

Lecture 16: Tracking Part 2; Pervasive Surveillance Systems

CMSC 25910

Spring 2023

The University of Chicago



Measuring Tracking via Data Access Rights



What Twitter Knows

**Characterizing Ad Targeting Practices, User Perceptions,
and Ad Explanations Through Users' Own Twitter Data**

Miranda Wei, Madison Stamos, Sophie Veys, Nathan Reitingner, Justin Goodman,
Margot Herman, Dorota Filipczuk, Ben Weinshel, Michelle L. Mazurek, Blase Ur
In *Proc. USENIX Security 2020*.

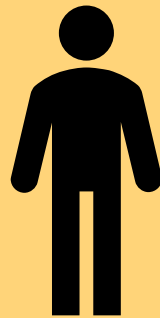


Targeted Advertising:

Using detailed information about users' demographics, preferences, opinions, and activity to target ads



expectation:



Blase Ur

gender: M

location: Chicago, IL

interests: bicycles,
succulents, punk rock

Reality: organic ketchup buyer + 15 other criteria

HEINZ Heinz Ketchup 
@HeinzKetchup_US

This is it, the last week of [#HeinzFantasySandwich](#)! This week, you're Team Grilled Cheese. You can only draft FOUR players. Who's on your team? [#FantasyFootball](#) [#FantasyDraft](#)

 WHAT'S ON YOUR #HEINZ FANTASY SANDWICH? WEEK 4: TEAM GRILLED CHEESE 	1 	2 	3 
	4 	5 	6 
	7 	8 	9 

5:30 AM · Sep 26, 2018 · [Twitter for Advertisers](#)

targetingType: Tailored audiences (lists)

targetingValue:
NCS_PD_04358_Kraft_Organic
and_natural_ketchup
buyers_1_26362226

...

targetingType: Keywords
targetingValue: #parenting

...

1.

What ad targeting mechanisms are currently used to target Twitter users?

2.

What do Twitter users think about the mechanisms for...

a)

ad targeting?

b)

transparency?

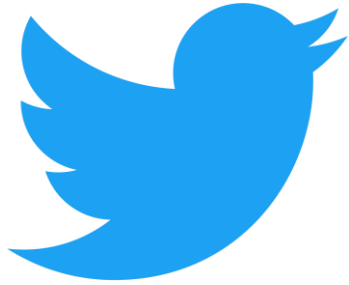
Requesting Data From Twitter

Settings	 Your Twitter data
@_weimf	Account >
Account >	Account history >
Privacy and safety >	Apps, devices & information >
Notifications >	Account activity >
Content preferences >	Interests and ads data >
General	Download an archive of your data
Display >	You can request a ZIP file with the information that we believe is most relevant and useful to you. You'll get an email sent to mirandaaa.wel@gmail.com when it's ready to be downloaded. Your download will include a file called "Your archive" that will allow you to see your data in a desktop web browser. Learn more
Data usage >	
Accessibility >	Twitter Request archive
About Twitter >	Periscope Request archive

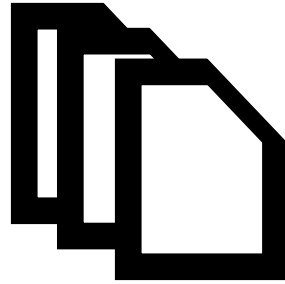
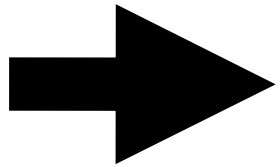
Contents of ad-impressions.js

```
[ {
  "ad" : {
    "adsUserData" : {
      "adImpressions" : {
        "impressions" : [ {
          "deviceInfo" : {
            "osType" : "Ios",
            "deviceId" : "#####",
            "deviceType" : "iPhone X"
          },
          "displayLocation" : "SearchTweets",
          "promotedTweetInfo" : {
            "tweetId" : "#####",
            "tweetText" : "RT @SpotifyBrands: Young people's digital lives are subtly shifting
                           culture. Discover more with our global trends report.",
            "urls" : [ ],
            "mediaUrls" : [ ]
          },
          "advertiserInfo" : {
            "advertiserName" : "Spotify",
            "screenName" : "@Spotify"
          },
          "matchedTargetingCriteria" : [ {
            "targetingType" : "Events",
            "targetingValue" : "Back to School 2019"
          }, {
            "targetingType" : "Age",
            "targetingValue" : "18 to 49"
          }, {
            "targetingType" : "Locations",
            "targetingValue" : "United States"
          }, {
            "targetingType" : "Platforms",
            "targetingValue" : "iOS"
          }
        ]
      }
    }
  }
}
```

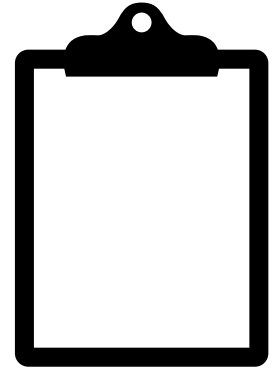
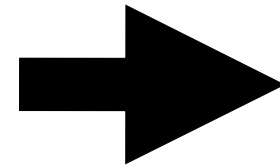
Study Protocol



request
Twitter data



upload ad-
related data

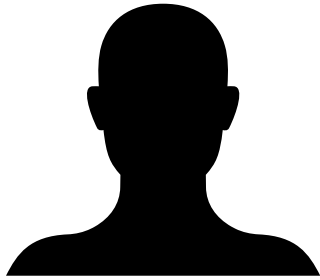


take customized
survey

Ethics and Participant Privacy

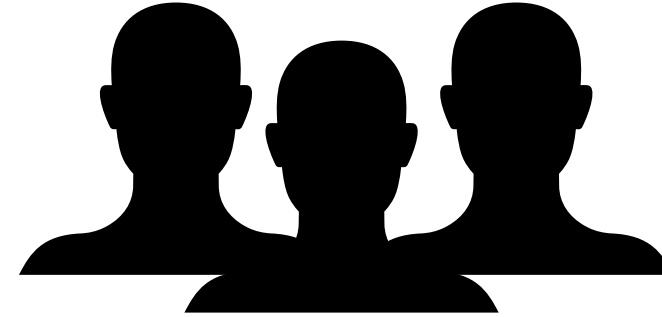
- Approved by IRB
- Did not collect any personally identifiable information
 - Only 3 advertising-related files from their Twitter archives
- Replace any potential identifiers in targeting data with #, *, MM, DD, YYYY as appropriate

231 Participants and Their Ads



per participant

- mean 6.6 years on Twitter
- mean 1,046.6 ads in last 3 months



across all participants

- observed 240,651 ads with at least one targeting type
 - e.g., location targeting
- 45,209 unique instances
 - e.g., Boston

Targeting Types

demographic:

characteristics about user and their device(s)

- provided by user or inferred by Twitter

targeting type	uses
language	350,121
platform	32,351
location	31,984
new device	236

Targeting Types

demographic:
*characteristics about
user and their device(s)*

- provided by user or
inferred by Twitter

targeting type	uses
language	350,121
platform	32,351
location	31,984
new device	236

psychographic:
*user lifestyles,
behaviors or attitudes*

- provided by user or
inferred by Twitter

targeting type	uses
follower lookalikes	590,502
conversation	128,005
behavior	35,008
interest	25,284

Targeting Types

demographic:
characteristics about user and their device(s)

- provided by user or inferred by Twitter

targeting type	uses
language	350,121
platform	32,351
location	31,984
new device	236

psychographic:
user lifestyles, behaviors or attitudes

- provided by user or inferred by Twitter

targeting type	uses
follower lookalikes	590,502
conversation	128,005
behavior	35,008
interest	25,284

advertiser:
user information collected offline

- provided by advertiser

targeting type	uses
tailored (list)	113,952
mobile	21,631
tailored (web)	18,016

Some Lesser-discussed Targeting Types

- **follower lookalikes:** target people who don't necessarily follow a given account, but have similar interests or demographics to the account's actual followers
 - used 242,709 times, e.g., @netflix
- **behavior targeting:** specific behaviors on Twitter; inferred behavior, such as shopping and lifestyle habits or income
 - used 35,088 times, e.g., US - Household income: \$30,000-\$39,000
- **tailored audience (list):** reach specific people by uploading lists containing PII (email addresses, phone numbers, or Twitter handles) that are matched to Twitter users' accounts
 - used 113,952 times, e.g., Lifetime Suppression [Installs] (Device ID)
- **conversation topic targeting:** allows advertisers to target people based on topics they have engaged with (e.g., Tweeted, clicked, Retweeted, replied, liked, viewed) on Twitter
 - used 128,005 times, e.g., Food

Targeting Types

(<https://business.twitter.com/en/targeting.html> and pages linked from it).

- **Age targeting** allows advertisers to target people by age buckets, such as 18+ years old or 18-24 years old.
- **Behavior targeting** allows advertisers to target people based on inferred behavior, such as shopping and lifestyle habits or income.
- **Conversation topic targeting** allows advertisers to target people based on topics they have engaged with (e.g., Tweeted, clicked, Retweeted, replied, liked, viewed) on Twitter.
- **Event targeting** allows advertisers to target people based on events they are interested in or have engaged with (e.g., Tweeted, clicked, Retweeted, replied, liked, viewed) on Twitter.
- **Follower lookalike targeting** allows advertisers to target people who don't necessarily follow a given account, but have similar interests or demographics to the account's actual followers.
- **Gender targeting** allows advertisers to target people based on their self-reported or inferred gender.
- **Interest targeting** allows advertisers to target people based on inferred interests, as determined by who they follow on Twitter and their Tweets, Retweets, and clicks.
- **Keyword targeting** allows advertisers to target people based on words or phrases they have Tweeted about or searched for on Twitter.
- **Language targeting** allows advertisers to target people who use a certain language on Twitter.
- **Location targeting** allows advertisers to target people based on region, city, metro or zip code.
- **Mobile audience targeting** allows advertisers to target people who use their mobile app.
- **Movie and TV show targeting** allows advertisers to target people based on movies and TV shows they have watched or are likely to watch.
- **Platform targeting** allows advertisers to target people who use a certain platform, such as iOS or Desktop, to access Twitter.
- **Retargeting campaign engager targeting** allows advertisers to target people based on prior engagement with (e.g., Tweeting, clicking, Retweeting, replying, liking, or viewing) their company.
- **Tailored audience (list) targeting** allows advertisers to reach specific people on Twitter by uploading lists, which contain personal information (email addresses, phone numbers, or Twitter handles) that are matched to Twitter users' accounts.
- **Tailored audience (web) targeting** allows advertisers to target people who have visited their website.

Potential Violations of Twitter's Policies?

prohibited to target by race, religion, sex life, health, politics, and financial status yet...

- **keyword:** “unemployment,” “Gay,” “#AfricanAmerican,” “latinas”
- **conversation:** “Liberal Democrats (UK)”
- **tailored list:** “YYYY account status: balance due,” “Christian Audience to Exclude,” “LGBT Suppression List”

Opinions of Targeting Types

vary by specificity and accuracy



tend to approve
abstractly, but object
to specific instances

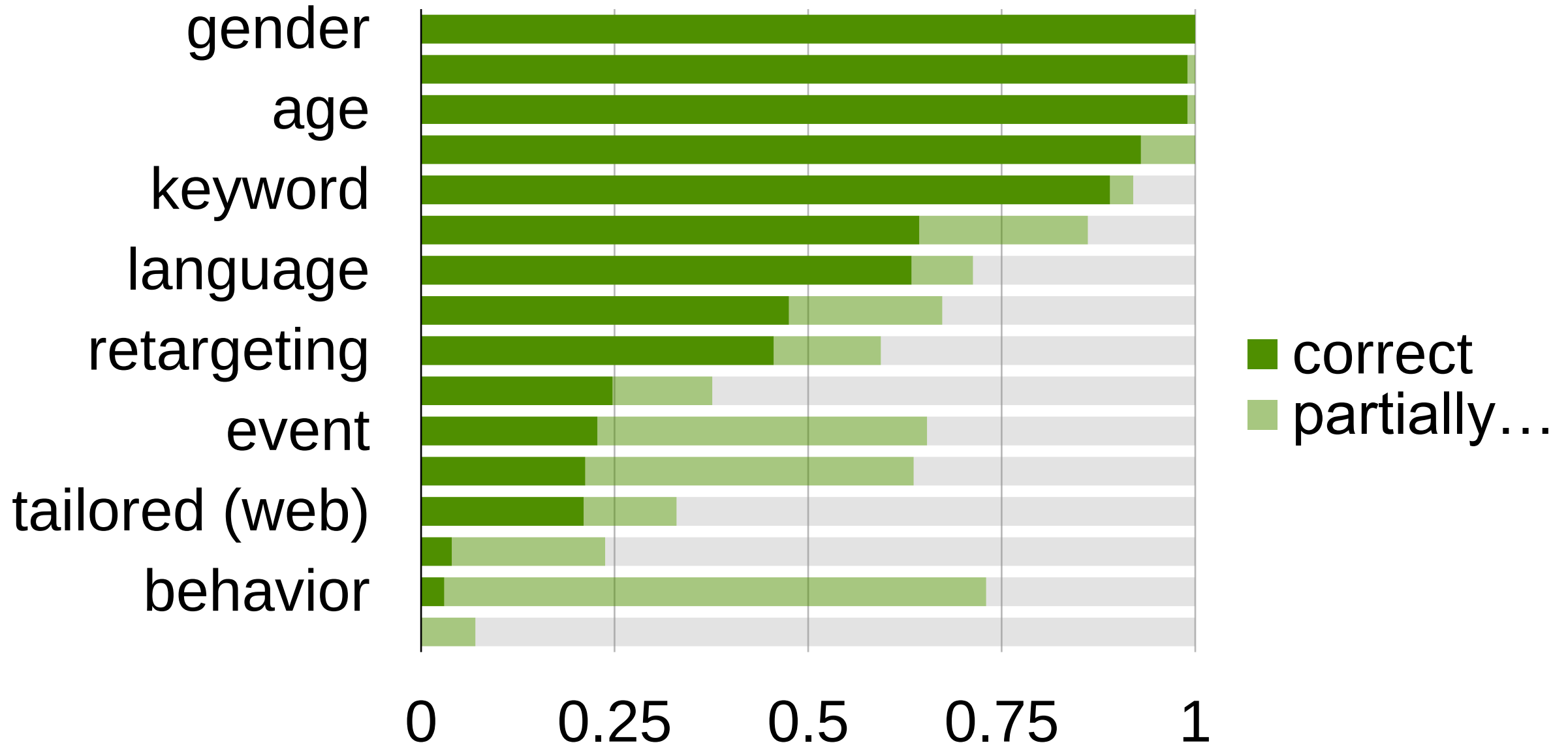
e.g., event targeting



accuracy significantly
correlated with fairness
and comfort

... to a certain point

Participants' Understanding of Targeting Types



Current Ad Explanations



Why am I seeing this ad?

One reason you may be seeing this ad is that **Postmates** wants to reach people interested in **Health news and general info**. There may be other reasons you're seeing this ad, including that **Postmates** wants to reach **people above the age of 18 and located here: Phoenix AZ, US**.

You can view and manage information connected to your account that Twitter may use for ads purposes. [See your Twitter data](#).

Twitter also personalizes ads using information received from partners as well as app and website visits. You can control these interest-based ads using the "[Personalize ads](#)" [setting](#).



Why am I seeing this ad?

You're seeing this ad because you're on a list **Postmates** wants to reach on Twitter. When the list was uploaded, Twitter did not learn any new identifying information about you.

Your Data



Postmates

[Learn more about Postmates](#)

- March 17, 2019
Postmates uploaded a **hashed** list. Twitter matched your information with information on that list.
- April 17, 2019
You saw this ad from **Postmates**

There may be other reasons you're seeing this ad, including that **Postmates** wants to reach **people who are ages 18 and up, are located in Phoenix AZ, US, and are Female**. This information is based on your Twitter profile and where you've connected to the internet.

Speculative Ad Explanations

detailed text

Why am I seeing this ad?

You may be seeing this ad because **Postmates** wants to reach people similar to people who follow **@chrishemsworth**; and **@BarackObama**.

You may also be seeing this ad because **Postmates** has added your Twitter username or email to a list of people who they want to reach. You may have been added if you **visited their webpage, used their mobile app, or signed up for their mailing list**.

You may also be seeing this ad because **Postmates** wants to reach people on the following audience lists: **Suppression (Installs All Time) (email)**; **Suppression (Installs All Time) (Device Id)**; and **Email Suppression List (May 2018)**

You may also be seeing this ad because **Postmates** wants to reach people interested in **Health news and general info**. Your interest profile is based on your **tweets and retweets, pages and people you follow, websites you visit, and more**.

You may also be seeing this ad because **Postmates** wants to reach people in the following demographics: **ages 18 and up; Phoenix AZ, US; and Female**.

You can view or manage account information used for ad purposes. Go to the "Personalize ads" setting to control internet-based ads.

detailed visual

Why am I seeing this ad?

Some of the targeting types used to target this ad to you were:



Tailored audiences: **Postmates** can add your name, your Twitter username, or your email to a list of people they want to reach.

Suppression (Installs All Time) (email) Suppression (Installs All Time) (Device Id) Email Suppression List (May 2018)



Follower Look-alikes: **Postmates** can target people who are similar to people who follow a person or page on Twitter.

@chrishemsworth @BarackObama



Interests: **Postmates** can target people based on inferred interests.

Postmates did not target you using inferred interests.



Demographics: **Postmates** can target based on demographics or inferred demographics.

Ages 18 and up Phoenix AZ, US Female

Speculative Ad Explanations

creepy

Why am I seeing this ad?

You saw this ad on **April 17, 2019 at 11:05 AM** on the **Twitter app** from a(n) **Android device**, IP address **###.###.##** (**Phoenix AZ, US**).

You are seeing this ad because **Postmates** used your information, such as your **email address or phone number**, to find you on Twitter.

You are also seeing this ad because **Postmates** has made the following determinations about you:

- Your information on Twitter was matched with external lists called **Suppression (Installs All Time) (email)**, **Suppression (Installs All Time) (Device Id)**, and **Email Suppression List (May 2018)**
- You have a lot in common with people who follow **@chrishemsworth**, and **@BarackObama**
- You are interested in **Health news and general info**.
- You are participating in the conversation about **Fitness** on Twitter.
- You **are ages 18 and up, and are Female**.
- You are located in or around **Phoenix AZ, US**.

These inferences are based on your Twitter profile and online activities, such as your **tweets and retweets**, **people and pages you follow**, and **websites you visit**, as **well as data that third parties have provided about you**.

You can view or manage account information used for ad purposes. Go to the "Personalize ads" setting to control internet-based ads.

Speculative Ad Explanations

control

Why am I seeing this ad?

One reason you may be seeing this ad is that **Postmates** paid for an ad on this site.

You can view or manage account information used for ad purposes. Go to the "Personalize ads" setting to control internet-based ads.

Ad Explanation Results

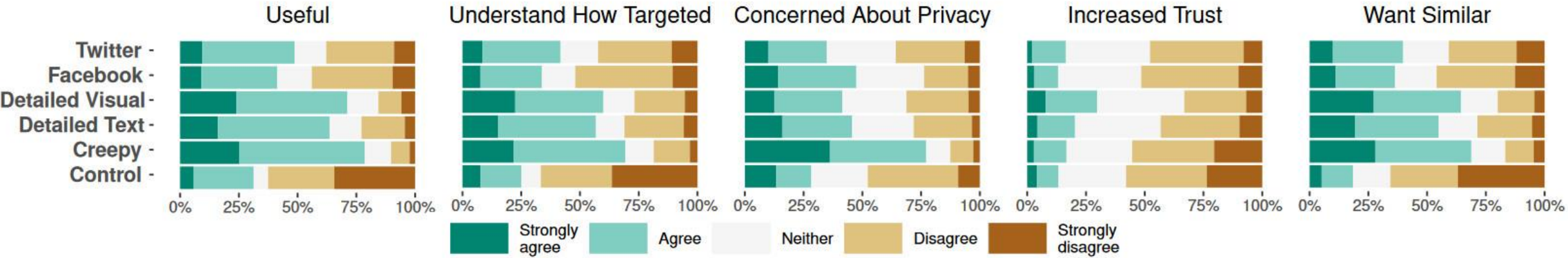
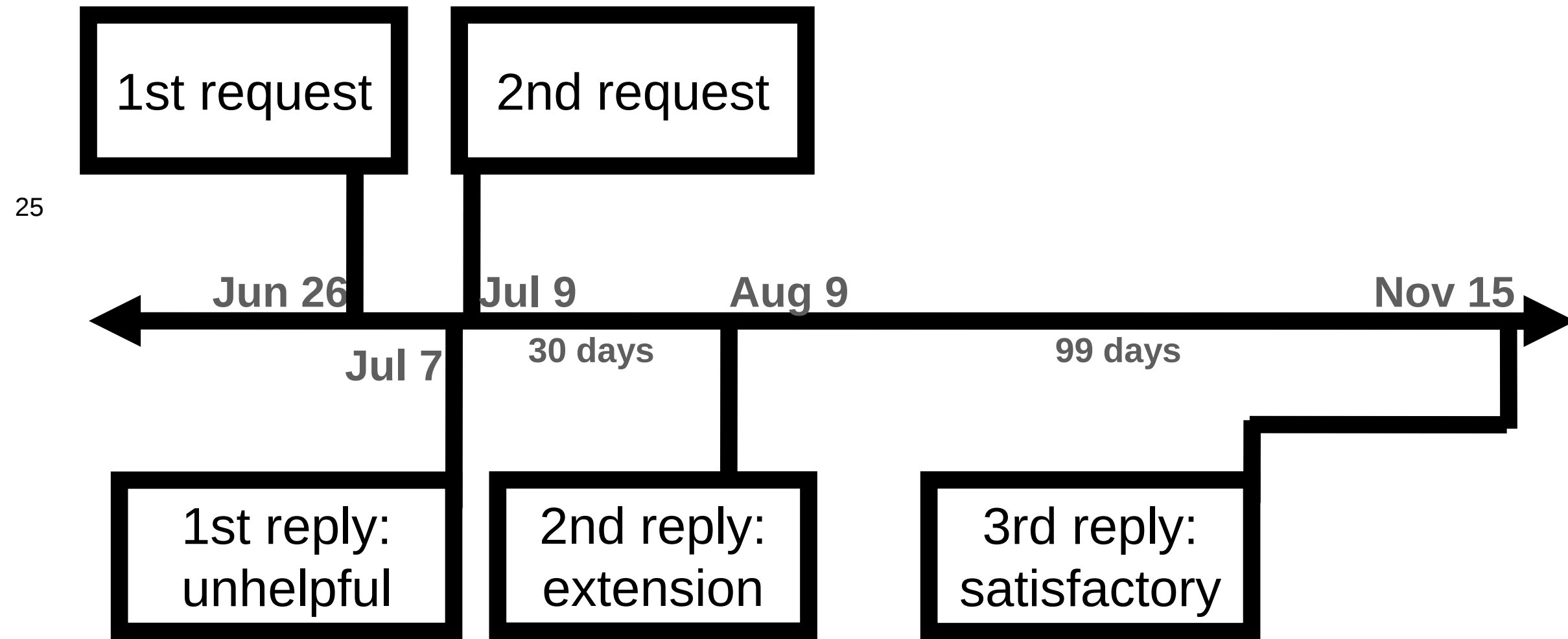


Figure 5: Participants' level of agreement to questions about ad explanations.

Clarifications from Twitter



Key Takeaways

- Transparency is key, especially data access
- Some of the most concerning targeting types are understudied
 - e.g., tailored audiences, follower lookalikes
- How to enforce targeting policies if skirting scrutiny is trivial?
- Ad explanations should be more detailed

Urban Surveillance

Surveillance of Street Corners



Surveillance of (My Former) Street Corner



Surveillance (?) of Street Corners

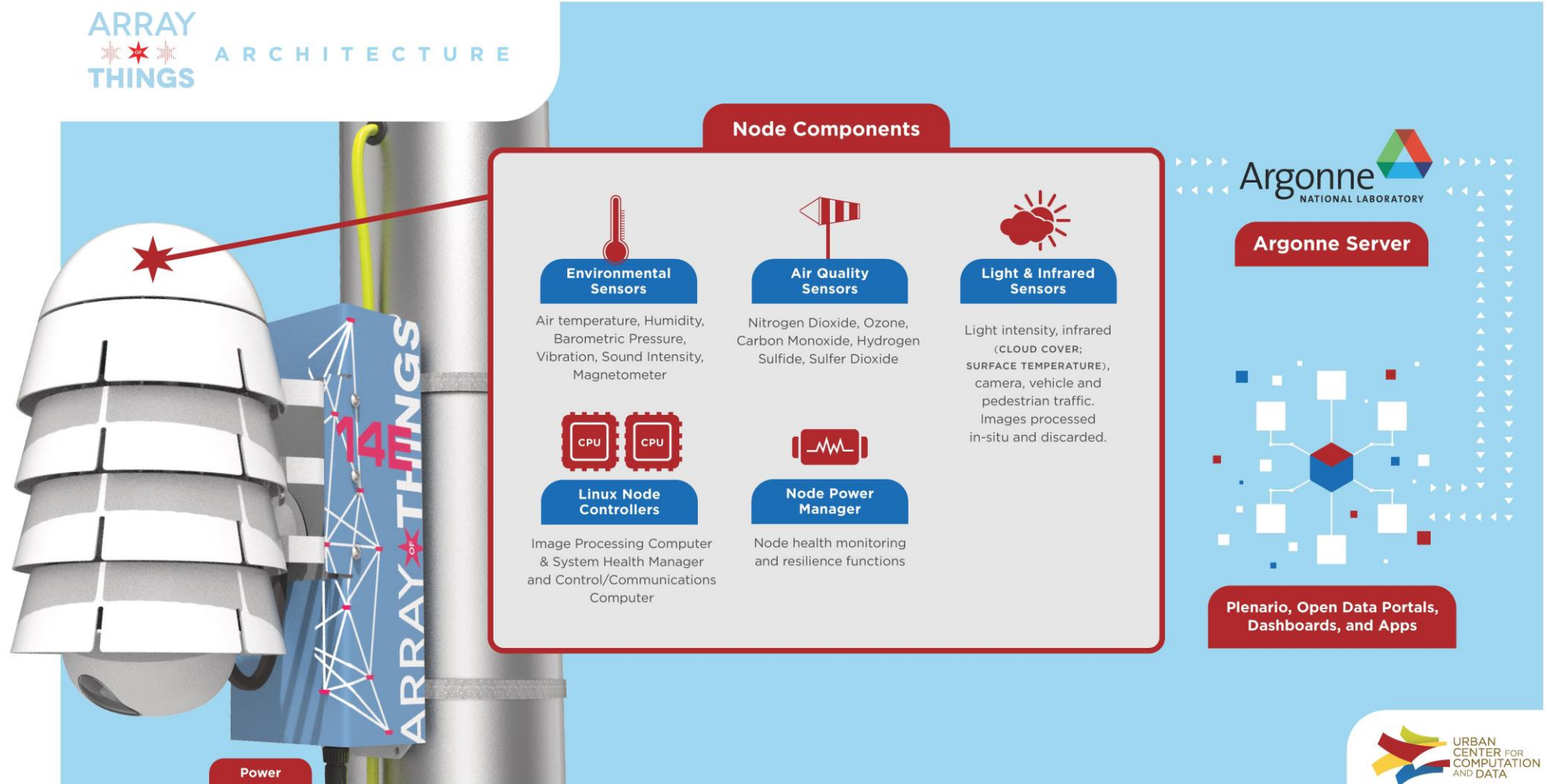


Image from <https://arrayofthings.github.io/>

Surveillance (?) of Street Corners

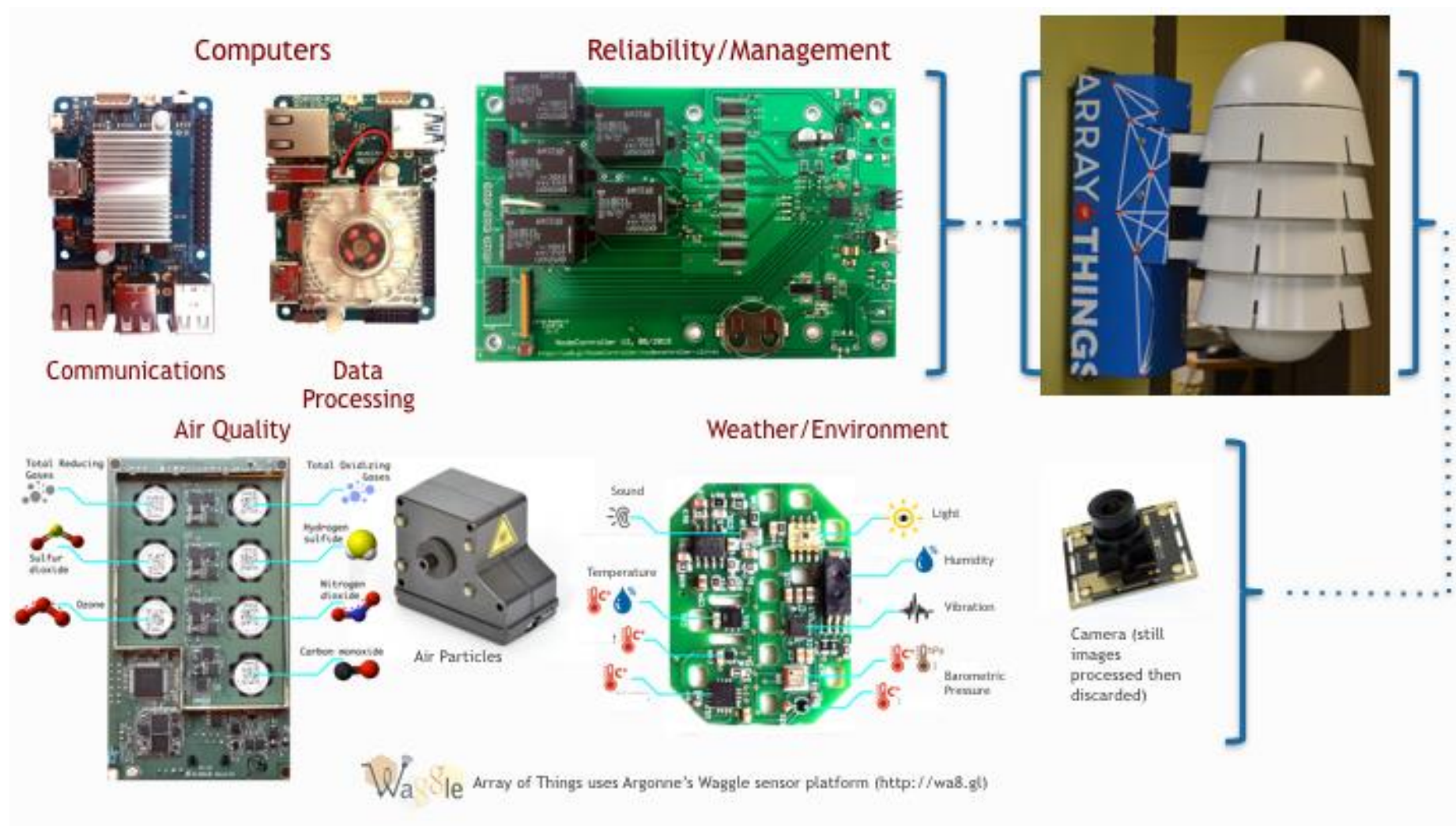


Image from <https://arrayofthings.github.io/>

Surveillance of a Population

Tracking Chicago Juveniles

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

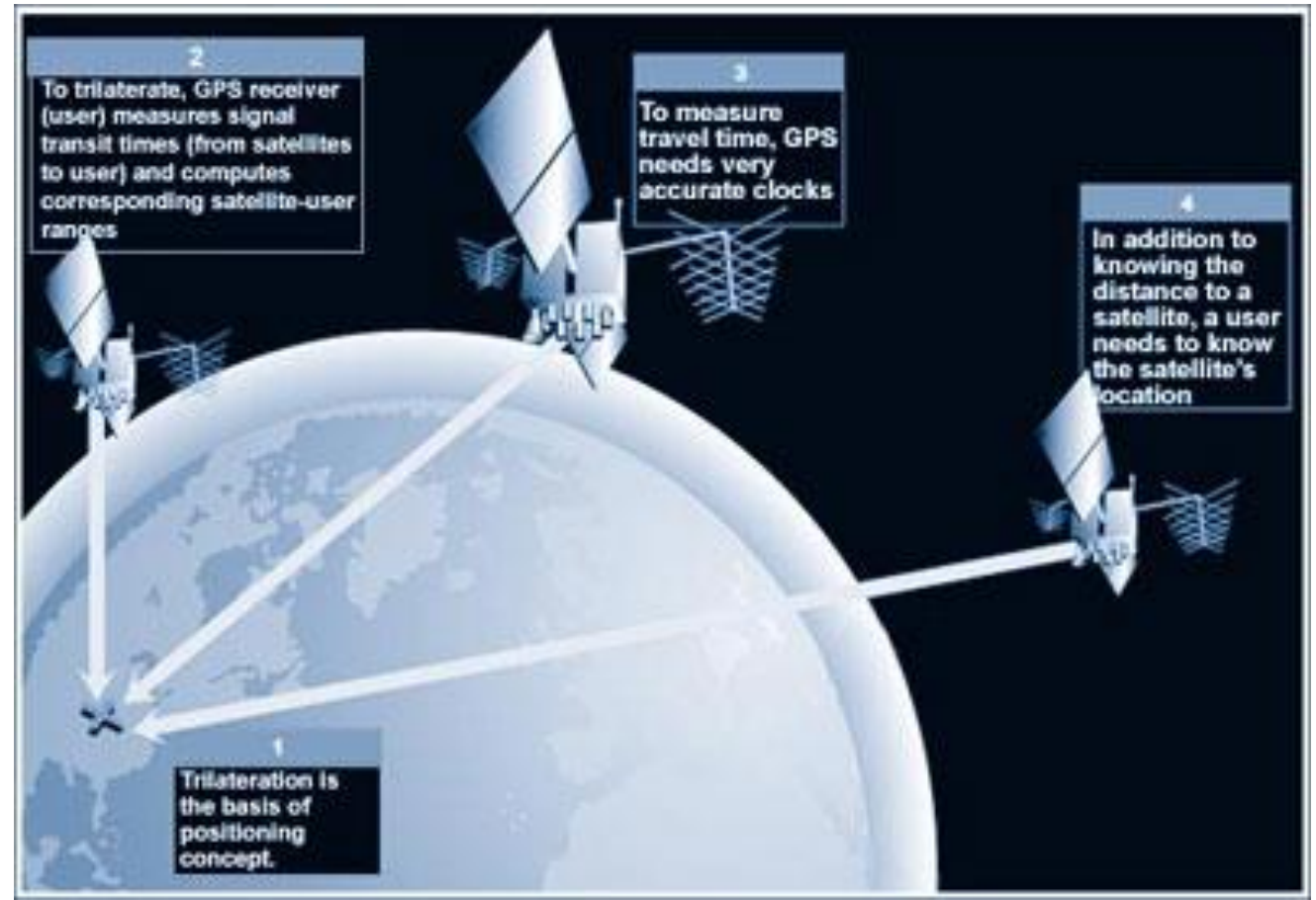
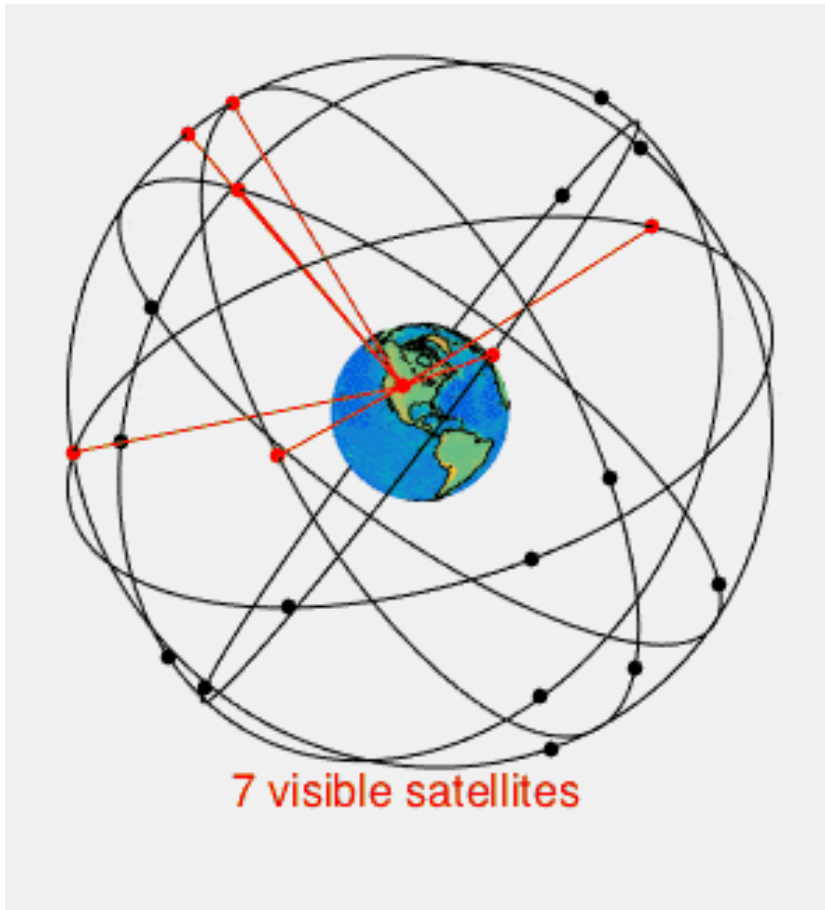
Cook County has a new contract for juvenile ankle monitors that critics say are an invasion of privacy.

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

- “China’s Social Credit System (SCS, 社会信用体系 or shehui xinyong tixi) is expected to become the first digitally-implemented nationwide scoring system with the purpose to rate the behavior of citizens, companies, and other entities... “good” behavior can result in material rewards and reputational gain while “bad” behavior can lead to exclusion from material resources and reputational loss.”
 - Redlist = “information on “good” behavior”
 - Blacklist = “information on “bad” behavior”

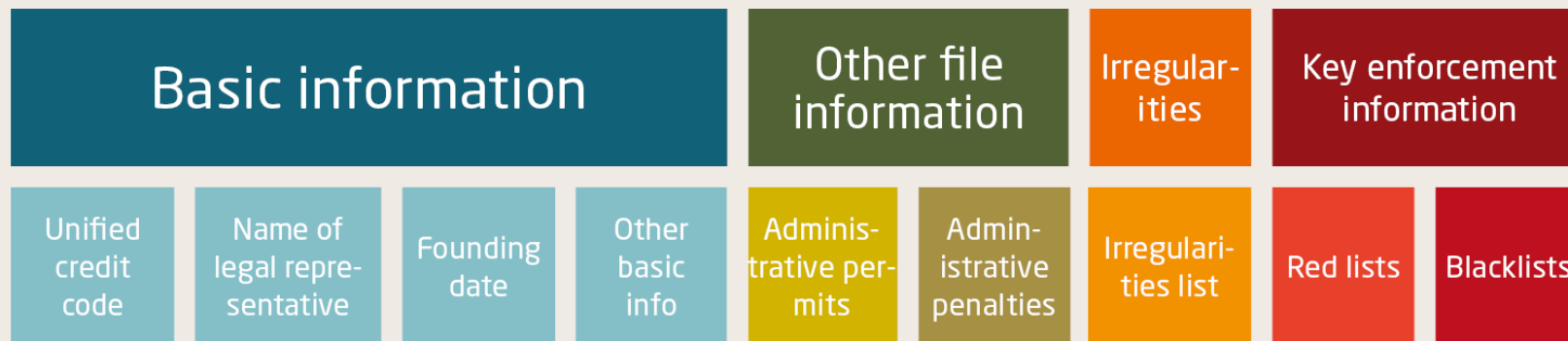
Social Credit System in China

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

数据来源：	证监会
数据类别：	市场禁入
主体名称：	吴[REDACTED]
加密证件号码：	110104*****4X
证件类型：	身份证
个人代码：	
处罚处理名称：	证监法律字[2006]12号 市场禁入决定书（梁[REDACTED]、吴[REDACTED]、孙[REDACTED]）
处罚处理日期：	2006/11/27
处罚处理种类：	市场禁入(5年)
处罚对象类型（1组织机构，2个人）：	
真实证件号码：	
信息类型：	
处罚机关：	中国证监会
处罚决定书id：	
处罚处理内容：	证监法律字[2006]12号市场禁入决定书当事人：梁[REDACTED]女，1948年出生，北京中兴信托投资有限公司（以下简称中兴信托）法定代表人、健富投资有限公司（以下简称健富投资）法定代表人，住址北京市东城区前门东大街1号2单元207号。吴[REDACTED]女，1949年出生，中兴信托北京亚运村营业部经理、健富投资经理，住址北京市朝阳区北四环东路106号3号楼1804号。孙[REDACTED]男，1942年出生，健富投资顾问，住址北京市东城区前门东大街1号2单元207号。依据原《中华人民共和国证券法》（以下简称《证券法》）的有关规定，本会对中兴信托北京亚运村营业部等机构违反证券法律法规行为进行了立案调查、审理，并依法向当事人告知了实施市场禁入措施的事实、理由及依据及当事人依法享有的权利，现已调查、审理终结。经查明，自2000年4月20日起，健富投资在中兴信托北京营业部开设并控制“健富公司”、“华健经贸”、“华健发展”、“兴发机械”、“兴发广告”、“国利通达”、“张[REDACTED]”、“孙[REDACTED]”、“孙[REDACTED]”、“孙[REDACTED]”、“孙[REDACTED]”、“张[REDACTED]”等资金账户，下挂个人股东账户842个，买卖证券。上述事实，有相关账户开户资料、客户对账单、资金划转凭据、情况说明等证据在案证实，证据确实、充分，足以认定。健富投资的上述行为违反了原《证券法》第七十四条“在证券交易中，严禁法人以个人名义开立账户，买卖证券”的规定，构成了原《证券法》第一百九十条所述“违反本法规定，法人以个人名义设立账户买卖证券”的行为。根据当事人违法行为的事实、性质、情节与社会危害程度，依据《证券市场禁入暂行规定》第二条第七项等相关规定，本会决定认定当事人梁[REDACTED]、吴[REDACTED]、孙[REDACTED]为市场禁入者，自本会宣布决定之日起5年内不得担任上市公司高级管理人员和从事证券业务。二〇〇六年十一月二十七日

Figure 3: An entry from the Blacklist of “Securities Market Entry Prohibition”. The first column, from top to down: the first arrow points to “name of punishment” and the second points to “content of punishment”. The table on the right side of the second arrow shows the detailed explanation of the punishment.

Image from Engelmann et al. Clear Sanctions, Vague Rewards: How China’s Social Credit System Currently Defines “Good” and “Bad” Behavior. In *Proc. FAT* 2019*.

Social Credit System in China

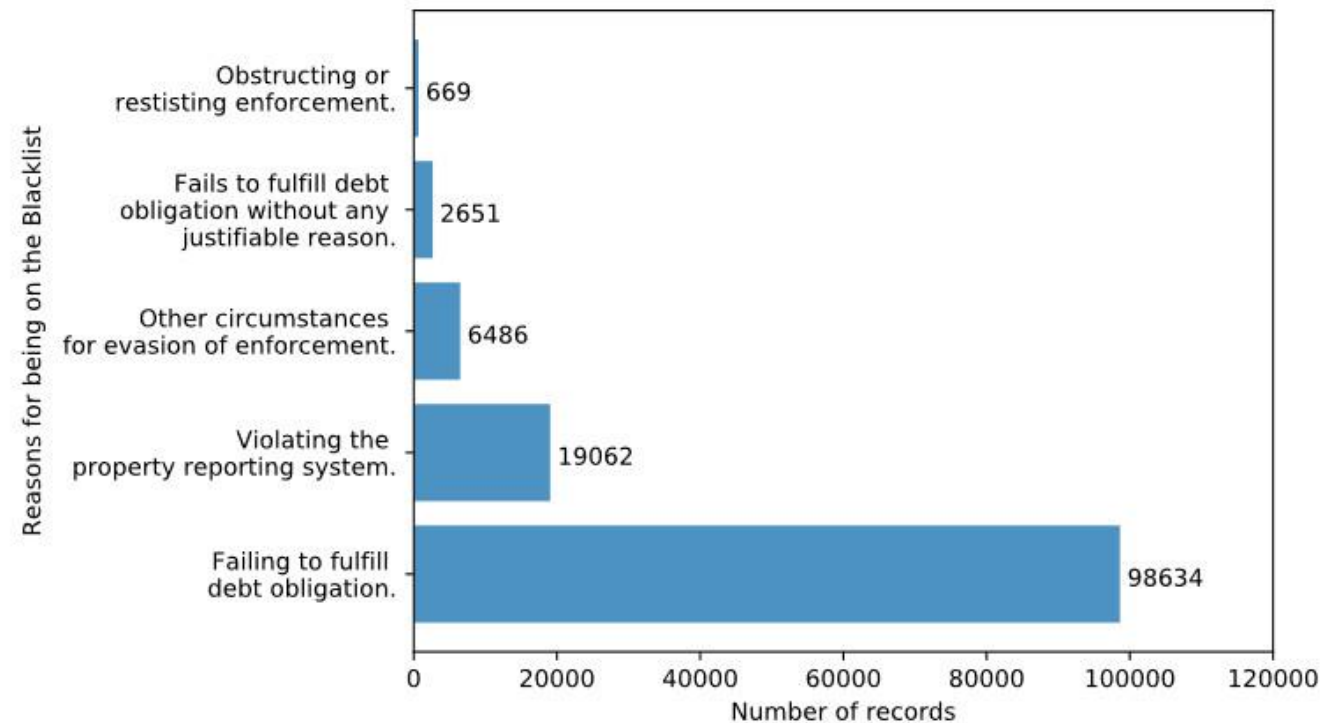


Figure 4: The top 5 reasons for being on the Blacklist of company debtors.

Image from Engelmann et al. Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines "Good" and "Bad" Behavior. In *Proc. FAT* 2019*.

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

💬 f 🐦

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

<https://www.engadget.com/2018-11-22-chinese-facial-recognition-confuses-bus-ad-with-jaywalker.html>

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

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

Surveillance at Borders

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

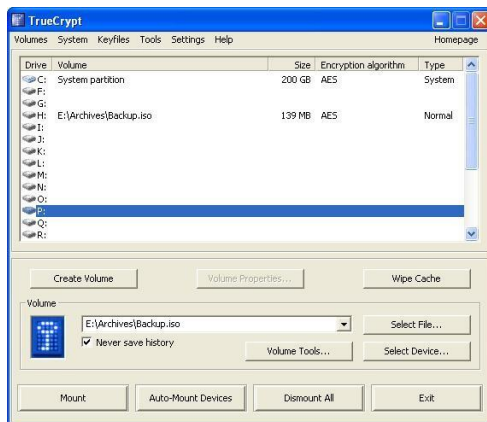
When Andreas Gal returned from a business trip in Sweden last fall, he was carrying two company-owned devices: an iPhone XS that flashed “Confidential and Proprietary” on its lock screen and a MacBook Pro bearing a sticker that read “PROPERTY OF APPLE. PROPRIETARY.”

<https://www.washingtonpost.com/technology/2019/04/03/apple-employee-detained-by-us-customs-agents-after-declining-unlock-phone-laptop/>

Phones in the Legal System

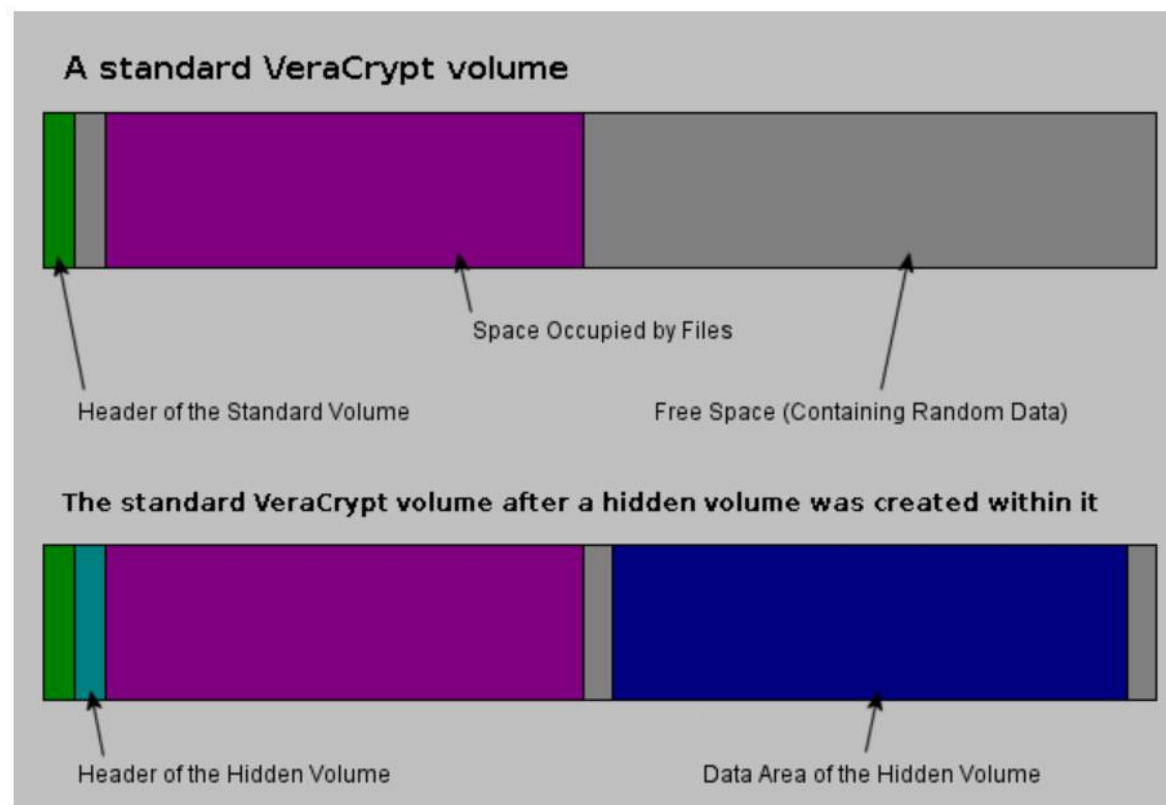
- Riley v. California
 - SCOTUS 2014
- Unanimous ruling that **warrantless** search of a phone during an arrest is unconstitutional
- Fifth Amendment from the Bill of Rights: Speech cannot be compelled
 - Many (but not all) courts consider passwords to be “speech”
 - Biometrics are not considered speech

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.

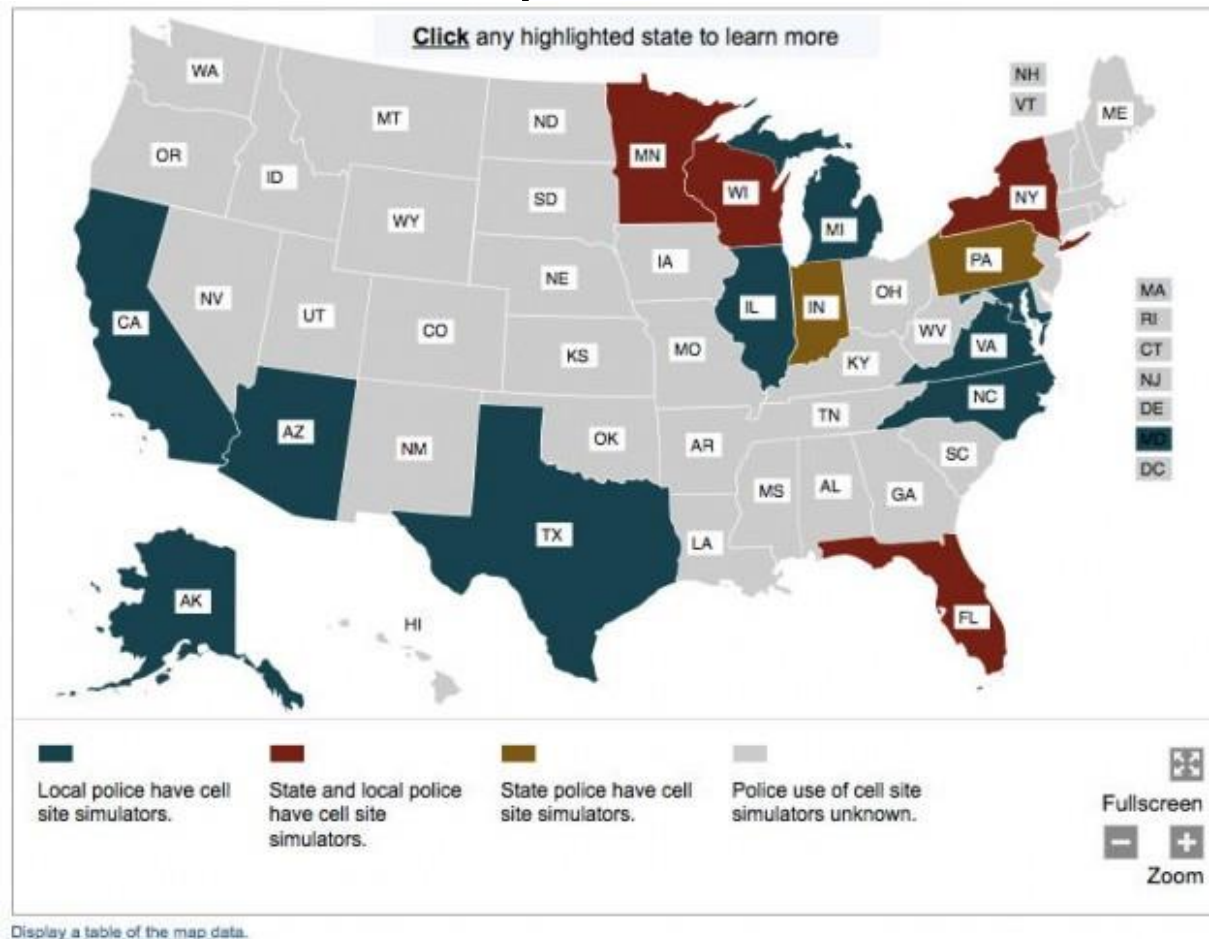


The layout of a standard VeraCrypt volume before and after a hidden volume was created within it.

Surveillance of Activism

Mobile Devices

- Stingrays (cell site simulator)



FBI Surveillance of Activists

The Intercept_


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-

<https://theintercept.com/2019/10/29/fbi-surveillance-black-activists/>

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





BLACK
LIVES
MATTER

NO JUSTICE
NO PEACE
PROSECUTE
THE POLICE
#BLM

AT
1

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

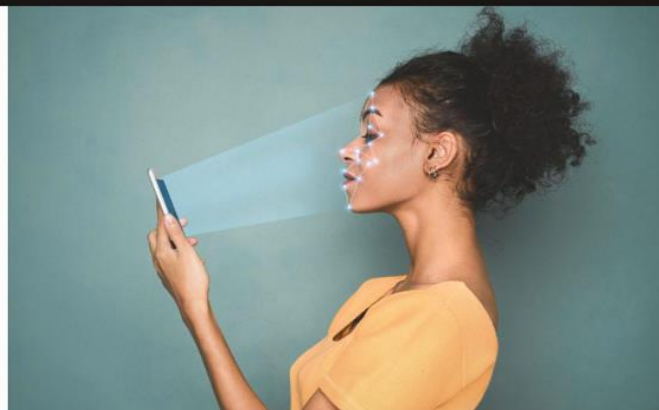
Anything you don't want to be arrested with



Contact lenses



Forbes



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 sharple on your body
be careful in case they are identified.

2. med bracelett

3. turn location/cellular data off.
enable emergency SOS.

4. passcode only option.

5. ductape camera
in case you have to secretly record eviden

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

AMNESTY
INTERNATIONAL



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



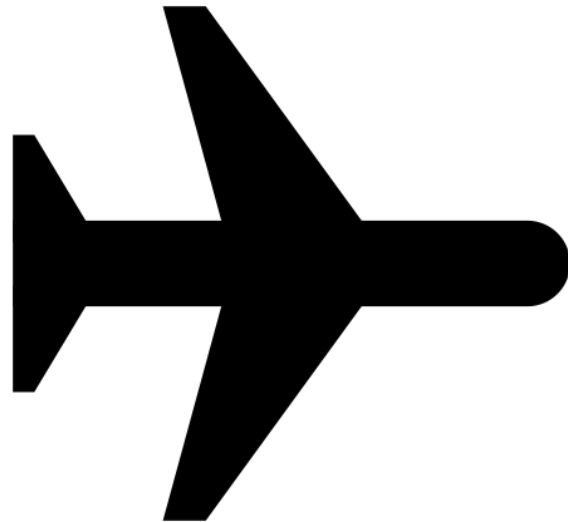
- + Freedom of Expression and Assembly: Everyone has the right to carry their opinion to the streets.
- + Protection of the Right to Freedom of Assembly: Law enforcement must facilitate and not restrict a peaceful public assembly.
- + Freedom from excessive use of force: In the policing of non-violent 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

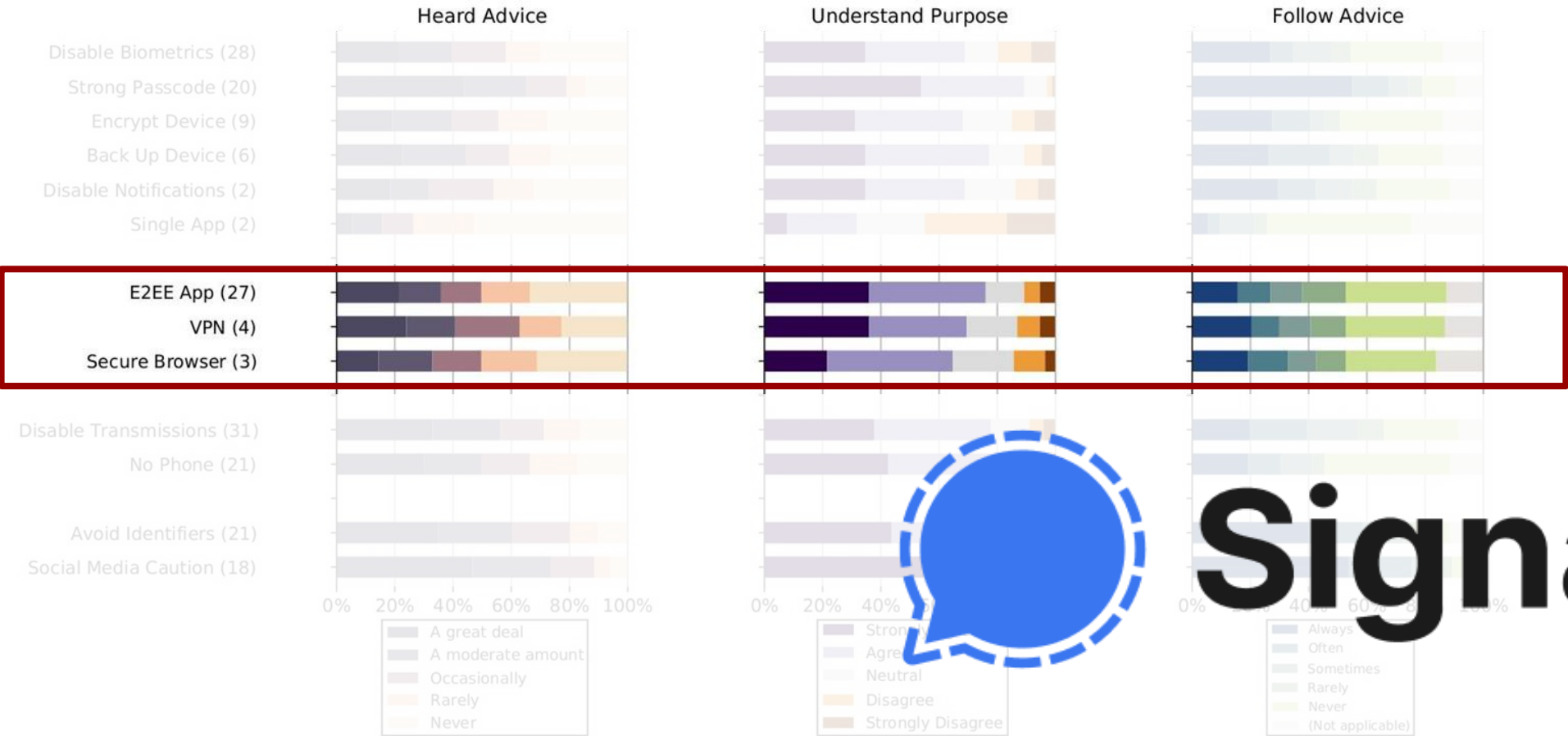


Using a strong passcode

- 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."

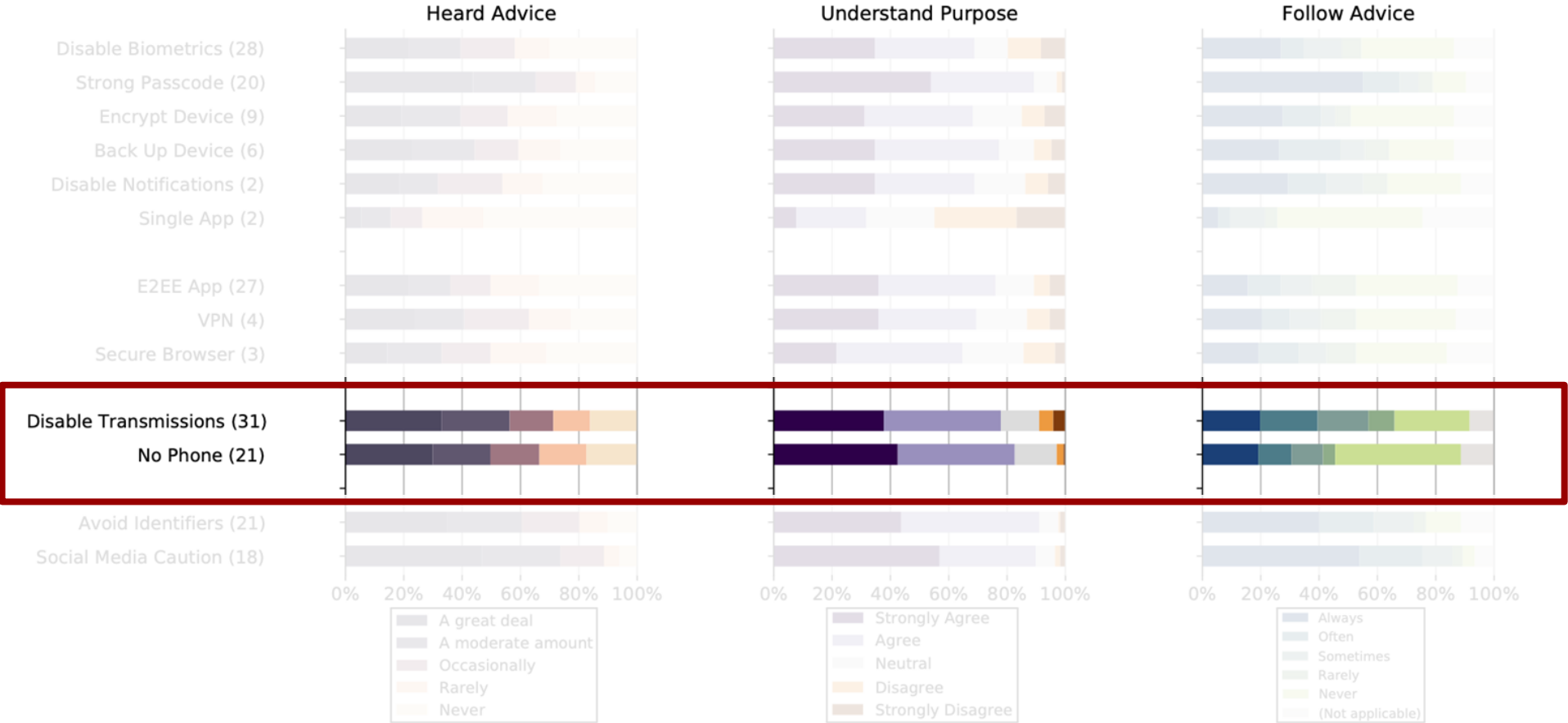
(b) "I feel that I understand the purpose of this advice about attending a protest."

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



Signal

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.

Virtual Meetings

1.888.799.9666

Webinars

Recordings

Settings

Account Profile

Reports

[Attend Live Training](#)

Reports

Usage

Usage

From: 05/19/2021

To: 05/25/2021

Search

JOIN A MEETING

HOST A MEETING



Maximum report duration: 1 Month

The report displays information for meetings that ended at least 15 minutes ago.

Export as CSV File

Toggle columns

Topic	Meeting ID	User Name	User Email	Department	Group	Has Zoom Rooms?	Creation Time	Start Time	End Time	Duration (Minutes)	Participants	Source
CS 259 (Spring 2021)		Blase Ur (he/him)	blase@uchicago.edu	Computer Sci	22	No	03/25/2021 03:59:57 PM	05/20/2021 02:39:22 PM	05/20/2021 04:01:52 PM	83	30	Zoom
							03/25/2021 03:59:57 PM	05/20/2021 02:39:22 PM	05/20/2021 04:01:52 PM			

Virtual Meetings

