid to potential issues that can arise from: 1) safety 2) behavioral manipulation 3) privacy/consent 4) security.

Safety: The physical safety of AR/VR users must be considered. These issues came to the forefront during the popularity of Pokemon Go. Many car accidents, lawsuits, and fatalities were the result of players paying too much attention to their digital environment and not their actual physical one. In addition, these altered states can result in nausea and bouts of dizziness. The overall safety of users must be factored in during the creation process.

Behavioral Manipulation: An immersive environment (VR) or digitally augmented environment can be very suggestive and persuasive, especially among vulnerable groups (children, elderly, those with cognitive disabilities, the mentally ill, etc). City departments must closely review and scrutinize VR/AR content they create to understand how it can affect their users and avoid content that reinforces negative behavior.

Privacy/Consent: An immersive or augmented experience may purposefully or inadvertently gather digital information from its users. Users would need to provide explicit permission before the collection or sharing of information. Additionally, privacy is not just about whether or not information is collected/shared, but about safety. Tracking current and historical locations may enable criminal conduct that puts the safety of users at risk.

Security: The cyber security risks of AR/VR should be considered. Security must be included during the creation of the application. Immersive or augmented environments must be secure and safe from hackers. The physical and mental safety of users is paramount among the concerns that can result from security or data breaches.

L.A. City Standards for Usage of Virtual & Augmented Reality

At the City of Los Angeles, the usage of virtual or augmented reality can be a tremendous benefit to the public so long as safety, behavioral, privacy, and security issues are avoided. The following are key standards for the use of virtual and augmented reality at the City of Los Angeles:

1. **Warnings and disclaimers must be provided to ensure physical safety when using Virtual or Augmented Reality.** Instruct the user to access the content within a safe environment free from distraction and require them to be seated if possible.
2. **Negative behavioral impacts must be assessed and avoided.** Creators of AR/VR content must consider and test mental consequences on a focus group prior to public release. Identify the potential risks and subsequent symptoms which may arise and make necessary content changes or else eliminate the app.
3. **Avoid data collection or obtain explicit consent from the user if data collection is necessary.** Ensure that users are made aware of the data to be collected and who it would be shared with. Users should be clearly presented with an option to opt out of any collection and sharing of data, unless for the specific purpose of job testing.
4. **Secure all Virtual and Augmented Reality applications**. Current encryption standards should be built into all AR/VR applications. If data must be collected, it must adhere to the City of Los Angeles Information Security Policy. In addition, City-issued devices must have malware protection that is regularly updated.

The Virtual & Augmented Reality topic above was prepared by Anthony Moore, Deputy Chief Information Officer over Infrastructure at the City of Los Angeles Information Technology Agency. Anthony has over 21 years of technical and managerial IT experience, working across multiple government agencies, telecommunications, and a health care company (https://www.linkedin.com/in/anthonymooremba/).

P222

OUR COMMITMENT TO LOS ANGELES

As Information Technology professionals at the City of Los Angeles, we are committed to serving the residents and businesses of Los Angeles by building thoughtful, human-centric technology solutions that are easy to use, cost-effective, and secure, through competitive contracting.

In our commitment to Los Angeles, we will hire an IT workforce that is as diverse as Los Angeles itself, and use technology to build bridges between City government and underserved communities.

We are committed to upholding the values and standards explained in this Digital Code of Ethics to build public trust, while deploying innovative and ethical technology solutions.

City of Los Angeles Departments

Aging
Airports
Animal Services
Building & Safety
Cannabis Regulation
Chief Legislative Analyst
City Administrative Officer
City Attorney
City Clerk
Civil & Human Rights
Controller's Office
Convention & Tourism Development
Cultural Affairs
Disability
Economic & Workforce Development
El Pueblo de Los Angeles
Emergency Management
Employee Relations Board
City Ethics Commission
Office of Finance
Los Angeles City Fire Department
Fire and Police Pensions
General Services
Harbor
Housing Authority
Housing and Community Investment
Information Technology Agency
Library
LA City Employee Retirement System (LACERS)
Mayor's Office
Neighborhood Empowerment
Office of Public Accountability
Personnel
City Planning
Los Angeles Police Department
Board of Public Works
Public Works, Bureau of Contract Administration
Public Works, Bureau of Engineering
Public Works, Bureau of Sanitation
Public Works, Bureau of Street Lighting
Public Works, Bureau of Street Services
Recreation & Parks
Transportation
Water and Power
Zoo

CONTACT US

For questions, comments, or concerns about digital ethics at the City of Los Angeles, please contact the Information Technology Agency through the LA City website (https://www.lacity.org/submit-feedback).

For potential fraud or abuse, please contact the anonymous Fraud, Waste, and Abuse Hotline from Controller’s Office (https://lacontroller.org/report-fraud-waste-and-abuse/).

P224

Ron Galperin
Controller

July 14, 2021

Honorable Eric Garcetti, Mayor
Honorable Michael Feuer, City Attorney
Honorable Members of the Los Angeles City Council

Re: Protecting Privacy Makes a Smarter L.A.

New technologies present exciting opportunities for local governments to improve the delivery of essential neighborhood services, increase efficiency and enhance the quality of life for residents — making cities more innovative and advanced, and, in turn, “smarter.” While Los Angeles continues to pursue smart city initiatives, it is increasingly critical for the City to prioritize the safety and privacy of the Angelenos we serve. This is especially important when it comes to programs that employ surveillance technologies and collect personal data, as they represent serious privacy risks if managed improperly.

The City is currently developing policies and plans to help guide how departments modernize their information services, and how smart technologies are deployed — including the SmartLA 2028 Plan, the Digital Bill of Rights, the Code of Ethics and more. However, at this time, no single City entity is responsible for evaluating the privacy implications created by using surveillance technologies, which often have the ability to analyze the movements, behavior or actions of identifiable individuals. My latest report analyzes the City’s privacy-related efforts and recommends a new framework for evaluating and mitigating risks, which will help the City protect residents as it develops new technologies and modernizes services.

A decentralized approach

As it stands, managing information and privacy is typically left to each City department. They must individually determine whether specific technologies or applications are necessary and how these tools will be used to meet their operational needs. My office found that City departments have taken many different approaches to address privacy risks associated with surveillance tools — an ad hoc method that creates inconsistencies and accountability gaps.

Additionally, the City does not currently define or inventory the surveillance technologies it uses, nor does it designate a responsible body for overseeing departments' use of these tools. While there are some existing data management and security measures in place to ensure that the City's information systems and sensitive records are protected, still lacking is a formal privacy management program that sets specific guidelines for addressing risks associated with the use of surveillance technologies.

Implementing best practices

To ensure the City is adequately protecting the public's privacy, more safeguards are needed and should be consistent with those established by the federal government, the State of California and other local jurisdictions. My report recommends that City policymakers should:

- Clearly **define surveillance technology** and identify what is used by departments.
- Develop a standardized **surveillance impact assessment and reporting** process.
- Establish a **privacy advisory board** to support departments' development of privacy policies and controls.
- Require departments to **update surveillance impact assessments** on an ongoing basis.

As Controller, my goal is to make Los Angeles the smartest, most transparent City in the world. To achieve this, we need to stay up to date with emerging technologies, but at the same time, keep the safety, needs and privacy of Angelenos at the forefront of our work. I urge City leaders to adopt a framework that allows us to evolve and innovate as a City and engender greater public trust in our government.

Respectfully submitted,

RON GALPERIN
L.A. Controller