Smart Cities Privacy & Equity
Online Course Outline and Content

This document provides an outline of the asynchronous, online Smart Cities, Privacy & Equity course we created as part of a 2021-2022 PIT-UN grant with links to all of the content and a text version of the quizzes with the answers highlighted. The course itself is publicly available for anyone to complete for free on udemy.com.

Please contact Professor Brian Ray if you have any questions about the materials or would like more information: b.e.ray@csuohio.edu.

Course Outline

Section 1: Introduction
- Lecture: Introductory Video

Section 2: Smart Cities, Privacy & Equity Overview
- Lecture: What is Privacy?
- Quiz: What is Privacy?
- Lecture: What's the Problem with Smart Cities
- Quiz: What's the Problem with Smart Cities
- Lecture: Shedding Light on Smart Cities
- Quiz: Shedding Light on Smart Cities
- Lecture: The Legal Gap
- Quiz: The Legal Gap
- Lecture: Community Control Over Policing: Introduction
- Lecture: Optional Resources to Dive Deeper

Section 3: Surveillance Technologies Overview
- Lecture: Street Level Surveillance
- Quiz: Street Level Surveillance
- Lecture: Police Surveillance
- Quiz: Police Surveillance
- Lecture: Interactive Surveillance Technology Tools
- Lecture: Tracking Data
- Lecture: Surveillance Meets the Internet of Things
- Lecture: Racial Equity and Data Privacy
- Quiz: Race and Regulation

Section 4: Analyzing Privacy & Equity Impacts of Technology
- Lecture: Smart Decisions About Surveillance
- Quiz: Smart Decisions About Surveillance
- Lecture: Community Transparency, Accountability & Oversight
- Lecture: Privacy Impact Assessment

Section 5: The City of Oakland Privacy Advisory Commission: Evaluating ALPRs
- Lecture: Oakland Privacy Advisory Commission (OPAC)
- Lecture: Oakland ALPR Use Policy

Quiz: The City of Oakland Privacy Advisory Commission: Evaluating ALPRs
Lecture: Oakland ALPR One-Year Report
Lecture: Additional Resources

Section 1: Introduction to Smart Cities, Privacy & Equity
Introductory Video

In this video meet the team that created the course and learn why should we care about surveillance technologies and what can you do to ensure they help rather than harm your community?

https://csuohio.hosted.panopto.com/Panopto/Pages/Sessions/List.aspx#folderID=%226a0a1745-1511-43a2-a560-aed0014141b9%22

Section 2: Smart Cities, Privacy & Equity Overview
Identify privacy and equity concerns Smart Cities raise.

Lecture: What is Privacy?

This article addresses the vexed question: What is Privacy? It introduces the major areas of privacy and explains how the concept is used in several contexts.

After you watch the following video, please take the What is Privacy Quiz before moving on to What's the Problem with Smart Cities?

Article: What is Privacy?
https://privacy.ucsd.edu/privacy/index.html

What is Privacy Video (Embed in UDEMY)

Video: What is Privacy?
https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=02cddf92-95c0-412a-b840-aed001415d01

QUIZ

What concept does this excerpt from University of California Privacy and Information Steering Committee Report describe?
"An individual's ability to conduct activities without concern of or actual observation"

a. Information Privacy
b. Autonomy Privacy
c. Communication Privacy
d. None of the Above

What category of personally identifiable information includes location information and web browser history?

a. Direct Identifiers
b. Indirect Identifiers
c. Pseudo-Identifiers
d. None of the Above

In our CUPS acronym for the data lifecycle what does the S stand for?

a. Security
b. Subject Rights
c. Sharing
d. None of the Above

What two factors do we consider when thinking about risk?

a. Probability and Likelihood
b. Probability and Impact
c. Harm and Impact
d. None of the Above

Which of the following is NOT an accepted response to risk discussed in the video?

a. Forget
b. Accept
c. Transfer
d. Mitigate

Lecture: What's the Problem with Smart Cities?

Saving the City: San Diego Smart Streetlights and the Promise and Perils of Smart Cities. From the documentary page: *How did the simple streetlight become an instrument of surveillance? Under the label of "Smart Cities" – meaning Big Data – cities can now watch, track and identify ordinary people in ways George Orwell could never imagine. Join us as we illuminate the issues that surfaced in San Diego after the city installed 14,000 new streetlights including over 3,000 with sensors, cameras and other data-gathering gear.*

Please watch the video linked above. Then take the *What's the Problem with Smart Cities* Quiz before moving on the *Shedding Light on Smart Cities*.

Video: Saving Our City | San Diego: Smart Streetlights and the Promise and Perils of Smart Cities
https://vimeo.com/608090394

QUIZ

When the Smart Streetlight installation initially occurred, who drafted the policy to regulate their use?

a. The San Diego Police Department drafted the use policy.

b. The public and city staff collaborated on the use policy.
c. Neither. There is no policy regulating the use of the Smart Streetlights.
d. The American Civil Liberties Union (ACLU) drafted the use policy.
e. The San Diego City Attorney drafted the use policy.

Which famous corporation coined the term "Smart City"?

a. General Electric
b. Amazon
c. International Business Machines (IBM)
d. Tesla

What are the features highlighted in the video that the Smart Streetlights provided to the City of San Diego?

a. Pedestrian Counters
b. Automobile Counters
c. Weather Sensors
d. Video
e. All of the above

Compared to the stated purpose of the Smart Streetlights installation at its inception, has any “mission creep” occurred as to its use?

a. No, the system has been used in alignment with its original stated purpose.
b. No, the system isn’t functional and hasn’t been used.
c. Yes, the San Diego Police Department used video footage to investigate violent crime and monitor protests

What are the key components of the proposed surveillance technology vetting framework highlighted in the video?

a. Community engagement and input into the rule making for use of such technology.
b. Privacy Advisory Board
c. Transparency and Efficacy reporting
d. A pre-checklist of issues to address prior to acquisition or use
e. All of the above.

Lecture: Shedding Light on Smart Cities

This lecture highlights some of the key industries, technology enablers, and stakeholders behind smart cities initiatives and explores the potential range of privacy risks posed by smart cities as well as some of the key tools for addressing them.

Please watch the following video, explore the interactive infographic, and take the *Shedding Light on Smart Cities* Quiz before moving on to *The Legal Gap.*

Article: Shedding Light on Smart City Privacy

https://fpf.org/uncategorized/smart-cities/

Video: Shedding Light on Smart City Privacy

https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=2f288da0-ff4c-46aa-b3a5-aed001415d1c

QUIZ

What technologies help enable "smart" features and services?

a. Connectivity services, like public WiFi or broadband
b. Internet-enabled devices and sensors, like noise sensors or drones.
c. Mobile services, like smartphone apps and location beacons.
d. Data analytics, like automated traffic controls or smart grids.
e. Crowd-sourced usage data, like buses or trash trucks that re-route based on demand.
f. All of the above.

Which of these are *not* smart city stakeholders?

a. Individuals
b. Businesses
c. Government officials
d. Universities
e. Public-private partnerships
f. Non-profits and advocacy groups
g. Community groups
h. Technology providers
i. It's a trick question - these are all stakeholders.

What are privacy concerns related to data quality?

a. Ubiquitous collection of data by corporate and government entities may lead to "mission creep" and strengthen power imbalances between individuals and institutions.
b. Data collected from individuals for one purpose may be used or disclosed for another unexpected purpose without additional notice or consent.
c. Public records laws and open data portals may reveal personally identifiable information to the public.
d. Biased, inaccurate, or incomplete data may lead to poor or inefficient decision-making, unethical or illegal uses of data, and discriminatory outcomes.
e. Personal information is leaked or exposed when an information system is compromised.

What privacy tool relies on engaging communities and informing individuals about how and why their personal data will be collected and used, and offer choices to participate where possible?

a. Privacy program management
b. Transparency and individual choices
c. Local storage and processing
d. Data minimization
e. Vendor management
f. De-identification

What privacy tool relies on rendering personal information unidentifiable?

a. Privacy program management
b. Transparency and individual choices
c. Local storage
d. Data minimization
e. Vendor management
f. De-identification

Lecture: The Legal Gap

This lecture summarizes the complex U.S. data privacy legal landscape and explains why our federal system has resulted in a patchwork of federal and state laws that fail to address the risks posed by smart cities.

Please read the linked article, watch the following video, and take *the Legal Gap* Quiz before moving on to the final*Community Control Over Policing: Introduction*.

Article: The Legal Gap

https://medium.com/golden-data/smart-cities-policing-technology-and-privacy-are-we-there-yet-c83dde7c218d

Video: The Legal Gap

This lecture explains how existing U.S. privacy laws - both federal and state - fail to address the privacy and related risks raised by public use of surveillance technologies.

https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=acedea22-c83d-4200-bbbf-aed001415d1d

QUIZ

Which federal law regulates the use of surveillance technologies by local and regional government?

a. The U.S. Privacy Act of 1974
b. No federal law regulates this area
c. The California Privacy Act of 2018
d. The EU General Data Protection Regulation (GDPR)

What does federalism mean in the US?

a. Federalism means that the federal government is not restricted in any way from regulating smart cities and municipalities
b. Federalism in the US means that the governments of the states coexist with the federal government and that this federal government has specific enumerated powers granted by the United States Constitution.
c. Federalism means that state legislators cannot regulate smart cities and municipalities.
d. None of the above.

The “Community Control Over Police Surveillance” (CCOPS) effort seeks to:

a. Ensure that local communities have a meaningful opportunity to review and participate in all decisions about how surveillance technologies are acquired and used locally.
b. Ensure that surveillance technologies are never deployed.
c. Promote the use of certain surveillance technology.
d. Reduce the cost associated with the deployment of surveillance technologies.

Smart cities and municipalities across the US:

a. Are subject to comprehensive state privacy laws that impose meaningful restrictions on how smart technologies collect, use and share data.
b. Are always legally required to involve their communities before making the decision of deploying surveillance technologies.
c. Are subject to very few federal or state legal requirements that impose meaningful restraints on whether and how to deploy surveillance technologies
d. Are generally not interested in deploying surveillance technologies.

Lecture: Community Control Over Policing: Introduction

Brian Hofer, CEO of Secure Justice and Chair of the City of Oakland's Privacy Advisory Commission, explains what community control over surveillance is and how the City of Oakland is using this approach to manage surveillance technologies. This is part of the panel 'Meet the experts on Surveillance and Digital Rights' organized by Smart City PDX on October 9, 2021.

Please watch the video. Then check out the optional resources in *Optional Resources to Dive Deeper* before moving on to *The CCOPS Model*.

Video: Community Control Over Policing: Oakland
https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=6a0e4970-e9c6-4554-a6ef-aed001415d13

Lecture: Optional Resources to Dive Deeper

These resources provide deeper background on U.S. privacy laws, surveillance technologies and local surveillance ordinances.

These are some excellent readings that provide broader context on U.S. privacy laws and surveillance technology ordinances:

- **Website:** Electronic Frontier Foundation: *Street Level Surveillance*. EFF's "Street-Level Surveillance" project shines light on the advanced surveillance technologies that law enforcement agencies routinely deploy in our communities. These resources are designed for members of the public, advocacy organizations, journalists, defense attorneys, and policymakers who often are not getting the straight story from police representatives or the vendors marketing this equipment.
- **PDF:** Samuelson Clinic Student White Paper, *Local Surveillance Ordinances*, (2021). This white paper outlines the history of surveillance technology oversight and compares multiple ordinances.
  ordinances and describes and compares their general features.
- **Website:** Council on Foreign Relations, *Reforming the U.S. Approach to Data Protection and Privacy,* (2011) This policy brief provides a nice overview and critique of the patchwork of sector-specific laws that the United States relies upon to protect data. It advocates for a single, comprehensive data protection law to protect individuals' privacy.
- **PDF:** Baker McKenzie, *Global Privacy Handbook* (Links to an external site.), United States overview (946-965). (Note: you must request access to the free pdf using this link (Links to an external site.). It can take up to 24 hours to receive a response). This reading provides a comprehensive survey of the data privacy and security legal landscape in the U.S. The U.S. has multiple data privacy and security laws at the federal and state levels, but it has not yet passed a comprehensive consumer data privacy law at the federal level. Several states, including most prominently, California, have enacted broad-based privacy laws as well as privacy laws regulating specific issues such as the Illinois Biometric Privacy Act.
- **PDF:** *An Overview of Privacy LawDownload An Overview of Privacy Law,* pp. 1-15 (Ch. 1 in IAPP Privacy Law Fundamentals Sample). This chapter provides a nice introduction to the field and a brief history of the major legal developments.
- **Website:** Complete Guide to Privacy Laws in the US (Links to an external site.). This provides a tour of US privacy laws.
- **PDF:** Steven Chabinsky and Paul Pittman, *USA: Data Protection Laws and Regulations 2020*, (Links to an external site.) (2020). This article summarizes the complex set of federal and state data privacy laws in the U.S. using the terminology developed in Europe and commonly used in privacy laws and regulations in other countries as well as newer U.S. state laws. We will refer back to key sections in later modules.

Please take some time to familiarize yourself with the following resources that you will find useful throughout the course:

1. The International Association of Privacy Professionals (IAPP) is the leading privacy organization in the world. Please review and periodically visit the IAPP's News Section (Links to an external site.) and Resources Section (Links to an external site.) for updated information about this field.
2. Familiarize yourself with the IAPP GLOSSARY OF PRIVACY TERMS (Links to an external site.). Please refer to this throughout the course for definitions of the terms you encounter. You also can print PDFs and create your own flashcards to review for the assessments.
3. Professor Daniel Solove's Information Privacy Law Website (Links to an external site.) contains a wealth of information and links to resources on substantive privacy law as well as careers in the field.

Section 3: Surveillance Technologies Overview

Lecture: Street Level Surveillance

Read the Electronic Frontier Foundation's description of Automated License Plate Readers and skim the other technologies described in the "Street Level Surveillance" website linked in the external resource.

EFF's "Street-Level Surveillance" project shines light on the advanced surveillance technologies that law enforcement agencies routinely deploy in our communities. These resources are designed for members of the public, advocacy organizations, journalists, defense attorneys, and policymakers who often are not getting the straight story from police representatives or the vendors marketing this equipment.

After you read this article, please take the Street Level Surveillance Quiz before moving on to Police Surveillance.

Article: EFF, "Street Level Surveillance"

https://www.eff.org/issues/street-level-surveillance

QUIZ

Which of the following is true about Cell-site simulators?

a. It is difficult for most people to know whether or not their phone's signals have been accessed by an active cell-site simulators
b. Data collected by cell-site simulators can reveal intensely personal information about anyone who carries a phone, whether or not they have ever been suspected of a crime
c. Can gather information from up to 10,000 phones at a time in private spaces such as homes or doctor's offices
d. All of the above

Some privacy concerns about iris recognition (iris scanning) include:

a. Data can be collected from a distance without a person's knowledge or consent
b. If a database containing a person's biometric scan is compromised, a person can't simply get new eyes to address this breach
c. Biometric data from iris scans are often collected and stored by third party vendors
d. All of the above are true
e. A and b only

Which of the following is true about body worn cameras?

a. Typically includes a time and date stamp and GPS coordinates
b. Typically includes audio and video
c. In some areas, police are given discretion over when to turn on body-worn cameras
d. All of the above
e. A and b only

Which of the following are privacy and equity concerns regarding body worn cameras?

a. Often, police can immediately access video recordings, but the recorded civilians (and their attorneys) cannot
b. Video and audio records may capture footage of children or people in various states of undress
c. May be used to surveil people engaging in protected speech
d. All of the above
e. A and c only

Which of the following is true about Acoustic Gunshot Detection?

a. Has a 100% accuracy rate of correctly identifying a gunshot in a geographic area
b. This technology is unable to detect human voices
c. Often placed in what police consider to be high-crime areas which can result in excessive scrutiny of the neighborhoods where people of color may live
d. All of the above are true

Lecture: Police Surveillance

Watch *Civilian Oversight of Police Technology* linked below (watch at least from 8:00 to 41:00; the rest is also useful as background):

As law enforcement applications of cutting-edge surveillance technology grow, police oversight agencies must keep pace with the practical implications of an array of sophisticated hardware & software tools that raise questions about the balance of privacy and public safety.

Many forms of police surveillance technology collect information on individuals regardless of whether they've committed a crime, and can make mistakes that negatively impact innocent people. An agency's use of this technology can be shrouded in secrecy. Surveillance information can be misused by unethical personnel and is vulnerable to breaches by malicious external actors.

On February 23, 2021 NACOLE welcomed Dave Maass for a technical overview of surveillance technology such as drones, license plate readers, facial recognition, and cell site simulators (Stingrays) and a discussion of how police agencies around the U.S. are using this technology and how to use by individual agencies is documented through records such as usage logs.

After you watch the video, please take the *Police Surveillance* Quiz before moving on to *Interactive Surveillance Technology Tools.*

Video: Civilian Oversight of Police Surveillance Technology
https://www.nacole.org/civilian_oversight_of_police_surveillance_technology_recording

QUIZ

What does the acronym *EFF* stand for?

a. Extended Financing Facility
b. Experimental Forecast Facility
c. Electronic Frontier Foundation
d. Enhanced Formation Flying

What is another name for Community Control Over Police Surveillance (CCOPS)?

a. Surveillance Equipment Regulation Ordinance (SERO)
b. Automatic License Plate Readers (ALPR)
c. Real-Time Crime Information Center
d. Civilian Oversight

What was the first county to adopt CCOPS laws?

a. Miami-Dade County
b. Santa Clara County
c. Cuyahoga County
d. Bronx County

What are common problems with surveillance?

a. Mass Surveillance
b. Disproportionate Policing
c. Waste of Public Funds
d. All of the Above

Lecture: Interactive Surveillance Technology Tools

Use each of the EFF's three interactive surveillance technology tools linked below:

(i) The Atlas of Surveillance: The Atlas of Surveillance is a database and map that will help you understand the magnitude of surveillance at the national level, as well as what kind of technology is used locally where you live.

(ii) Who has your face?: Half of all adults in the United States likely have their image in a law enforcement facial recognition database, according to a 2016 report from the Center on Privacy & Technology at Georgetown Law. Today, that number is probably higher. But what about your face?

(ii) Spot the Surveillance: If you drove past an automated license plate reader, would you know what it looks like? Ever look closely at the electronic devices carried by police officers? Most of the time, people might not even notice when they've walked into the frame of surveillance technology. Spot the Surveillance is a virtual reality experience where you will learn how to identify local law enforcement agencies' surveillance technology.

Use the interactive tools before moving on to Tracking Data.

Article: Atlas of Surveillance
https://atlasofsurveillance.org/

Article: Who has your face?
https://whohasyourface.org/

Article: Spot the Surveillance
https://www.eff.org/pages/spot-surveillance-vr-experience-keeping-eye-big-brother

Lecture: Tracking Data

Watch Ashkan Soltani, "Your Data and Who Has Access to It": "I [Ashkan Soltani] collaborated with NPR and the Center for Investigative Reporting to develop this script describing who is tracking you throughout your day. The video shows how your digital trail can be assembled into a pretty complete picture of who you are. Some of the script may seem pretty far fetched, but every example was vetted by yours truly and occurs every day (in the US)." (4:40)

Watch this video before moving on to Surveillance Meets the Internet of Things.

Video: Your Data and Who Has Access to It
https://www.youtube.com/watch?v=bqWuioPHhz0&t=233s

Lecture: Surveillance Meets the Internet of Things

Read Angel Diaz, *When Police Surveillance Meets the 'Internet of Things'* linked below. Doorbell cameras, smart thermostats, digital assistants, and other always-on devices open up a whole new world of privacy risks when the government has access to their data.

Read the linked article before moving on to *Racial Equity and Data Privacy.*

Article: When Police Surveillance Meets the 'Internet of Things'

https://www.brennancenter.org/our-work/research-reports/when-police-surveillance-meets-internet-things

Lecture: Racial Equity and Data Privacy

Listen to (or read the transcript of) the *Race and Regulation Podcast: Episode 5: Racial Equity and Data Privacy* (34:37) linked below.

Listen to or read the transcript before taking the *Race and Regulation* Quiz.

Audio: Racial Equity and Data Privacy

https://pennreg.org/episode-5/

QUIZ

According to Dr. Allen, privacy related racial injustice includes which of the following:

a. Discriminatory forms of surveillance
b. Exclusion of Black people
c. Predation of Black Americans
d. All of the Above

Using social media facial recognition technology to identify peaceful protestors labeled as "Black identity extremists" is an example of

a. Discriminatory forms of surveillance
b. Exclusion of Black people
c. Both a and b
d. None of the Above

Facebook allowed advertisers to choose, by race, which Facebook users could and could not see their advertisements. This is an example of

a. Discriminatory forms of surveillance
b. Exclusion of Black people
c. Predation of Black Americans
d. None of the Above

To solve the panopticon problem, Dr. Allen suggests:

a. An end to all surveillance
b. Racially attuned decision making about surveillance
c. Legislative reform
d. B and C only

Section 4: Analyzing Privacy & Equity Impacts of Technology

Lecture: Smart Decisions About Surveillance

Watch *Making Smart Decisions About Surveillance.* This video identifies the costs and consequences of surveillance, identifies steps for evaluating the risks of surveillance technologies and how to ensure accountability for use policies related to those technologies.

Watch this video before taking the *Smart Decisions About Surveillance* Quiz.

Video: Making Smart Decisions About Surveillance

https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=1b8a9f6b-6fd4-4d09-902a-af02011765af

QUIZ

What financial risks does surveillance pose?

a. Litigation
b. Data Breach
c. A + B
d. None of the Above

What does the acronym *"ECPA"* stand for?

a. Energy and Climate Partnership of the Americas
b. Early Career Policy Ambassadors
c. Electronics Communications Privacy Act
d. European Community Psychology Association

What is a surveillance impact report?

a. Report detailing the costs and benefits of surveillance technology
b. Report provided by government detailing issues with technology
c. Report received from public detailing approval of technology
d. Internal audit after surveillance technology is approved

What is a necessary element of a surveillance use policy?

a. Input from public
b. Input from government oversight agency
c. Suggestions from industry leaders
d. Access control measures

What are some of the considerations before a surveillance technology proposal is accepted?

a. Transparency
b. Accountability
c. Oversight
d. All of the Above

Lecture: Community Transparency, Accountability & Oversight

Read ACLU, Northern California, *Making Smart Decisions About Surveillance: A Guide for Community Transparency, Accountability & Oversight* linked below. Download this guide that provides a step-by-step framework to approach surveillance proposals, properly evaluate their true costs, and develop policies that provide transparency, oversight, and accountability. It also includes dozens of case studies highlighting smart approaches and missteps to avoid. The guide concludes with model language for policymakers to adopt to make sure the right process is used every time a surveillance proposal is considered.

Read the linked article before moving on to *Privacy Impact Assessment.*

Article: Making Smart Decisions About Surveillance: A Guide for Community Transparency, Accountability & Oversight
https://www.aclunc.org/publications/making-smart-decisions-about-surveillance-guide-community-transparency-accountability

Lecture: Privacy Impact Assessment

Read/Watch G20 Global Smart Cities Alliance Privacy Impact Assessment. Work through this website's explanation of how Privacy Impact Assessment (PIA) policies can help cities establish a consistent method for identifying, evaluating, and addressing privacy risks. Watch the first short video and read the entire website. Feel free to watch the longer video for more a extensive background.

Article: Global Policy Roadmap for Successful, Ethical, Smart Cities
https://www.globalsmartcitiesalliance.org/home

Section 5: The City of Oakland Privacy Advisory Commission: Evaluating ALPRs

Lecture: Oakland Privacy Advisory Commission (OPAC)

Read City of Oakland Privacy Advisory Commission (OPAC) "About". This website summarizes the history of the Commission and its duties.

Read City of Oakland Founding Ordinance and Bylaws. These documents establish the Committee and provide the authority for OPAC's work.

Watch *Oakland ALPR Intro & SIR Part 1* (14:40) and *Oakland ALPR SIR Part 2* (11:07) . These videos introduce the Surveillance Impact Report (SIR) process and walk through the still-draft SIR OPAC drafted for Automated License Plate Readers (ALPRs).

Article: About City of Oakland Privacy Advisory Commission (OPAC)
https://www.oaklandca.gov/boards-commissions/privacy-advisory-board#page-about

Article: City of OPAC Founding Ordinance and Bylaws

https://www.oaklandca.gov/documents/bylaws-and-establishing-ordinance

Video: Oakland ALPR Intro & SIR Part 1
https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=4ddbbd09-b3dd-4ac2-85a9-af0e00e56270

Video: Oakland ALPR SIR Part 2
https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=de705c9e-ad8d-4f83-bf49-af0e00e56261

Lecture: Oakland ALPR Use Policy

Watch *Oakland ALPR Use Policy* (12:08). This video walks through the Commission's draft Use Policy for ALPRs.

Video: Oakland ALPR Use Policy

https://csuohio.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=b4e65768-44a8-40ab-8553-af0e00e83c4a

QUIZ

Prior to possibly detaining the vehicle after an ALPR “hit”, what must a patrol officer do?

a. Confirm the accuracy of the license plate numbers
b. Confirm that the make, model, and color matches the description
c. Confirm whether the alert pertains to the car or the driver
d. All of the above

What sorts of data errors might arise from ALPR use and lead to misidentification?

a. Inaccurate plate scan
b. Plate placed erroneously on hotlist
c. Stolen plates placed on another vehicle
d. All of the above

What mitigating steps did Oakland take to lessen the potential privacy impact and civil Liberties concern?

a. Restricted use to just lieutenants
b. Only allowed to receive data from ICE
c. Shorter retention period for data
d. District Attorney must verify each “alert”

How many members serve on the Privacy Advisory Commission?

a. Nine
b. Seven
c. Six

d. Eight

Lecture: Oakland ALPR One-Year Report

Watch Oakland ALPR One-Year Report. This video explains how the Oakland Privacy Commission conducts follow-up analyses of existing use policies and uses the ALPR policy as an example to illustrate the benefits and challenges of the process.

Lecture: Additional Resources

- G20 Global Smart Cities Alliance Website. Established in June 2019, the G20 Global Smart Cities Alliance on Technology Governance unites local and national governments, private-sector partners and city residents around a shared set of principles for the responsible and ethical use of smart city technologies. The Alliance establishes and advances global policy norms to help accelerate best practices, mitigate potential risks, and foster greater openness and public trust. The World Economic Forum serves as the secretariat for the Alliance.
- DHS Privacy Impact Assessments. The Department of Homeland Security (DHS) maintains a public website with all of the privacy impact assessments it has conducted.
- CNIL DPIA resource. The Commission Nationale de l'Informatique et des Libertés (CNIL) is the French Data Protection Agency. CNIL created the linked documents as a set of good practices aiming to address the privacy risks and impact on the protection of personal data that processing can result in.
- UK ICO Video Surveillance Guidance. The Information Commissioner's Office (ICO) is the UK's data protection agency. This website provides guidance for public agency's to evaluate the use of video surveillance.

Article: FPF PIA for G20

https://www.globalsmartcitiesalliance.org/home

Article: CNIL DPIA Resource

https://www.cnil.fr/en/PIA-privacy-impact-assessment-en

Article: UK ICO ANPR DPIA

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079855/ANPR__DPIA_V3.0_approved.pdf