



# Technology & Innovation Ad Hoc Committee

## Facial Recognition Technology Research

September 22, 2021

# Facial Recognition Technology Research

## Agenda

- Research Focus: *FRT Best Practices*
  - Georgetown Law
  - IJIS Institute & IACP
  - National League of Cities
- Research Focus: *FRT Transparency Best Practices & Case Study*
- Questions/Discussion
- References

# Research Focus: FRT Best Practices

- **Georgetown Law's Center on Privacy & Technology** published a comprehensive study, the *Perpetual Line-Up*, on facial recognition technology in 2016 that included 30 recommendations tailored by stakeholder group.
- The Law Enforcement Imaging Technology Task Force, a joint effort of the **IJIS Institute and the International Association of Chiefs of Police**, released a Facial Recognition Use Case Catalog in 2019 that also includes four core recommendations.
- **The National League of Cities** published a Facial Recognition report in 2021 to help guide cities, which includes analysis of FRT, use cases, benefits and risks, regulatory approaches, and five core recommendations.

# Georgetown Law: FRT Best Practices

With one in two U.S. adults in a law enforcement FRT network—a perpetual line-up—yet with very little known publicly about these systems or guaranteed protections for privacy and civil liberties, Georgetown sought to close these gaps with a one-year investigation that included over 100 records requests and interviews to police departments nationwide; an overview of the report follows:

- Executive Summary & Background
- Risk Factors & Framework (*optional: see Q&A slide 10*)
- Findings & Scorecard
  - Deployment; 4<sup>th</sup> Amendment; Free Speech; Accuracy; Racial Bias; Transparency & Accountability (includes Los Angeles County scorecard)
- **Recommendations**

# Georgetown Law: FRT Best Practices

Recommendations directed to legislatures offers relevant best practices (1/4):

- Use individualized suspicion of criminal conduct for FRT searches
  - A reasonable suspicion standard should apply to all Stop and Identify, Arrest and Identify, and Investigate and Identify searches run on mug shot databases
- Exclude people who were found innocent or who have had charges against them dropped or dismissed from Mug shot databases that are used for FRT searches
  - Recommends following the lead of Michigan that requires the destruction of biometric data who were arrested but have been found innocent, or who have had charges against them dropped or dismissed
    - “A single act of peaceful civil disobedience should not result in a lifetime in a criminal face recognition database”

# Georgetown Law: FRT Best Practices

Recommendations directed to legislatures offers relevant best practices (2/4):

- A court order issued based on probable cause should be done prior to searches of driver's license and ID photos
- Limit searches of license photos to investigations of serious offenses
  - In an Investigate and Identify search, where a suspect is identified after the commission of the offense from a video still or surreptitious photograph, consider the following:
    - In this case, there is a risk that some officials may use a minor offense such as jaywalking as a pretext to justify a search to identify a peaceful protestor
    - Thus, police should limit Investigate and Identify searches—even when they are limited to mug shot databases—to investigations of felonies

# Georgetown Law: FRT Best Practices

Recommendations directed to legislatures offers relevant best practices (3/4):

- Real-time video surveillance should only occur in life-threatening public emergencies under a court order backed by probable cause
  - Real-time, continuous face recognition from street public surveillance footage or potential police-worn body cameras would enable police to secretly locate people and track their movements
- Prohibit use of FRT *by statute* to track down people on the basis of their race, ethnicity, religious or political views
  - Without such prohibitions, the danger exists that FRT could chill free speech or endanger access to education or public health

# Georgetown Law: FRT Best Practices

Recommendations directed to legislatures offers relevant best practices (4/4):

- Create public reporting requirements and rigorous internal audits for all police use of FRT, including:
  - The number of FRT searches run
  - The nature of those searches by type of deployment:
    - Stop & Identify; Arrest & Identify; Investigate and Identify (*optional: see Q&A slide 10 for more*)
  - The crimes that those searches were used to investigate
  - The arrests and convictions that resulted from those searches
  - The databases that those searches accessed
  - Any other information that the jurisdiction deems appropriate



# Georgetown Law: FRT Best Practices

Recommendations for state & local law enforcement largely build from the recommendations directed to legislatures:

- Impose a moratorium on face recognition searches of state driver's license and ID photos until state legislatures regulate that access
- Adopt and make public FRT use policies that have received elected or legislative review and approval
- Use contracts and the contracting process to maximize accuracy
- Implement internal audits, tests for accuracy and racial bias, and the use of trained face examiners

## Georgetown Law: FRT Best Practices – Q&A

### ***Q&A: How do police best assess, categorize and report the nature of FRT searches?***

Answer: Georgetown developed a risk framework that helps police departments assess, categorize and calculate the risk of various FRT searches by the most common types of deployments:

1. Stop and Identify
2. Arrest and Identify
3. Investigate and Identify

DEPLOYMENT		LESS RISK	MORE RISK
MODERATE RISK	Stop and Identify (Mug shot Database)	<ul style="list-style-type: none"><li>• Targeted Search</li><li>• Targeted Database</li><li>• Transparent</li></ul>	<ul style="list-style-type: none"><li>• Real-Time</li><li>• Novel Use</li></ul>
	Arrest and Identify (Mug shot Database)	<ul style="list-style-type: none"><li>• Targeted Search</li><li>• Targeted Database</li><li>• Established Use</li></ul>	<ul style="list-style-type: none"><li>• Invisible</li></ul>
	Investigate and Identify (Mug shot Database)	<ul style="list-style-type: none"><li>• Targeted Search</li><li>• Targeted Database</li><li>• After-the-Fact</li><li>• Established Use</li></ul>	<ul style="list-style-type: none"><li>• Invisible</li></ul>

# IJIS Institute & IACP: FRT Best Practices

The Task Force's catalog provides numerous use cases of facial recognition, then promotes FRT's use in policing through implementation of its recommendations:

- Recommendation #1: Fully inform the Public
  - "Law enforcement should endeavor to completely engage in public dialogue regarding purpose-driven facial recognition use, including how it operates, when and how images are taken and retained, and the situations in which it is used."
- Recommendation #2: Establish Use Parameters
  - "Appropriate systems use conditions, even preliminary ones, must be established as soon as possible to engender public confidence in its use and avoid any further proliferation of mistrust."

# IJIS Institute & IACP: FRT Best Practices

- Recommendation #3: Publicize its Effectiveness
  - “All public agencies should widely publish facial recognition success stories to heighten overall awareness of its usefulness, especially those cases in which suspects are exonerated, or where facial recognition is used to protect vulnerable persons.”
- Recommendation #4: Create Best Practice Principles and Policies
  - “Model law enforcement facial recognition guidance and regulation documents should be immediately established and broadly adopted, to include training benchmarks, privacy standards, human examiner requirements, and anti-bias safeguards.”
  - “Initial training and periodic re-training certifications are required as part of most law enforcement technologies, and facial recognition seems to need such best practice standards to ensure both the courts and the public have confidence in its consistent, fair use.”

# National League of Cities: FRT Best Practices

Acknowledging the sensitive nature of FRT due to its imperfections and how it's frequently implemented behind closed doors, NLC offers five recommendations for cities to better facilitate FRT discussions publicly in their communities:

1. Engage with residents to develop policies, and be transparent about FRT use
  - Actions include: requiring vote on FRT by elected officials before use; insisting on community input through public forums prior to FRT vote; collaborating with a diverse group of non-governmental organizations when deciding FRT policy; establishing a citizen overview board with real authority and budget; making FRT use policies public
2. Establish a training program for law enforcement and other users of FRT
  - Actions include: requiring implicit bias training; requiring double-blind confirmation before match determined; forbidding officers from using police sketches or celebrity doppelganger photos in lieu of real photos

# National League of Cities: FRT Best Practices

## 3. Limit the scope of FRT use to reduce the risk of misidentifications and privacy violations

- Actions include: limiting use of FRT to investigations of violent offenses; limiting the use of real-time public surveillance to a narrow set of situations and ensure law enforcement obtains warrant based on probable cause; considering pros and cons of using either mug shot photos or driver's license photos for the source of FRT database

## 4. Institute rigorous standards for data storage and cybersecurity to protect citizens' biometric data

- Actions include: regularly scrubbing databases of mug shot photos to exclude people found innocent or against whom chargers were dropped; deleting any photo or video footage analyzed with FRT but not pertinent to an ongoing investigation; restricting the length of time that data is stored to reduce the risk of a data breach

# National League of Cities: FRT Best Practices

5. Follow best practices for drafting contracts to ensure accuracy & reduce legal risk
  - Actions include: requiring contracts with FRT vendors to regularly test their algorithms for both accuracy and racial bias; requiring vendors to certify that their algorithms use a demographically representative training set and are updated regularly; removing contract language in which vendors disclaim responsibility for the facial recognition's algorithm's accuracy; paying close attention to the wording of FRT contracts' indemnification clauses to ensure cities do not adopt too much liability for vendors' errors

# Research Focus: FRT Transparency Case Study

- *The city of Oakland and 20 other jurisdictions, including BART, have implemented by ordinance a surveillance technology vetting framework for FRT and other surveillance technologies that provides for ongoing oversight via impact reports, use policies, and annual reporting.*



# FRT Transparency Best Practices: Initial Process

As first debuted in Oakland, for each piece of surveillance technology, the relevant department must provide for public review and input on an **Impact Review** and a proposed **Use Policy**—a process that requires a mindfulness in thinking about and researching the potential impact from use of a technology before its implementation

- **Impact Review:** During the analysis of the technology, any privacy, civil liberties/civil rights, racial bias, and/or accuracy concerns are identified
- **Proposed Use Policy:** Any concerns identified in the impact review process are specifically addressed and/or mitigated

# FRT Transparency Best Practices: Approval & Review Process

After public review and input, the department submits its **Impact Review** and a proposed **Use Policy** for approval by relevant elected body and/or civilian board

- If the technology use policy is approved, then the vetting framework ordinance requires an ongoing annual report for that specific technology

The **annual review** requires the department to demonstrate how the technology has been used, whether public safety goals are being met, how much it has cost the taxpayer, and the results of audits; including answering two key questions:

- Does the technology work in a cost-effective manner at achieving the purported goals?
- Do the benefits of using this technology according to its (proposed) use policy outweigh the potential costs to civil liberties and the taxpayer?

# FRT Transparency Case Study: Results & Feedback

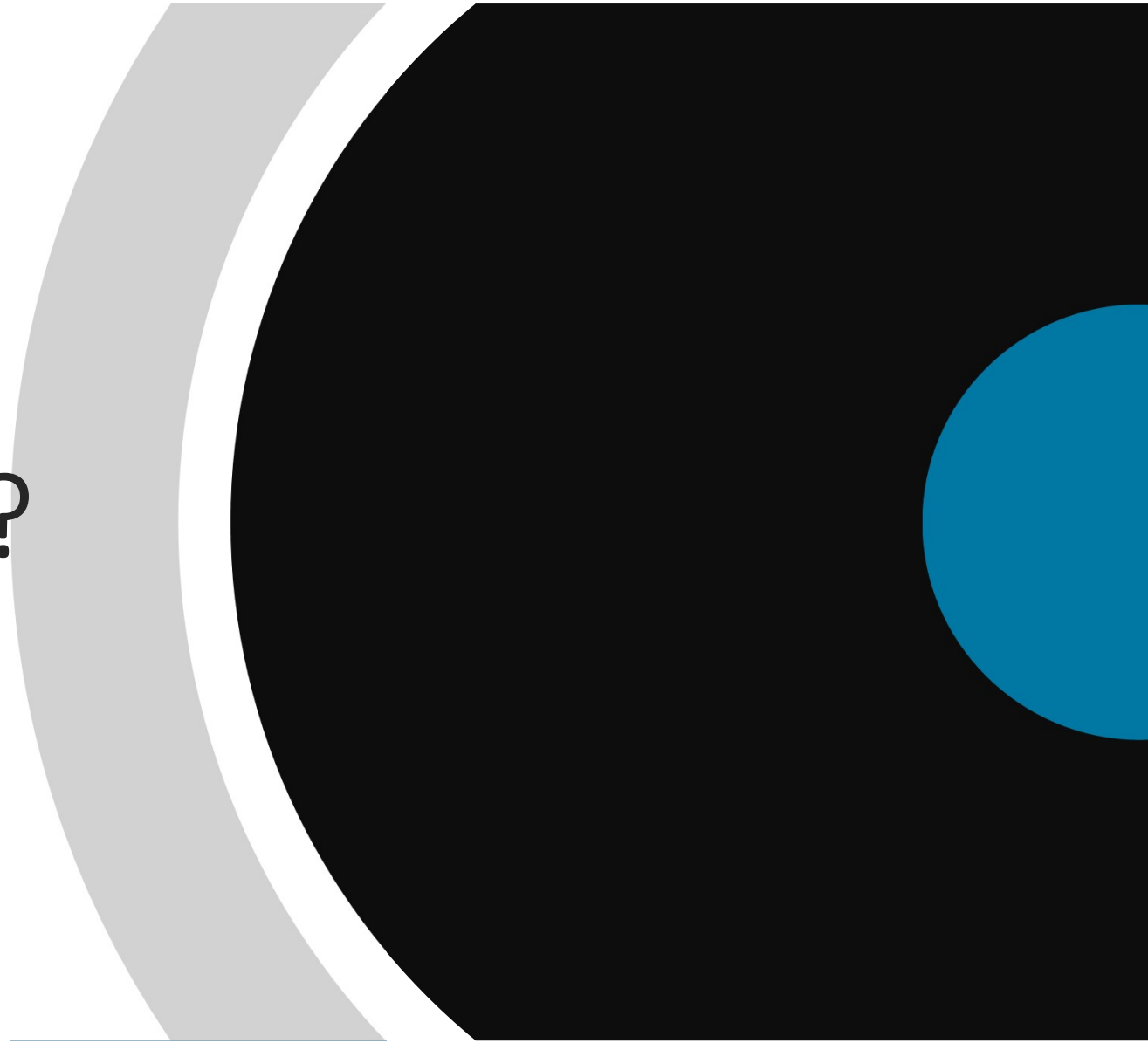
For BART's first cycle of annual reporting of seven technologies under this surveillance technology vetting framework ordinance, staff from relevant departments collectively rated the administrative burden in producing these reports as a "4" (scale of 1 to 10)

- Further, staff estimated they collectively spent 100 hours on these seven annual reports, which included building new processes and templates for first-time reports

An external organization, Secure Justice, rated BART's annual reporting under this ordinance as an "A" and said it was leading the way in exemplifying transparency

- This group found that BART supplied sufficient specificity and information that the public should have confidence that its use of surveillance technologies "appears responsible, that certain technology is proven to be effective, and where other technologies have not met the standard, BART is ceasing such use so as not to cause taxpayers an undue burden or negatively impact civil liberties"

Questions?



# References

City of Oakland. (2021, January 21). *Approved Impact Reports and Use Policies*. City of Oakland. <https://www.oaklandca.gov/topics/approved-impact-reports-and-use-policies>

Garvie, C., Bedoya, A., & Frankle, J. (2016a). *The Perpetual Line-Up*. Perpetual Line Up. Georgetown Law. <https://www.perpetuallineup.org/>

Hofer, B. (2021b, January 10). *BART Gets An “A” For Annual Reporting*. Secure Justice. <https://secure-justice.org/blog/bart-gets-an-a-for-annual-reporting>

IJIS Institute & International Association of Chiefs of Police. (2019, March). *Law Enforcement Facial Recognition Use Case Catalog*. IACOP. [https://www.theiacp.org/sites/default/files/2019-10/IJIS\\_IACP%20WP\\_LEITTF\\_Facial%20Recognition%20UseCasesRpt\\_20190322.pdf](https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf)

National League of Cities. (2021, April). *Facial Recognition Report*. <https://www.nlc.org/wp-content/uploads/2021/04/NLC-Facial-Recognition-Report.pdf>

Oakland City Council Ordinance, Municipal Code Chapter 9.64, which regulates the City’s acquisition and use of surveillance technology, 2018, <https://bit.ly/3fOukeJ>

*Surveillance Technology Reports*. Bay Area Rapid Transit. <https://www.bart.gov/about/reports/surveillance>