

Lecture 16: Pervasive Surveillance Systems

CMSC 25900 / DATA 25900

Spring 2021

The University of Chicago



**THE UNIVERSITY OF
CHICAGO**

Urban Surveillance

Surveillance of Street Corners

CCTV in operation 

Images are being recorded and monitored for your safety and to prevent crime.

We will use CCTV images to aid successful prosecution.

This CCTV system is operated by Thameslink

You can contact Thameslink at:
Thameslink Customer Relations
PO Box 10240
ASHBY-DE-LA-ZOUCH
LE65 9EB

To report a crime to the British Transport Police, call freephone 0800 40 50 40



Surveillance of (My) Street Corner



Surveillance (?) of Street Corners

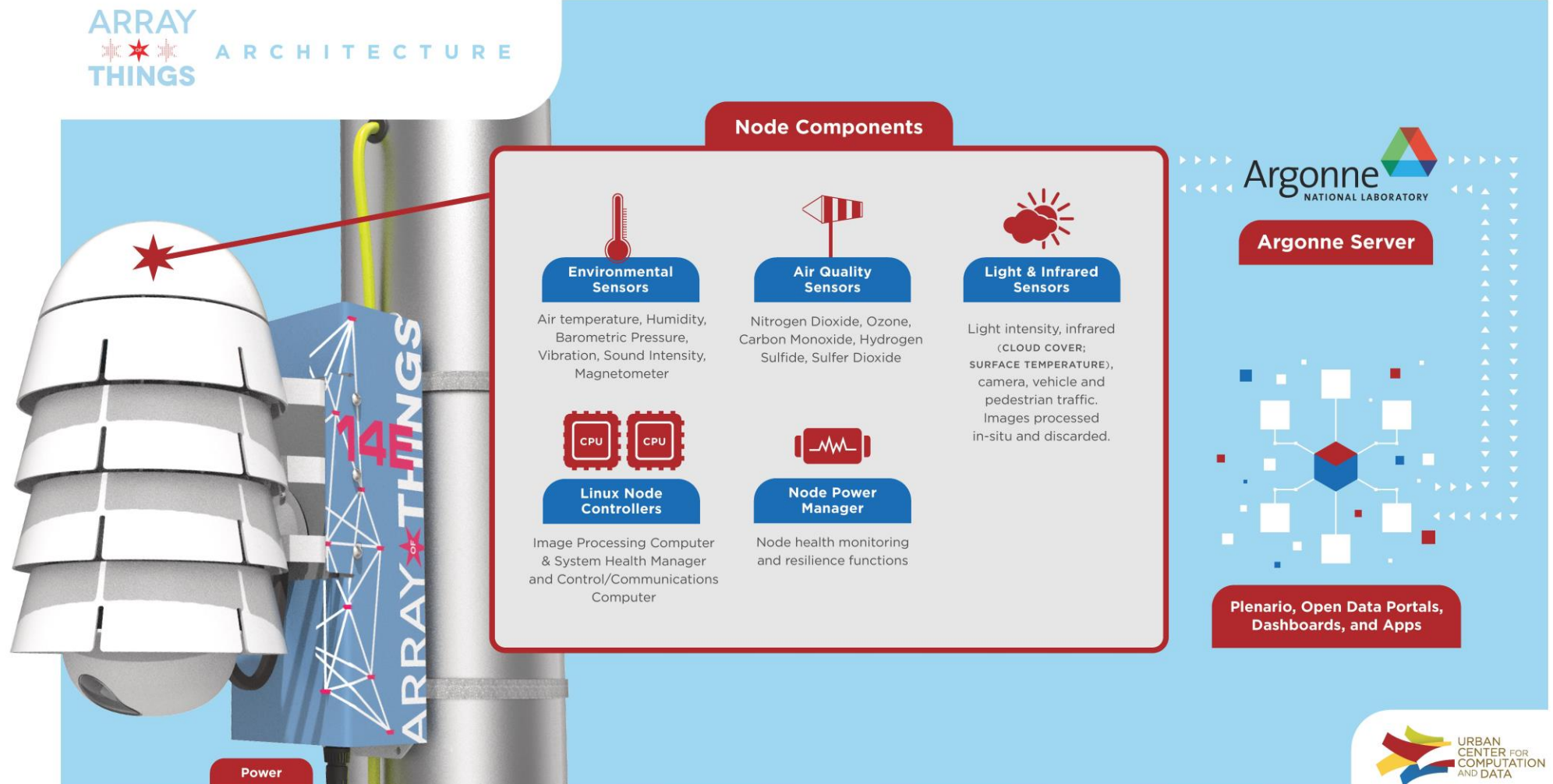


Image from <https://arrayofthings.github.io/>

Surveillance (?) of Street Corners

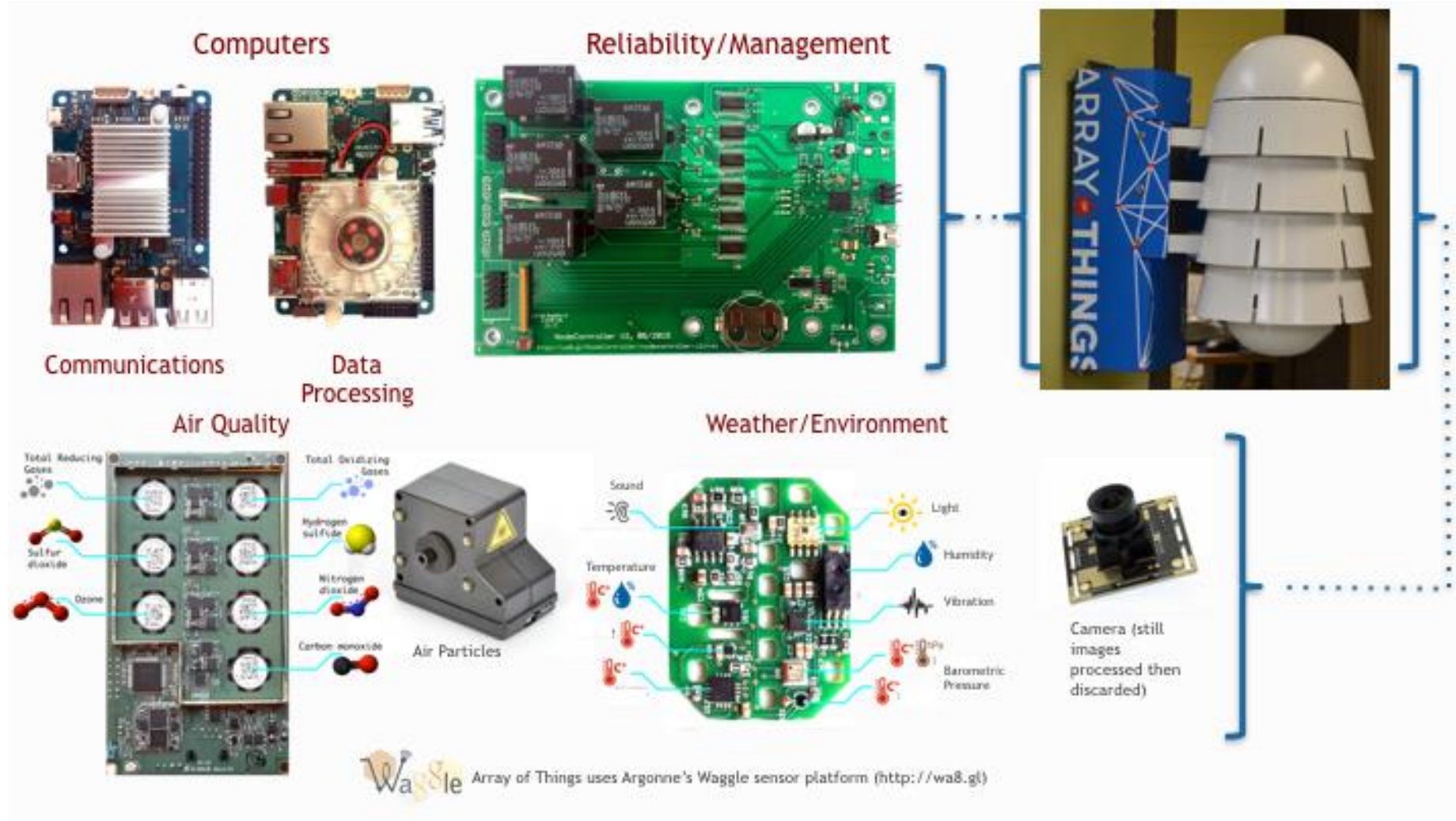


Image from <https://arrayofthings.github.io/>

Surveillance of a Population

Tracking Chicago Juveniles

CHICAGO IS TRACKING KIDS WITH GPS MONITORS THAT CAN CALL AND RECORD THEM WITHOUT CONSENT

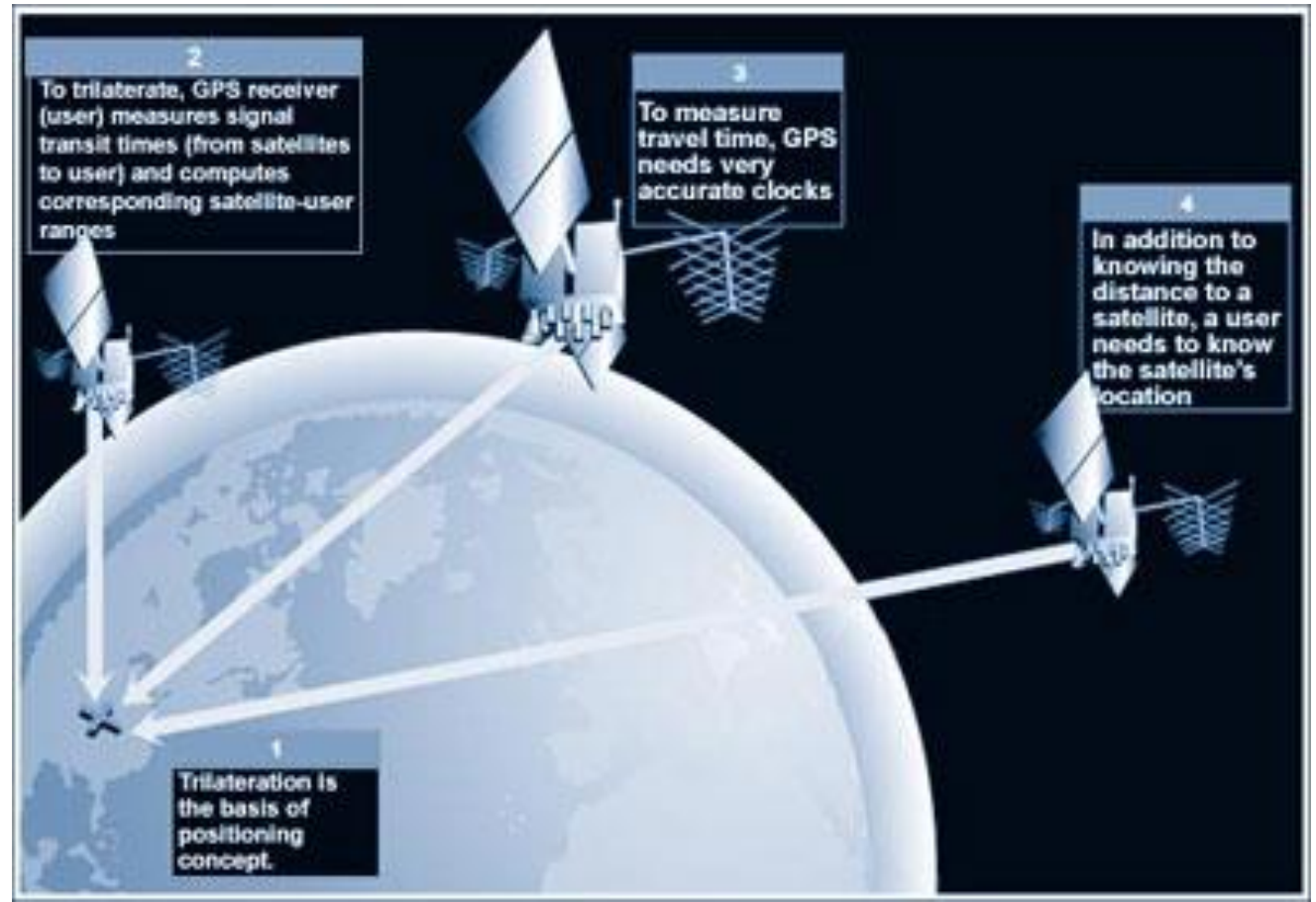
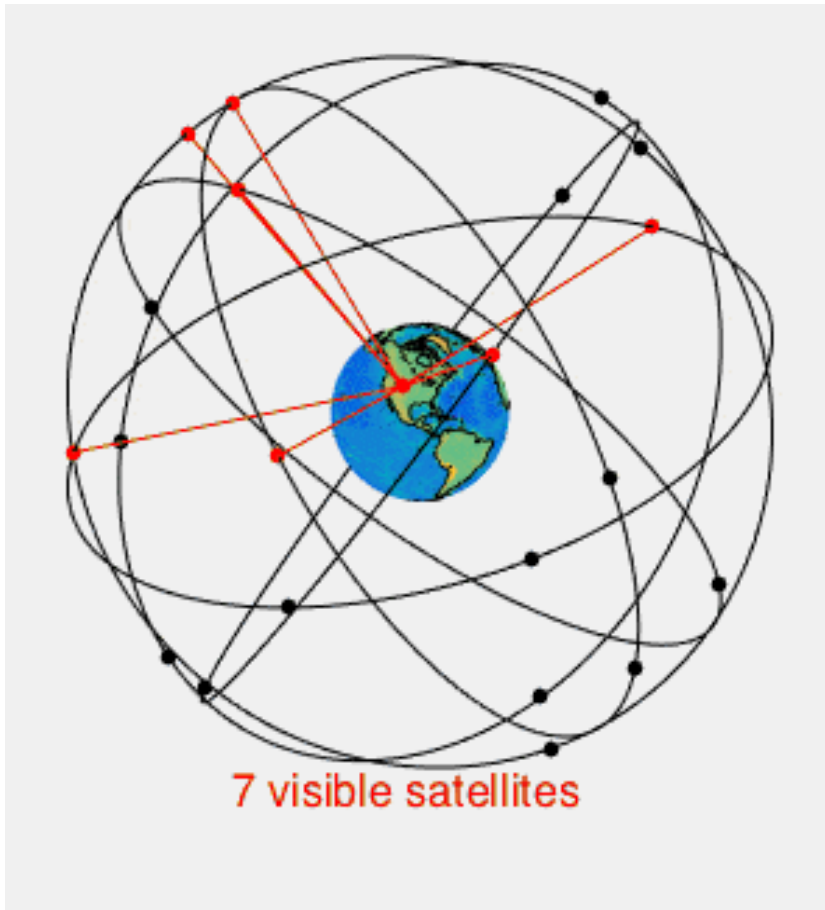
Cook County has a new contract for juvenile ankle monitors that critics say are an invasion of privacy.

This story was co-published with [Citylab](#).

On March 29, court officials in Chicago strapped an ankle monitor onto Shawn, a 15-year-old awaiting trial on charges of armed robbery. They explained that the device would need to be charged for two hours a day and that it would track his movements using GPS technology. He was told he would have to be given permission to leave his house, even to go to school.

<https://theappeal.org/chicago-electronic-monitoring-wiretapping-juveniles/>

Side Note: How GPS Works



Images from https://en.wikipedia.org/wiki/Global_Positioning_System and https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps/howitworks

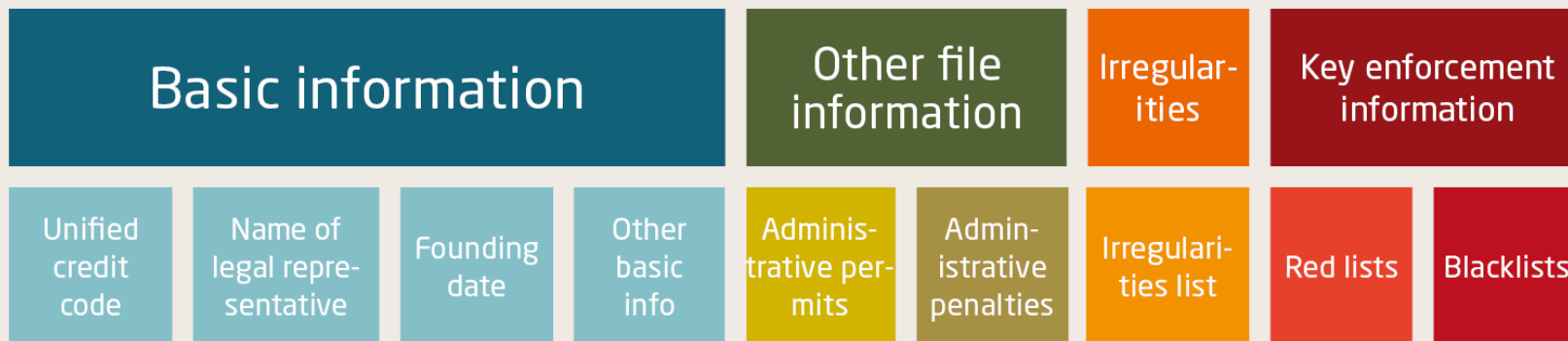
Social Credit System in China

The Social Credit System integrates various types of data into its public files*

Not all data is related to blacklists or red lists



The Social Credit File



*Note: This is the file represented in the national Credit China and Corporate Credit Information databases. While these are the model for national implementation, different formats exist and are shattered across different administrative levels. A significant portion (in some cases over eighty percent) of this data remains confined to these local portals.


Source: Credit China


Social Credit System in China

engadget Sections Login


Chinese facial recognition system confuses bus ad with a jaywalker

It illustrates one of the many issues with China's surveillance culture.


J. Fingas
@jonfingas
November 23rd, 2018



In this article: bigbrother, china, facialrecognition, gadgetry, gadgets, gear, politics, surveillance



Weibo

There are many criticisms you can level at China's [growing reliance on facial recognition](#), including its absolute faith in technology: what happens if there's a false positive? Unfortunately, we just saw an example of that in action. Police in the city of Ningbo have taken [corrective action](#) after the facial recognition system at a crosswalk mistakenly accused famous businesswoman Deng

Facial Recognition in China

The Washington Post
Democracy Dies in Darkness

Technology

Huawei tested AI software that could recognize Uighur minorities and alert police, report says

An internal report claims the face-scanning system could trigger a 'Uighur alarm,' sparking concerns that the software could help fuel crackdown on the mostly Muslim minority group



<https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/>

Facial Recognition in China

- “A document signed by Huawei representatives... shows that the telecommunications firm worked in 2018 with the facial recognition start-up Megvii to test an artificial-intelligence camera system that could scan faces in a crowd and estimate each person’s age, sex and ethnicity. If the system detected the face of a member of the mostly Muslim minority group, the test report said, it could trigger a “Uighur alarm” — potentially flagging them for police in China, where members of the group have been detained en masse as part of a brutal government crackdown.”

Facial Recognition in the USA

BAN FACIAL RECOGNITION

[JOIN A LOCAL EFFORT](#) [SIGN THE PETITION](#) [DONATE](#)

This interactive map shows where facial recognition surveillance is happening, where it's spreading to next, and where there are local and state efforts to rein it in. See something missing? Contact us: team@fightforthefuture.org

- Amazon Ring
- Bans
- Other Laws
- Local
- State
- In Use
- Airports
- Local Police
- State Police
- Other
- Clearview

MADISON FACIAL RECOGNITION BAN
📍 Madison, WI
On December 1, 2020, the Madison City Council voted to ban the use of facial recognition by city government.

MINNEAPOLIS FACIAL RECOGNITION BAN
📍 Minneapolis, MN
On February 12, 2021, Minneapolis City Council voted unanimously to ban facial recognition. This was in part a response to the police killing on George Floyd in the city in the summer of 2020, and the general call to defund the police

Leaflet | © Mapbox © OpenStreetMap

<https://www.banfacialrecognition.com/map/>

Tracking You

Opinion
Surveillance

Amazon's Ring is the largest civilian surveillance network the US has ever seen *Lauren Bridges*

Tue 18 May 2021 08.51
EDT



2699 383

One in 10 US police departments can now access videos from millions of privately owned home security cameras without a warrant



Surveillance At Borders

Learn More >

Technology

Apple employee detained by U.S. customs agents after declining to unlock phone, laptop



Customs and Border Protection officers violated a citizen's rights when they demanded he turn over passwords to his electronic devices at the airport, the American Civil Liberties Union Foundation of Northern California said in a civil complaint filed Tuesday. (Daniel Acker/Bloomberg)

By **Hamza Shaban**
April 3

When Andreas Gal returned from a business trip in Sweden last fall, he was carrying two company-owned devices: an iPhone XS that flashed “Confidential and Proprietary” on its lock screen and a MacBook Pro bearing a sticker that read “PROPERTY OF APPLE. PROPRIETARY.”



Problem solving solved with iPhone and iPad.

LEARN MORE

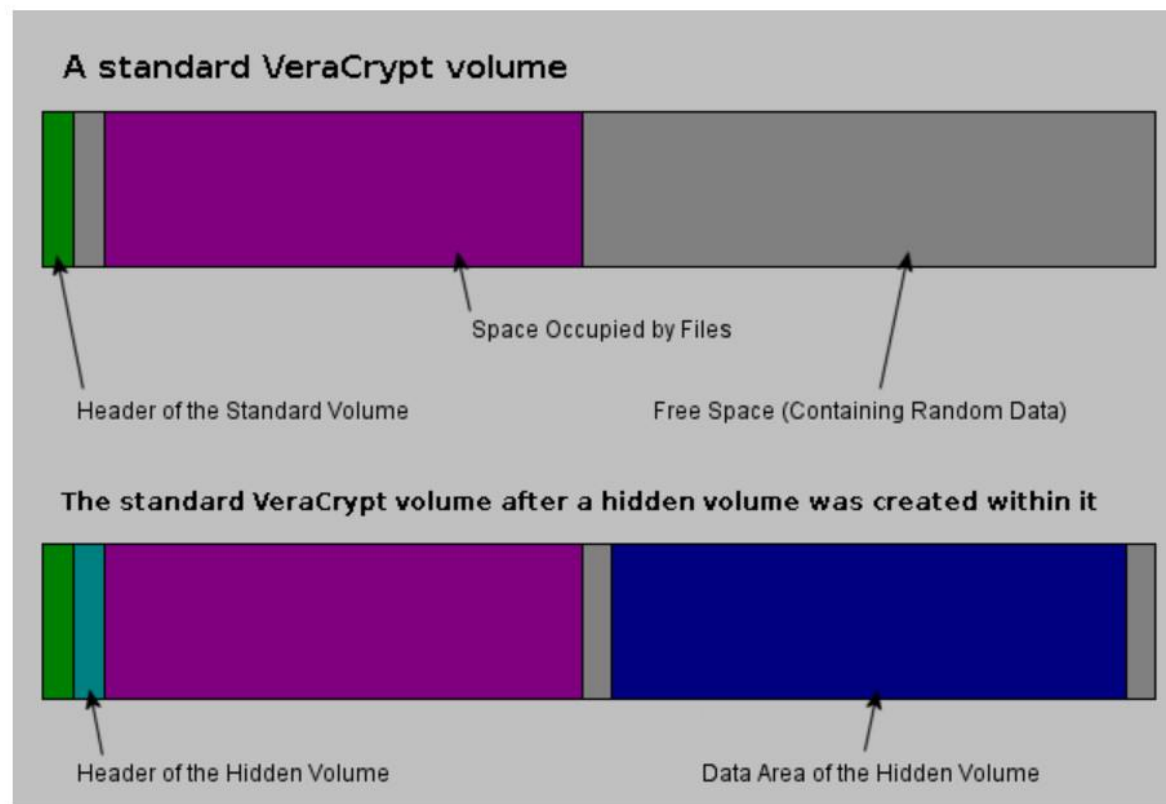


Apple at Work

Plausible Deniability of Encryption

Hidden Volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.



The layout of a standard VeraCrypt volume before and after a hidden volume was created within it.

<https://veracrypt.eu/en/docs/hidden-volume/>

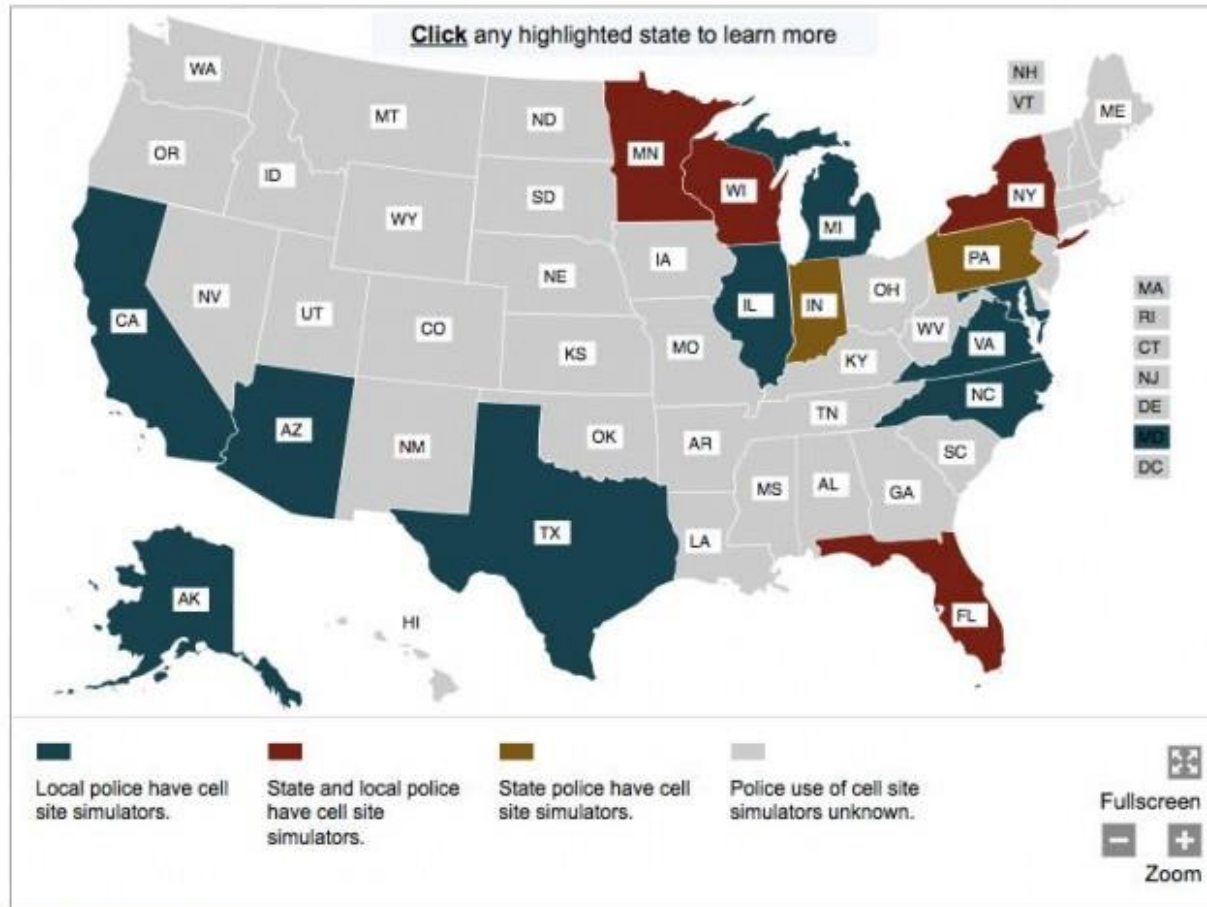
Phones in the Legal System

- Riley v. California
 - SCOTUS 2014
- Unanimous ruling that **warrantless** search of a phone during an arrest is unconstitutional
- Fifth Amendment from the Bill of Rights: Speech cannot be compelled
 - Many (but not all) courts consider passwords to be “speech”
 - Biometrics are not considered speech

Surveillance of Activism

Mobile Devices



- Stingrays (cell site simulator)




[Display a table of the map data.](#)

FBI Surveillance of Activists


The Intercept_

DONATE  49

THE FBI SPENDS A LOT OF TIME SPYING ON BLACK AMERICANS

The FBI released a new trove of documents relating to its surveillance of black activists. They're mostly redacted.

 [Alice Speri](#)
October 29 2019, 9:07 a.m.

THE FBI HAS come under intense criticism after a [2017 leak](#) exposed that its counterterrorism division had invented a new, unfounded domestic terrorism category it called “[black identity extremism](#).” Since then, legislators have pressured the bureau’s leadership to be more transparent about its investigation of black activists, and a number of civil rights groups have filed public records requests to try to better un-

Understanding the Security and Privacy Advice Given to

BLACK LIVES MATTER Protesters

Maia Boyd, Jamar Sullivan, Marshini Chetty, Blase Ur



THE UNIVERSITY OF
CHICAGO





**JUSTICE FOR
TRAYVON**

NAACP.ORG



JUSTICE FOR
TRAYVON

TEA
+ CANDY
= DEATH
IS A

I TAUGHT
TRAYVON
TO TEACH

JUSTICE FOR
TRAYVON

LOCAL



SEENA

BLACK
LIVES
MATTER

NO JUSTICE
NO PEACE
PROSECUTE
THE POLICE
#BLM

AT

Our Goals

- Characterize advice given to novice protesters
- Test protesters' understanding and use of advice
- Focus on security or privacy advice given to participants in BLM protests

PROTESTING SAFELY

WHAT TO WEAR



Nondescript, solid color, layered clothing; cover identifying tattoos

Goggles & mask

Emergency contacts written down

Heat resistant gloves

Tie your hair up

WHAT TO BRING



Water for drinking & tear gas

Snacks

Cash/change & ID

Washcloth

Ear plugs

Bandages & first aid supplies

Protest signs

~~DON'T BRING~~



Cell phone without first turning off Face/Touch ID, going on airplane mode, and disabling data.

Jewelry

Anything you don't want to be arrested with

Contact lenses



Passwords might be safer than biometric authentication methods. GETTY

Turn off biometric authentication

In January 2019, a federal judge ruled that police can't force you to unlock your phone using your fingerprint, eyes or face. Still, to be on the safe side, it's probably best to turn off those biometric authentication methods while you're protesting.

Passwords may be safer, as they're generally protected under the Fifth Amendment. Besides, you might conveniently happen to forget yours if an officer asks you to unlock your device.

protesting tips for being safe and strong + #blacklivesmatter

- COMMUNICATION:**
1. make sure you write 2+ phone numbers in sharpie on your body be careful in case they are identified.
 2. med bracelet!
 3. turn location/cellular data off. enable emergency SOS.
 4. passcode only option.
 5. ductape camera in case you have to secretly record evidence
 6. **DO NOT POST PHOTOS OF PEOPLE. THEY WILL BE TRACKED BY POLICE. YOUR ACTIONS HAVE CONSEQUENCES. YOU ARE NOT THERE TO BE A TOURIST. SOME PEOPLE WILL BREAK YOUR CAMERA!**
 7. cash for transportation. have a plan. it will be chaotic. be careful with bikes. buses and streets will be shut down. try to be as local as possible. i repeat. have a plan.



SAFETY DURING PROTEST



WHAT TO DO

- + Plan ahead: For essential needs, care and supplies. Know what to expect. Know how to get assistance. Plan for how to re-contact your buddies if separated
- + Be calm and focused: when things get most intense, react to danger or warning signs sooner, not later
- + Watch for signs of physical and mental problems in yourself and others. Cool down others who exhibit panic behavior
- + Document: film or write down police actions, brutality, and injuries

WHAT NOT TO DO

- + Don't put vaseline, mineral oil, oil-based sunscreen or moisturizers on skin as they can trap chemicals
- + Don't wear contact lenses, which can trap irritating chemicals underneath
- + Don't wear things which can easily be grabbed (i.e. jewelry, ties, loose hair)
- + Don't go alone, if you can help it - go with an affinity group or some friends who know you well
- + Don't forget to eat food and drink lots of water

WHAT TO BRING

- + Water in a plastic bottle with squirt top, to drink and to wash off your skin or eyes
- + Energy snacks
- + Identification and/or emergency contact information
- + Enough money for pay-phone, food, transportation
- + Watch, paper, pen for accurate documentation of events
- + Inhaler, epipen, insulin & several days of prescription medication
- + Menstrual pads. Avoid using tampons - if you're arrested you may not have a chance to change
- + Basic First Aid Kit
- + Wet Wipes and tissues

WHAT TO WEAR

- + Shatter resistant Swimming Goggles and a N95 Facemask
- + Comfortable, protective shoes that you can run in
- + Clothing covering all your skin to protect from sun and pepper spray exposure
- + Shatter-resistant eye protection (i.e. sunglasses, swim goggles, or gas mask)
- + Bandana to cover nose and mouth soaked in water, lemon juice or vinegar. it can aid in breathing during chemical exposure
- + Fresh clothes in plastic bag (in case yours get contaminated by chemical weapons)
- + A hat to protect you from the sun and from chemical weapons

DEALING WITH TEARGAS

- + Avoid use of oils & lotions because they can trap the chemicals and thereby prolong exposure
- + Gas masks provide the best facial protection, if properly fitted and sealed. Alternatively, goggles, respirators, or a wet bandana over the nose & mouth will help
- + STAY CALM. Panicking increases the irritation. Breathe slowly and remember it is only temporary
- + Blow your nose, rinse your mouth, cough & spit. Try not to swallow
- + Wearing contacts: you must remove the lenses or get someone to remove them for you, with CLEAN, uncontaminated fingers. Destroy the lenses after exposure
- + DO NOT RUB IT IN
- + Use an eye flush using a solution of half liquid antacid and half water. This only applies to aluminum hydroxide or magnesium hydroxide

KNOW YOUR RIGHTS

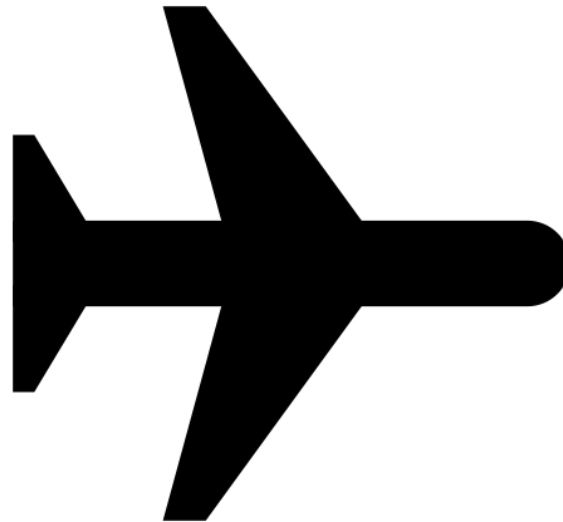
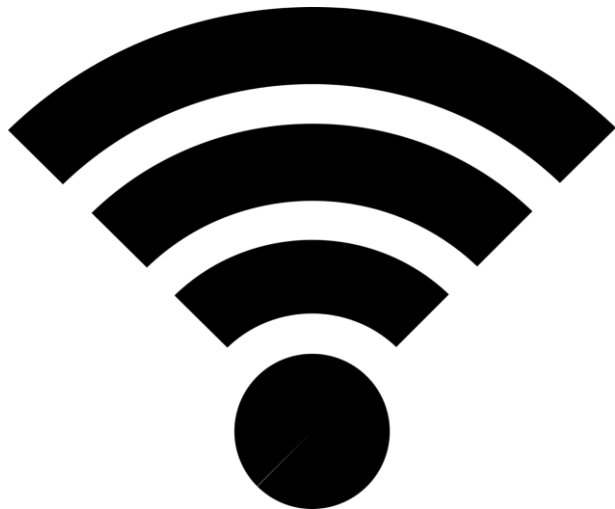
- + Freedom of Expression and Assembly: Everyone has the right to carry their opinion to the streets.
- + Protection of the Right to Freedom of Assembly: Law enforcement must facilitate and not restrict a peaceful public assembly.
- + Freedom from excessive use of force: In the policing of non-violent protests, police must avoid the use of force.
- + Right to Medical Assistance: If you are injured you have a right to medical assistance without delay.
- + Freedom from Arbitrary Arrest and Detention: If you are arrested you have a right to be told of the reason for your arrest, you also have the right promptly after your arrest to have access to a lawyer and to your family.
- + Right to Complain: If your rights have been violated you have a right to file a complaint and to be provided information on how to do so.

Part 1: Analysis of Safety Guides

- 13 classes of advice, including advice about:
 - Protecting against phone confiscation
 - Protecting messages and web browsing
 - Disabling communication features
 - Protecting against identification

Part 1: Analysis of Safety Guides

- Disabling transmissions (31 guides)
 - Using airplane mode (18 guides)
 - Turning off phone (8 guides)
 - Turning off location services (20), WiFi (8), Bluetooth (7), and cellular data (7)



Part 1: Analysis of Safety Guides

- Leave primary phone at home (21 guides)
 - Bring a burner phone (16 guides)
 - Provided rationale for advice (14 guides)
 - Vague
 - “To protect your privacy and prevent surveillance, the best thing you can do is leave your phone at home.”

Part 1: Analysis of Safety Guides

- Disable biometrics (28 guides)
 - Use a passcode instead (11 guides)
 - Explained importance of advice (6 guides)
 - Vague explanations
 - “It might be best to deactivate facial recognition or fingerprint unlocking if you’re concerned about being approached by the police.”
 - Specifically mention key rationale (2 guides)



Part 1: Analysis of Safety Guides

- Using a strong passcode (20 guides)
 - Recommended using passcode/password instead of biometrics (12 guides)
 - Explained purpose of following advice (7 guides)



Part 1: Analysis of Safety Guides

- Using end-to-end encrypted (*E2EE*) apps (27 guides)
 - Use Signal (26 guides)
 - Use WhatsApp (3), Wire (3), Wickr (2), Dust (1), Keybase (1), or Telegram (1)



Signal



Part 1: Analysis of Safety Guides

- Avoid identifiers (21 guides)
 - Avoid people in photos/recordings (20 guides)
 - Avoid faces (14 guides), identifying features (14), and locations (6)
 - Remove metadata (9 guides)
 - Blur features (12 guides)
- Social media caution (18 guides)



Part 1: Analysis of Safety Guides

- Less prevalent classes of advice:
 - Encrypt device (9 guides)
 - Back up device (6 guides)
 - Use a VPN (4 guides)
 - Use a secure browser (3 guides)
 - Disable notifications (2 guides)
 - Use screen pinning (2 guides)

Part 2: Survey of Primarily Novice Protesters

- US-based supporters of BLM
- Had attended at least one BLM protest in person
- 167 eligible survey respondents
 - 100% supported the BLM movement
 - 7% considered themselves organizers (vs. participants)
 - 53% women, 46% men, 1% non-binary
 - 52% Black, 31% White, 5% Asian, 5% Hispanic/Latinx
- 75% of respondents had attended 1 - 4 BLM protests total

Part 2: Survey of Primarily Novice Protesters

- 13 classes of advice, 13 statements
 - “Disable biometric (face or fingerprint) unlocking for your phone. Use a password/passcode instead.”
- For each statement, we asked:
 - Had they seen this advice?
 - Did they understand this advice?
 - Did they follow this advice? (Why or why not?)

Part 2: Survey Results



(a) "I have seen or heard similar advice about attending a protest."

(b) "I feel that I understand the purpose of this advice about attending a protest."

(c) "I follow this advice when attending a protest."

Biometric authentication

- Not protected by 5th amendment
- Device can be forcefully unlocked

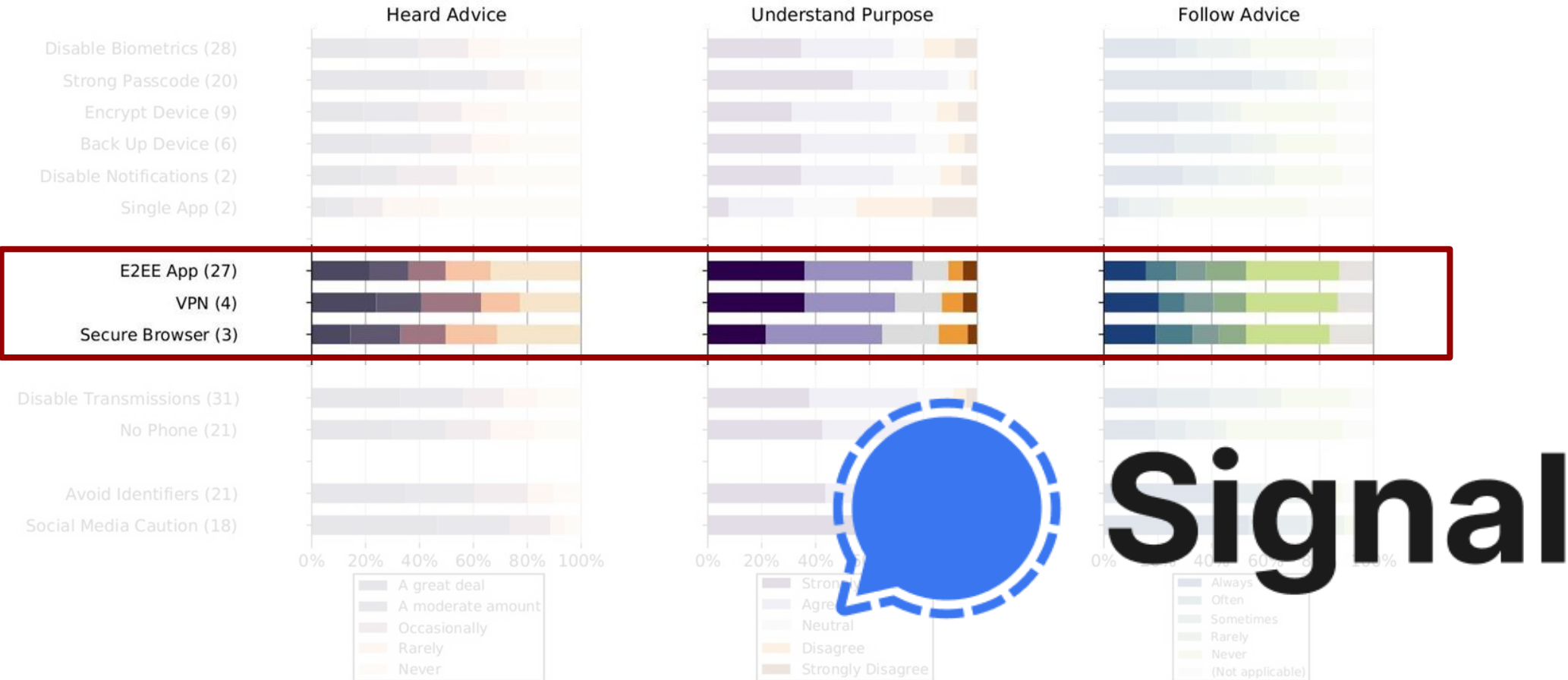


Using a strong passcode

- Protected by 5th amendment
- Device cannot be forcefully unlocked



Part 2: Survey Results

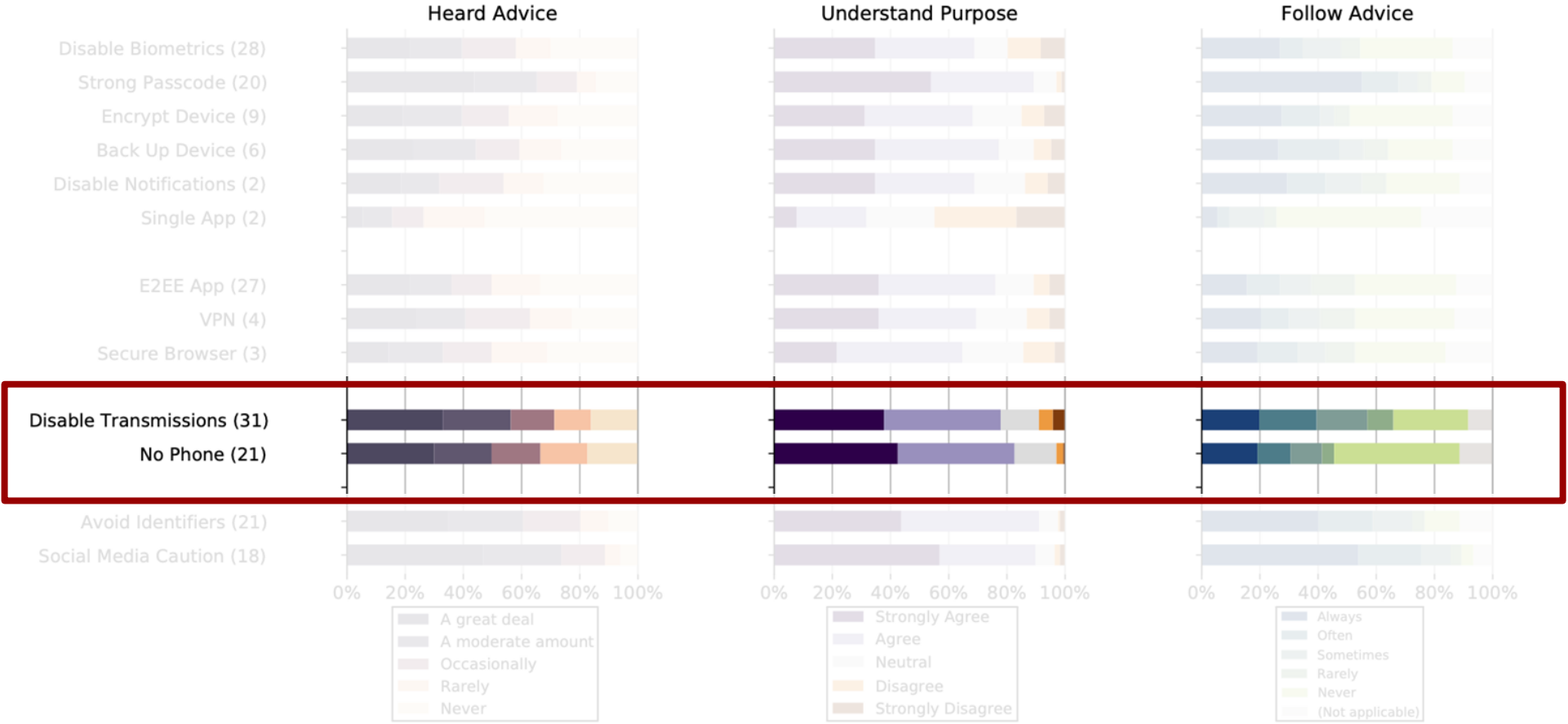


(a) "I have seen or heard similar advice about attending a protest."

(b) "I feel that I understand the purpose of this advice about attending a protest."

(c) "I follow this advice when attending a protest."

Part 2: Survey Results



(a) "I have seen or heard similar advice about attending a protest."

(b) "I feel that I understand the purpose of this advice about attending a protest."

(c) "I follow this advice when attending a protest."

Surveillance of Students

Exam-Proctoring Software

Online exam monitoring can invade privacy and erode trust at universities

December 3, 2020 5:16pm EST

Testing and exam proctoring methods that invade privacy and erode trust undermine the very integrity that institutions demand students uphold. (Shutterstock)

Email

Twitter

72

Facebook

353

LinkedIn

Print

The health risks posed by COVID-19 mean most Canadian university classes are online this year. As a result, some students will write exams online via remote proctoring platforms that surveil their activities.

These tools go by names like ProctorU, Examity, Respondus and Proctorio, among others. Designed by for-profit tech startups, they monitor students' laptops, tablets or phones during the course of an exam. Proctoring tools can monitor eye movements, capture students' keystrokes, record their screens and track their searches as well as their home environments and

Author



Bonnie Stewart

Assistant Professor, Online Pedagogy & Workplace Learning, Faculty of Education, University of Windsor

Disclosure statement

Bonnie Stewart does not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.