

Video Analytics and Simple Obfuscation

Information Privacy with Applications
David Sidi (dsidi@email.arizona.edu)

toward our integrated session: obfuscation and
standoff biometry

Biometrics with computers

“Technical progress in image acquisition guarantees observability now; technical progress in standoff biometrics guarantees identifiability real soon now. Venture capitalists regularly hear new ideas in standoff biometry, and Moore’s law is its friend ...

Question: What is ‘observability,’ as used in the anonymity literature?
‘Identifiability?’



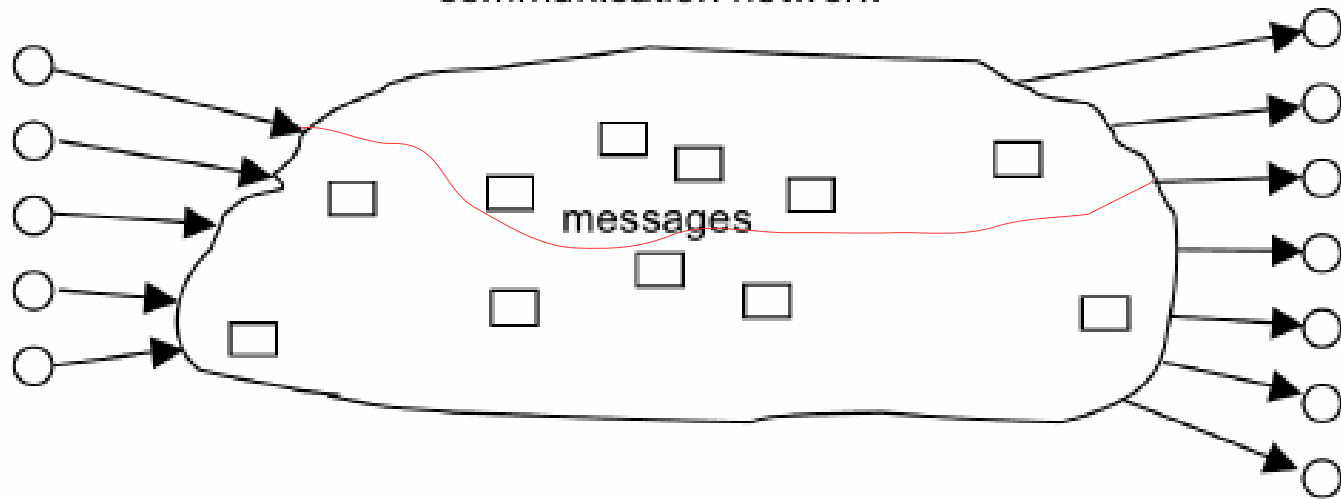
Identifiability and anonymity sets: definitions and their practical upshots

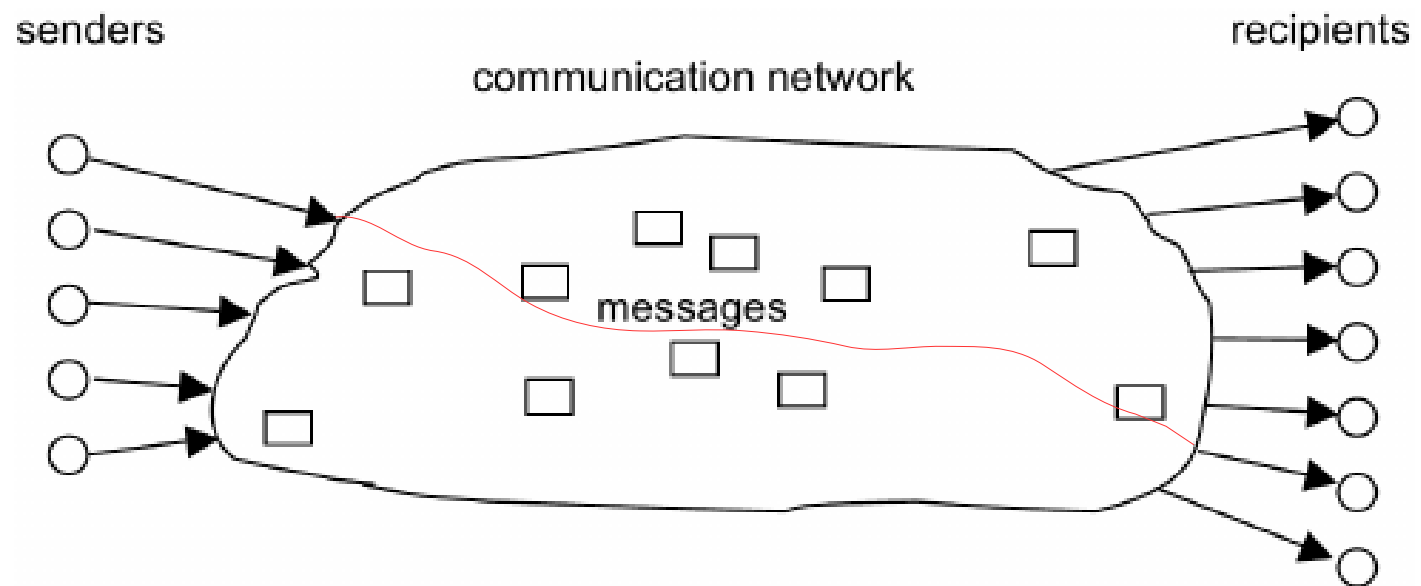
(we will return to this at the end of October)

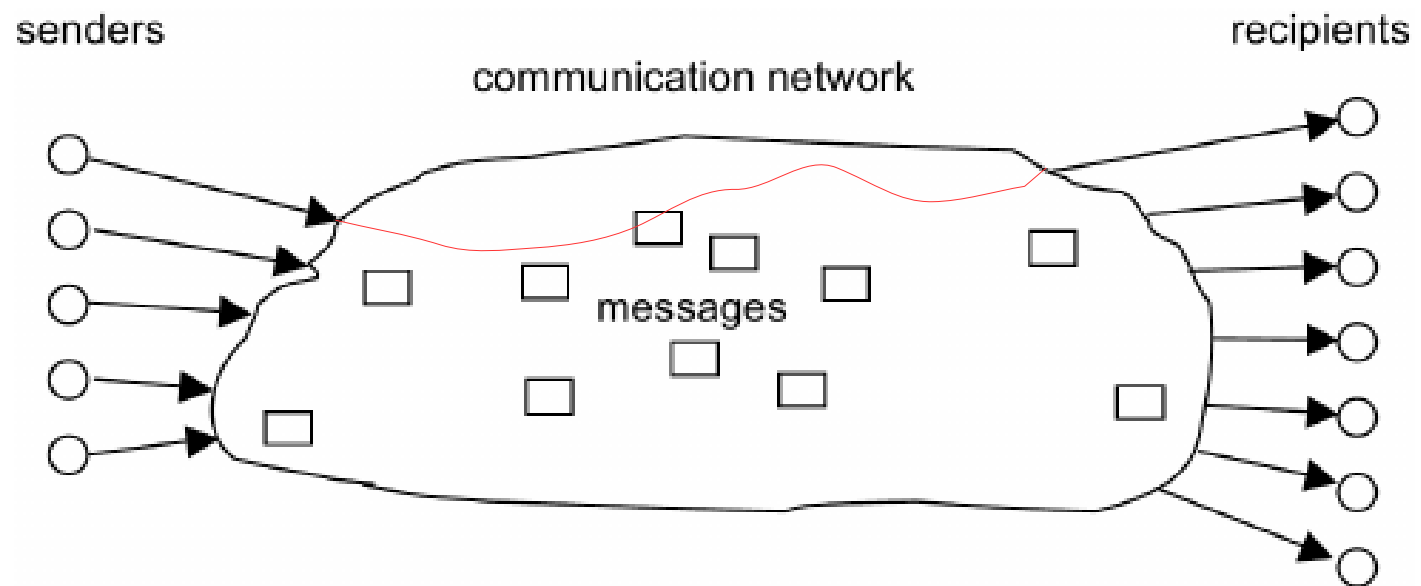
senders

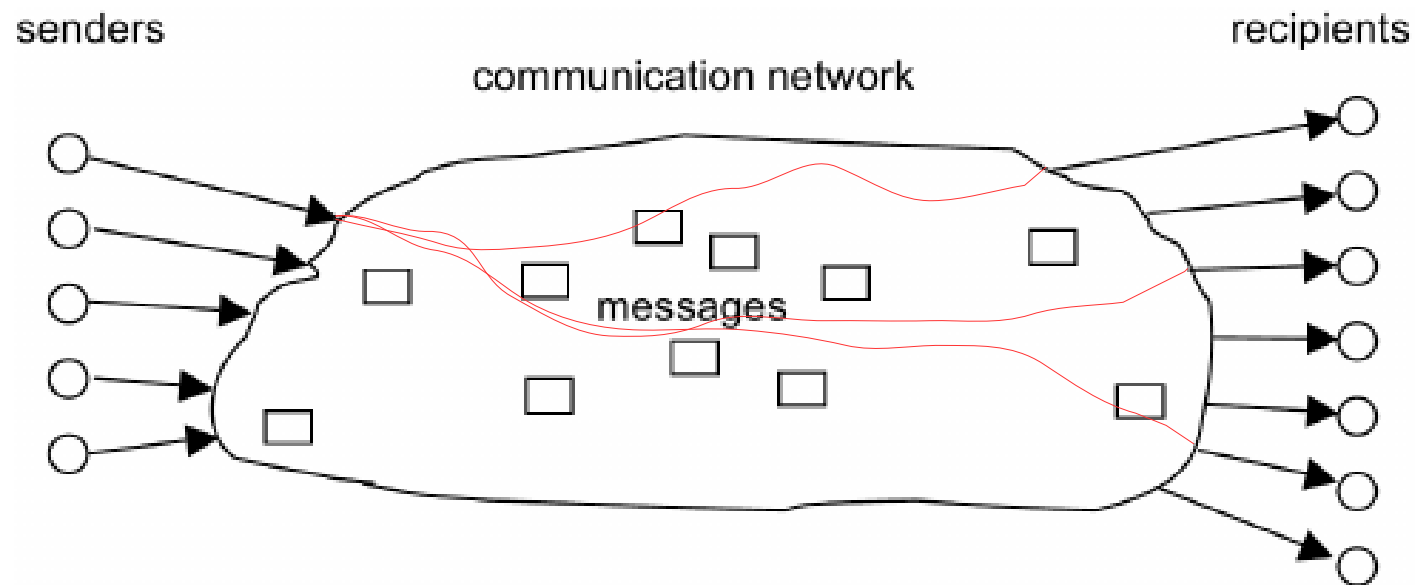
communication network

recipients









Biometrics with computers

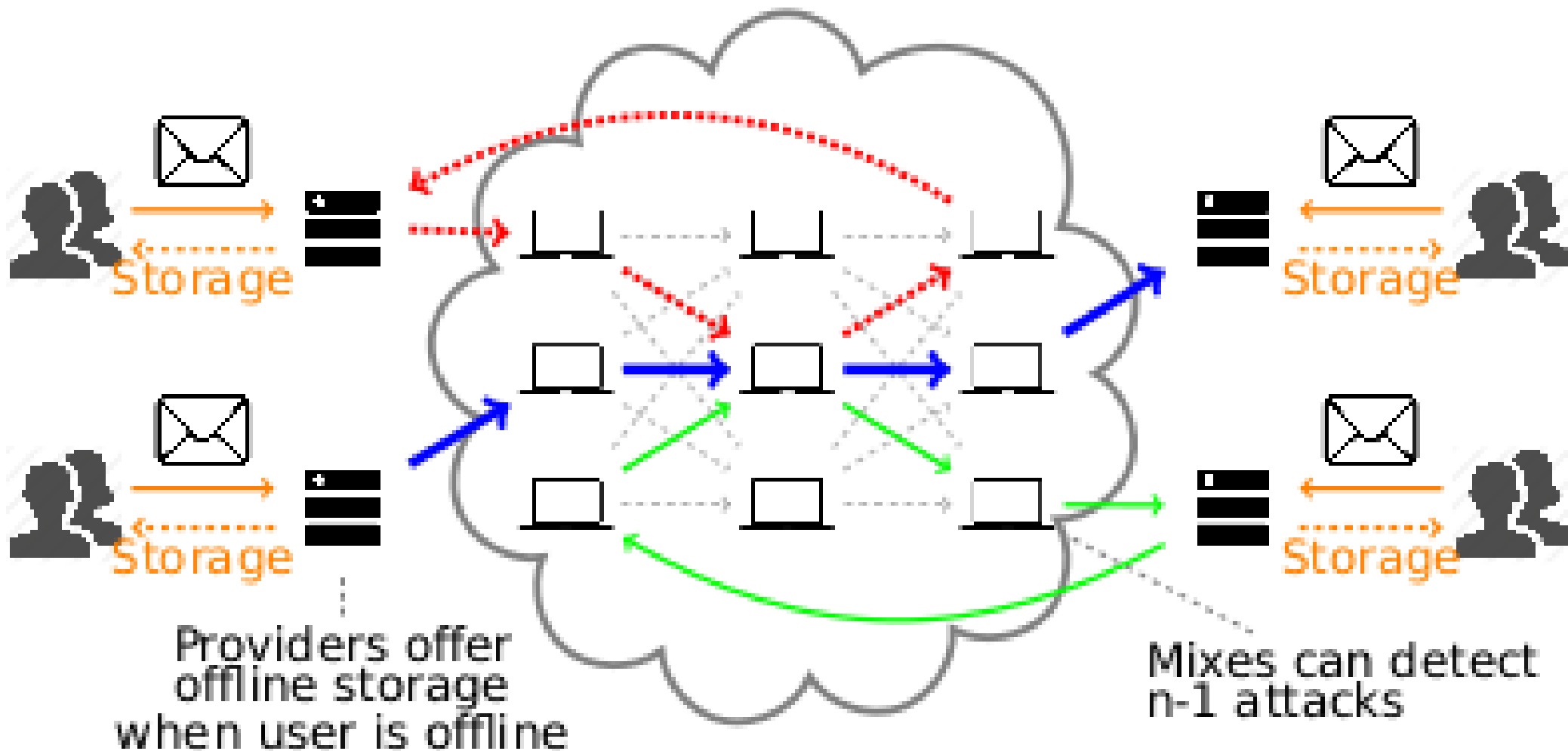
“Technical progress in image acquisition guarantees observability now; technical progress in standoff biometrics guarantees identifiability real soon now. Venture capitalists regularly hear new ideas in standoff biometry, and Moore’s law is its friend ...

Question: What is ‘observability,’ as used in the anonymity literature?
‘Identifiability?’



Reminder: obfuscation for unobservability in
Loopix

Users' loop cover traffic
generates traffic
in two directions



Biometrics with computers

“Technical progress in image acquisition guarantees observability now; technical progress in standoff biometrics guarantees identifiability real soon now. Venture capitalists regularly hear new ideas in standoff biometry, and Moore’s law is its friend ...

Question: What is ‘observability,’ as used in the anonymity literature?
‘Identifiability?’



“We will soon live in a society where identity is not an assertion (“Call me Dan”) but rather an observable (“Sensors say that’s Dan”). Your breath, the microwave emissions of your beating heart, the idiosyncratic anomalies of how you type, talk, and walk say who you are.”

Dan Geer, *Identity as Privacy*, in 2013

Question: How does what Geer is saying relate to what Doctorow said in our reading for the last integrated session



“Moore’s law is its friend We will soon live in a society where identity is not an assertion (“Call me Dan”) but rather an observable (“Sensors say that’s Dan”).”

Question: Which approach to privacy technology is favored when observability is unavoidable, and encryption is not an option (as for biometrics)? (think about our discussion last time)

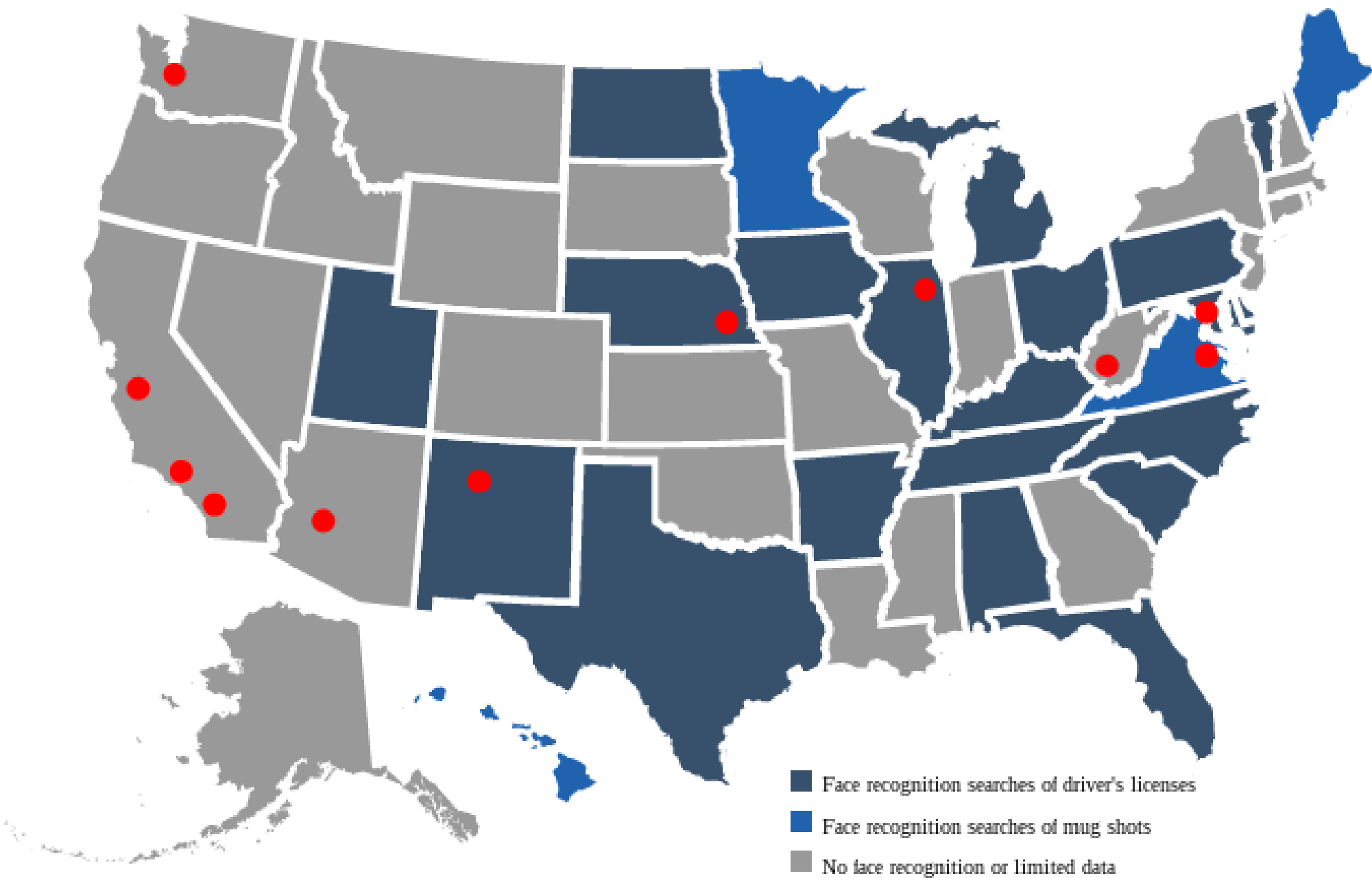


Figure 1: Law Enforcement Face Recognition Use By Jurisdiction

Click on state or city for more information

The logo features a large, stylized black outline of a face with a wide, open-mouthed smile. A thick red horizontal bar is positioned across the middle of the face, containing the text "FindFace" in a white, bold, italicized sans-serif font.

FindFace

Nest
Google Wallet Gmail
Slides
Google Analytics Books
Chromecast
Google+ Maps AdSense
Drive
Sheets Android
it's finally here Pixel
Google News ChromeOS
DNS Calendar Chrome Allo
PRISM Home Duo
Docs Google Wifi
YouTube Search DeepMind
Photos
Translate
Google Fiber
Keep

“In identity verification, the subject looks straight at the camera under controlled lighting conditions, and their face is compared with the one on file. A related but harder problem is found in forensics, where we may be trying to establish whether a suspect’s face fits a low-quality recording on a security video. The hardest of all is surveillance, where the goal may be to scan a moving crowd of people at an airport and try to pick out anyone who is on a list of perhaps a few hundred known suspects.” (Biometrics, 265)