

Privacy, Local Governments, & Facial Recognition Technologies

Kelsey Finch, Senior Counsel

April 2021



Future of Privacy Forum

The Supporters

150+

Companies

25+

Leading
Academics

15+

Advocates and
Civil Society

5

Foundations

The Mission

Bridging the policymaker-industry-academic gap in privacy policy
Developing privacy protections, ethical norms, & responsible business practices

The Workstreams

AI & Ethics

Student Data

Ad Tech & IOT

Mobility & Location

Privacy-Enhancing Technologies


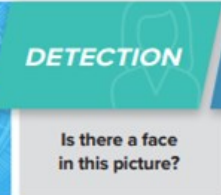
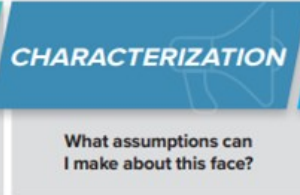
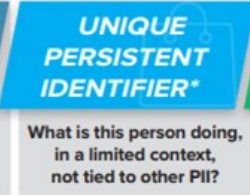
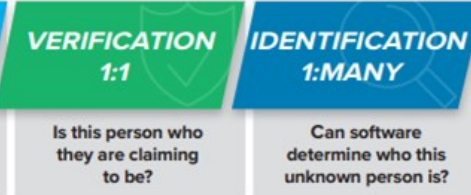
Smart Cities & Communities

Understanding Facial Detection, Characterization and Recognition Technologies

Produced by



March 2018

	 DETECTION	 CHARACTERIZATION	 UNIQUE PERSISTENT IDENTIFIER*	 VERIFICATION 1:1	 IDENTIFICATION 1:MANY
	Is there a face in this picture?	What assumptions can I make about this face?	What is this person doing, in a limited context, not tied to other PII?	Is this person who they are claiming to be?	Can software determine who this unknown person is?
IDENTIFIABILITY	» Not identifiable	» Not identifiable ³	» Potentially identifiable if linked to other data	» Identifiable	» Identifiable
PRIVACY CONCERNS	» None ³	» Possibility of discrimination based on gender, race, and/or other characteristics » Perception of poor accuracy, with associated mislabeling or categorization » Perception of possible identification without consent ⁴	» Possible identification without consent » Surreptitious tracking » Detailed profiling could allow for exploitation » Misalignment with consumer expectations through use of databases never expected/intended to be used for facial identification purposes	» Security breach leading to loss of PII or account access information » Possibility of false positive and false negative rates; either unduly burdening authorized users, or insufficiently preventing unauthorized access » Out of context use	» "FindFace" – apps that claim to identify unknown persons in public without additional info from the app user » Possibility of user tracking or profiling across contexts » Possibility of false matches, resulting in false suspicions or accusations » Unexpected use/sharing

Policy Approaches by Local Governments

- **Prohibitions on FRT**

- Largely focused on police and government use (PDX includes private use)
- Several in tandem with a surveillance ordinance
- ~ 17 across the U.S.

- **Surveillance ordinances**

- Technology-neutral frameworks for ex ante privacy review, focused on government use
- ~ 19 across the U.S. (plus some pending)

- **Data governance and privacy programs**

- Internal, technology-neutral, policies and procedures for government use of data
- ~ dozens across the U.S. (various levels of maturity)

- **Advisory groups, task forces, and studies**

- May be either technology-specific or general purpose bodies
- Impact studies often commissioned at state level



Some Key Considerations

- **Public engagement and communications** - How to ensure the community's perspectives and priorities are included?
- **Appropriate exceptions, tailored to nature and sensitivity of data**
 - How to address differences between detection, characterization, persistent identifier, verification, and identification?
 - Context-specific considerations (public spaces, public buildings, online; a park, a stadium, a tollbooth, a courtroom; exigent vs. routine use, etc.)
- **Unintended consequences** - What about using facial biometrics for...
 - personal/work device logins and authentication; anti-fraud purposes; people counting; in art, sports, or other special venues; technology assistance for persons with disabilities; year books; etc.?
- **Accuracy** - Systems increasingly work effectively across all demographic groups, but that does not necessarily address civil rights/equities issues.
- **Scope of application** - How to address police use (specifically), government use (generally), or private use in public spaces? What about legacy systems?
- **Enforceability and implementation** - What resources would be available to implement and enforce restrictions on access and use? Impact assessments, training, policies, audits/annual reporting, transparency/accountability, etc.
- **State activity** - Are there complementary (or conflicting) efforts at the state level?

Questions?

@k_finch
kfinch@fpf.org

www.fpf.org
facebook.com/futureofprivacy
@futureofprivacy



Additional Resources

