Say something interesting about me

Gabriele Zanoni

@infoshaker

Who's Who

Gabriele Zanoni
@infoshaker

Cloud Security

Penetration testing

Incident Response

Anti-Fraud

Computer Forensics

Mobile Security

Let’s start from your identity: a true story.

Chloe is an investigative journalist working for an international broadcast service; we will call the TV show she works for The Inquirer.

Upon arriving in the country [West Africa] Chloe buys a local SIM card. She will be using this to communicate with her sources.

She makes phone calls to her sources telling them clearly who she is, who she works for and what she is trying to achieve.

One day, Chloe needs to meet with a source. She uses her local phone to order a cab from a cab company. Her number is shared with the driver, who calls her to confirm he has arrived. When she enters the cab, the driver greets her “So… you work for The Inquirer?”

https://privacyinternational.org/case-study/2997/betrayed-app-she-had-never-heard-how-truecaller-endangering-journalists

What happened

The driver points at his phone. Her number is registered on the driver's phone as "Chloe The Inquirer Journalist."

What happened to Chloe is that one of her sources was using TrueCaller. She called her source and after they hung up, TrueCaller offered the source the option to tag Chloe's number, since the number was not in their database. The source did not see the potential for harm and tagged Chloe's number as "Chloe The Inquirer Journalist." Now every time Chloe makes a phone call using that phone number, her name appears to TrueCaller users, like the cab driver, as "Chloe The Inquirer Journalist."

https://privacyinternational.org/case-study/2997/betrayed-app-she-had-never-heard-how-truecaller-endangering-journalists

Metadata analysis from phone calls 1/2

- An experiment from Jonathan Mayer
- “Participants run the **MetaPhone** app on their Android smartphone; it submits device logs and social network information for analysis.”
- “We began by identifying the MetaPhone participants’ contacts. We used the same approach as in our prior work on number identifiability, matching phone numbers against the public Yelp and Google Places directories. In total, our 546 participants contacted 33,688 unique numbers. 6,107 of those numbers (18%) resolved to an identity.”

http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

Metadata analysis from phone calls 2/2

Category	Participants
Health Services	57%
Financial Services	40%
Pharmacies	30%
Veterinary Services	18%
Legal Services	10%
Recruiting and Job Placement	10%
Religious Organizations	8%
Firearm Sales and Repair	7%
Political Officeholders and Campaigns	4%
Adult Establishments	2%
Marijuana Dispensaries	0.4%

Category	Participants with ≥ 1 Calls
Dentistry and Oral Health	18%
Mental Health and Family Services	8%
Ophthalmology and Optometry	6%
Sexual and Reproductive Health	6%
Pediatrics	5%
Orthopedics	4%
Chiropractic Care	3%
Rehabilitation and Physical Therapy	3%
Medical Laboratories	2%
Emergency or Urgent Care	2%
Cardiology	2%
Dermatology	1%
Ear, Nose, and Throat	1%
Neurology	1%
Oncology	1%
Substance Abuse	1%
Cosmetic Surgery	1%

http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

Metadata analysis from phone calls: Pattern Results

- “A pattern of calls will often, of course, reveal more than individual call records. ”
  - Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis.
  - Participant B spoke at length with cardiologists at a major medical center, talked briefly with a medical laboratory, received calls from a pharmacy, and placed short calls to a home reporting hotline for a medical device used to monitor cardiac arrhythmia.
  - Participant C made a number of calls to a firearm store that specializes in the AR semiautomatic rifle platform. They also spoke at length with customer service for a firearm manufacturer that produces an AR line.
  - In a span of three weeks, Participant D contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop.
  - Participant E had a long, early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after.

http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

Bonus topic: deepfake with your data!

Who might have interest in such data?

Who might have interest in such data?

Do you want a bank loan?

…Or an insurance?

Never Give Stores Your ZIP Code!

«Users simply capture name from the credit card swipe and request a customer's ZIP code during the transaction. GeoCapture matches the collected information to a comprehensive consumer database to return an address." In a promotional brochure, they claim accuracy rates as high as 100%»

Adam Tanner Contributor ⓘ

I write about the business of personal data.

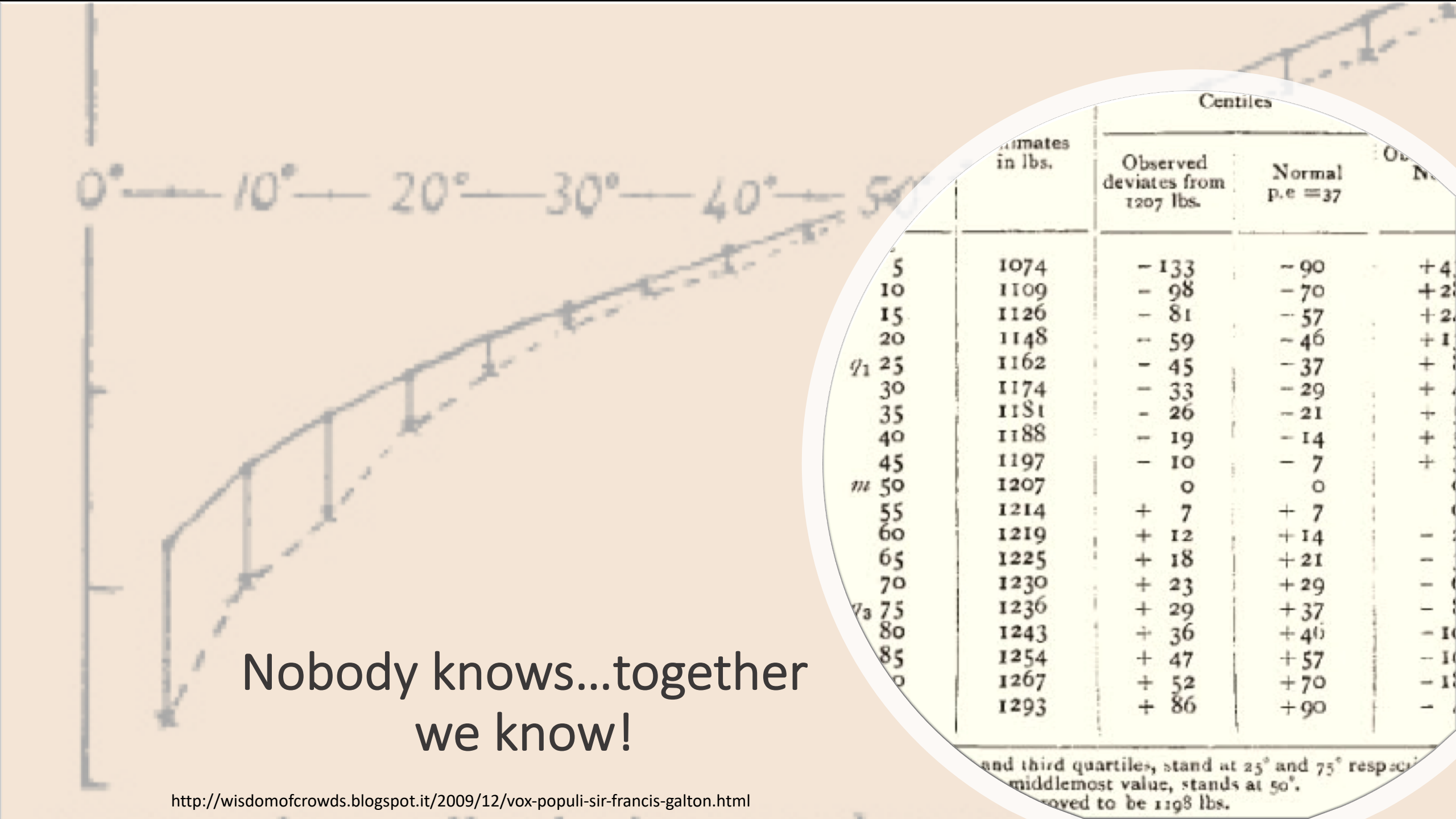
Why do merchants sometimes ask us for our ZIP code when we buy something?

(AP Photo/Julie Jacobson)

I recently visited the Mob Museum in Las Vegas, an interesting addition to Sin City's attractions. I paid my admission with a credit card, prompting the museum ticket seller to ask me: "What's your ZIP code?"

When I paused for a moment, she added: "It's for marketing purposes."

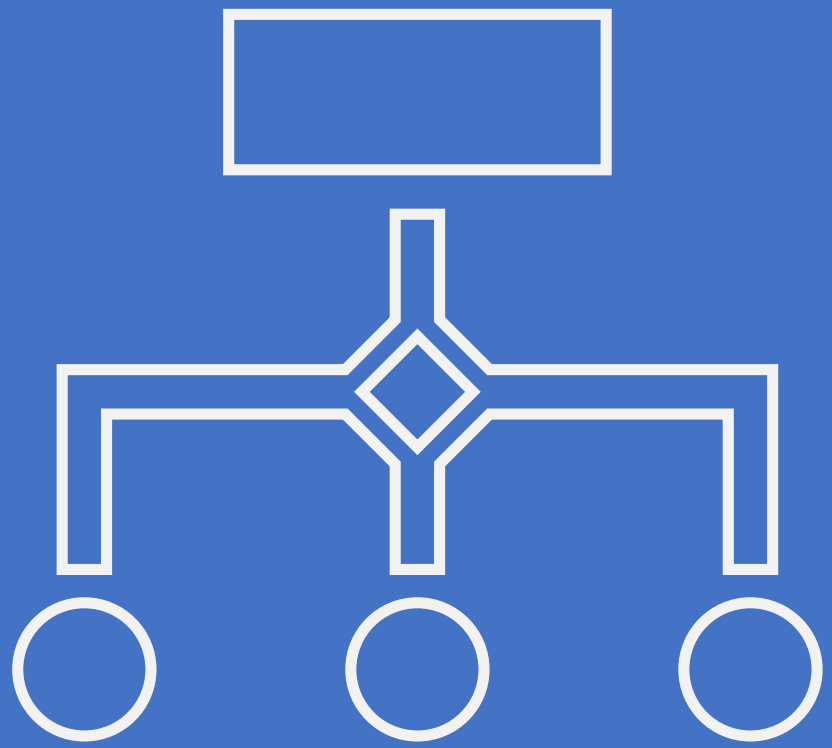
https://www.forbes.com/sites/adamtanner/2013/06/19/theres-a-billion-reasons-not-to-give-stores-your-zip-code-ever/#4f63b4f4786f



http://wisdomofcrowds.blogspot.it/2009/12/vox-populi-sir-francis-galton.html

Is it just an idea (?)

- “For the past three years, Elaine Rich and 3,000 other average people have been quietly making probability estimates about everything from Venezuelan gas subsidies to North Korean politics as part of , an experiment put together by three well-known psychologists and some people inside the intelligence community.”
- “According to one report, the predictions made by the Good Judgment Project are often better even than intelligence analysts with access to classified information, and many of the people involved in the project have been astonished by its success at making accurate predictions.”



http://www.npr.org/blogs/parallels/2014/04/02/297839429/-so-you-think-youre-smarter-than-a-cia-agent

http://www.goodjudgmentproject.com/

Location determination techniques

Examples:

- WIFI related data can be used to determine your location. You only need to match MAC addresses with a map of known Access Points.
- Battery consumption can be used to identify your movements
- **It might be obvious but apps for taxi services/maps/health etc.. could have a history of your preferred places.**

http://www.zdnet.com/article/how-google-and-everyone-else-gets-wi-fi-location-data/
http://www.theregister.co.uk/2015/02/23/mobe_battery_stats_the_latest_tracking_trick_for_spies_creeps/
http://www.ibtimes.com/spying-celebrities-nyc-taxi-metadata-exposes-celeb-locations-strip-club-clients-1696744?rel=rel1

Tracking Metro Riders Using Accelerometers

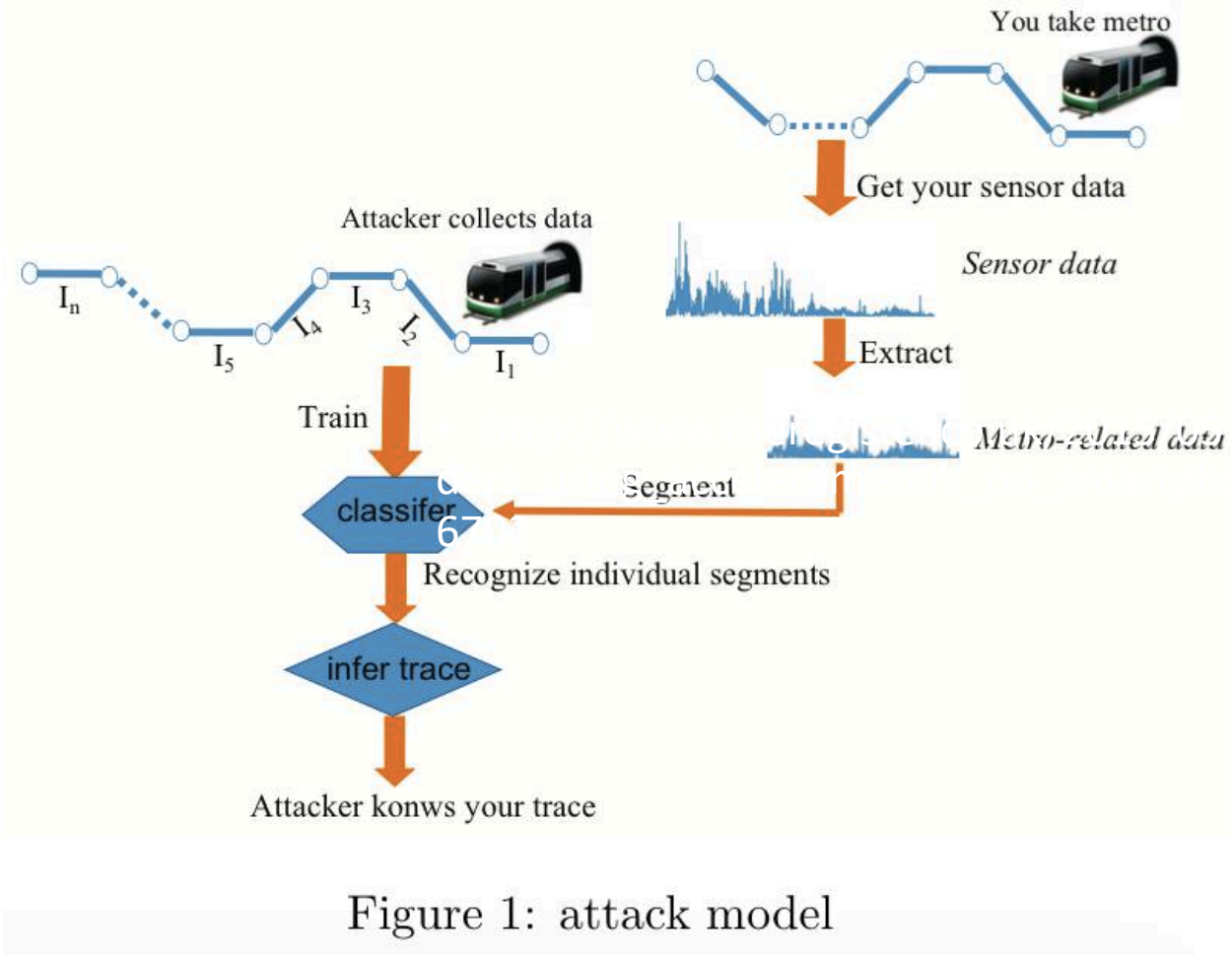
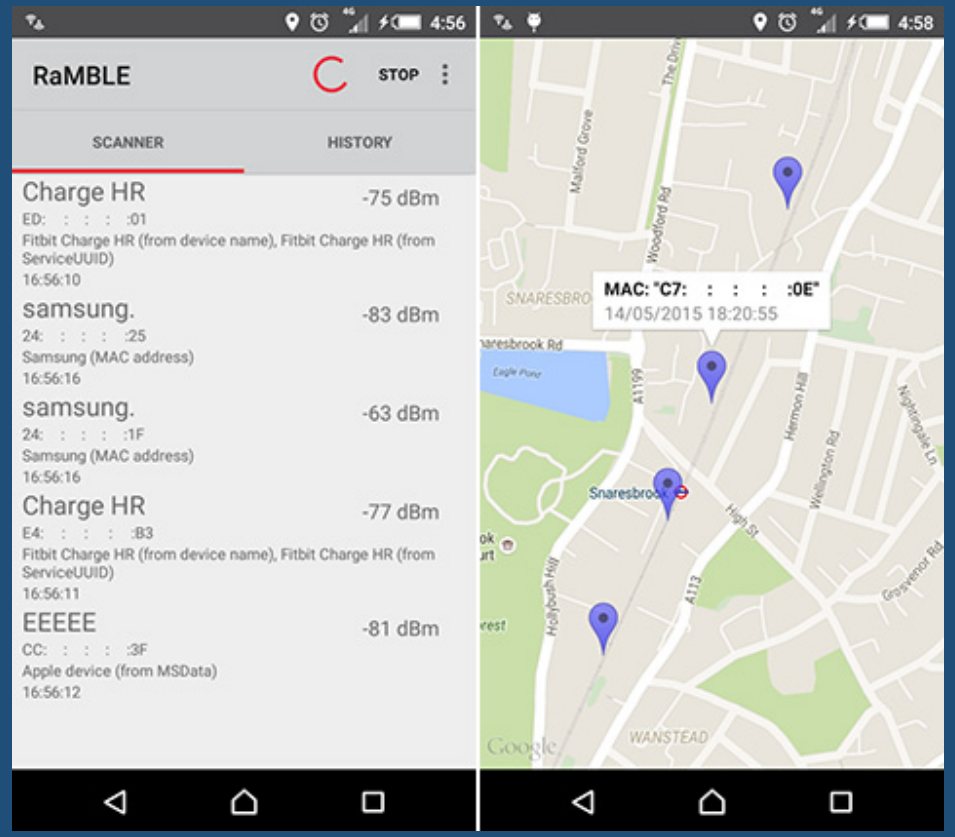


Figure 1: attack model

http://www.theregister.co.uk/2015/05/26/tracking_metro_riders_using_accelerometers_on_smartphones/?mt=1462545176702

Sniffing and tracking wearable tech and smartphones

- “Researchers at Context Information Security have demonstrated how easy it is to monitor and record Bluetooth Low Energy signals transmitted by many mobile phones, wearable devices and iBeacons, including the iPhone and leading fitness monitors, raising concerns about privacy and confidentiality. ”



https://www.helpnetsecurity.com/2015/05/25/sniffing-and-tracking-wearable-tech-and-smartphones/

It’s happening also here!

- https://telesia.it/privacy

- Il Dispositivo è costituito da un Single Board Computer dotato di adattatore di rete ethernet 802.3 e adattatore di rete WiFi 802.11(b/g/n) operante nella banda di frequenze dei 2.4 Ghz, è prodotto da terze parti, è normalmente in commercio e dispone delle certificazioni di legge.
- **Il Dispositivo è dotato di una serie di procedure informatiche che realizzano il conteggio anonimo di terminali, mobili e non, presenti nell'area circostante l'ubicazione del dispositivo stesso e dotati a loro volta di un adattatore di rete WiFi 802.11(b/g/n) operante nella banda di frequenze dei 2.4 Ghz.**

Telesia opera da oltre 20 anni nel settore della telematica multimediale, offrendo prodotti e servizi a tutte le aziende pubbliche e private che desiderano dotarsi di un sistema di audio-videocomunicazione.

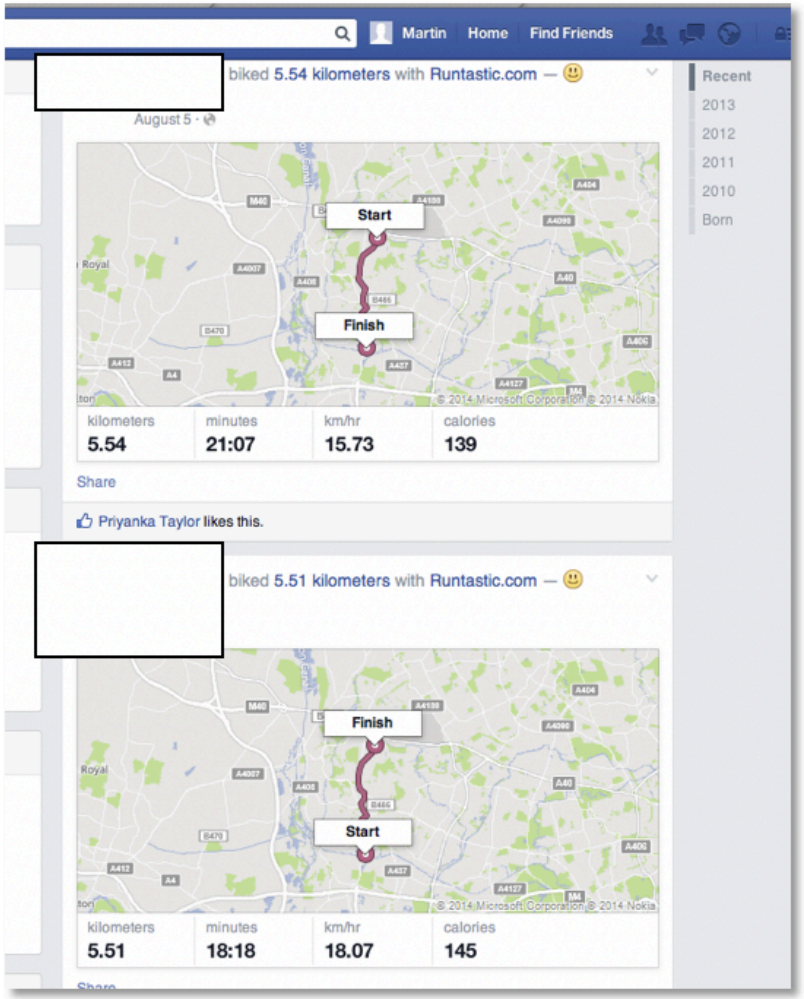
La consolidata esperienza nel **digital broadcasting** ha permesso a Telesia di realizzare numerosi progetti integrati di videoinformazione per il pubblico, che attualmente sono operativi presso **tutti i principali aeroporti italiani,** le metropolitane di **Roma**, **Milano** e **Brescia**, a bordo degli **autobus di Milano** e dei **treni della metro di Roma**.

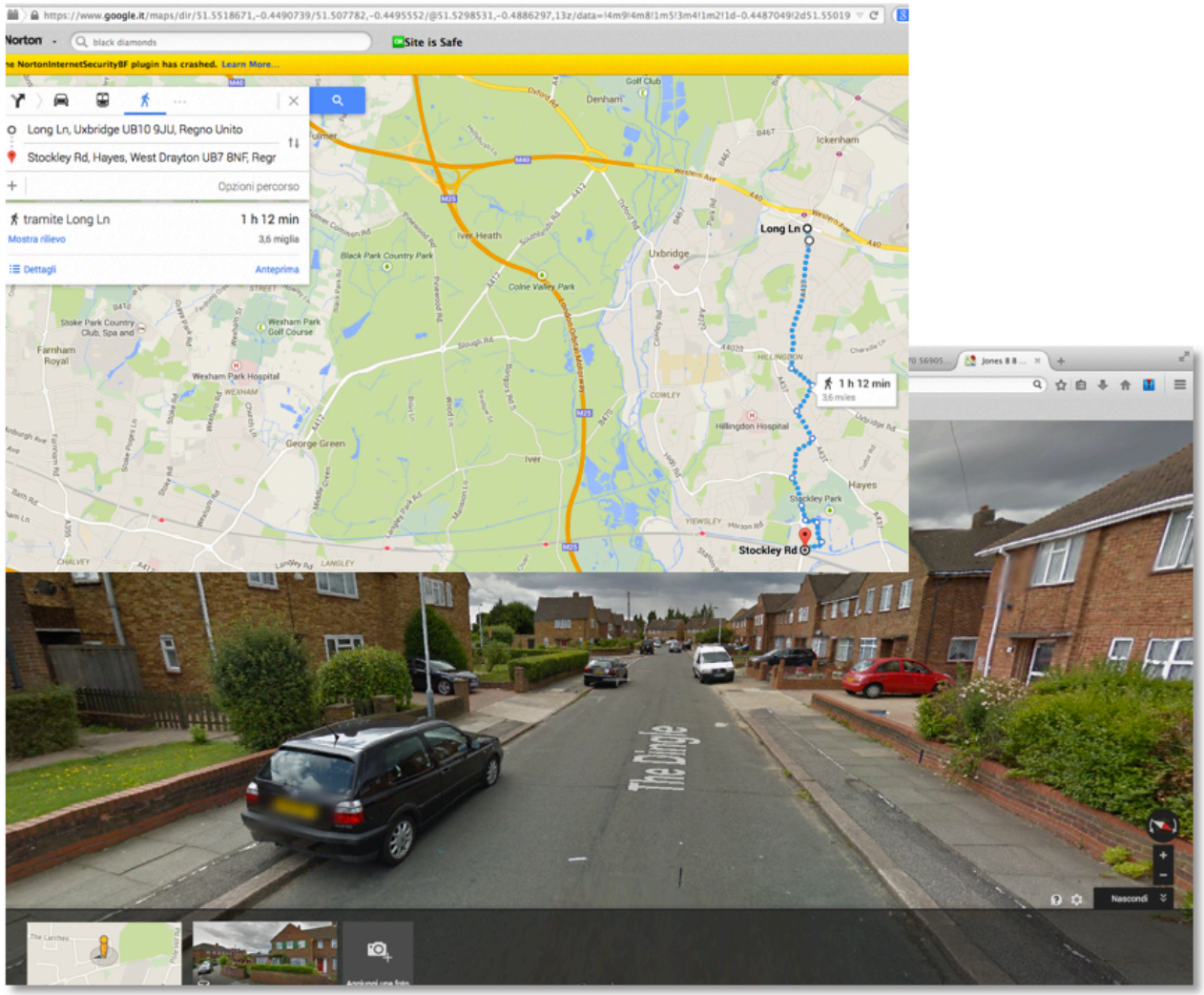
Strava app «leaking» military bases locations

- **Security concerns have been raised after a fitness tracking firm showed the exercise routes of military personnel in bases around the world.**
- Online fitness tracker Strava has published a "heatmap" showing the paths its users log as they run or cycle.
- It appears to show the structure of foreign military bases in countries including Syria and Afghanistan as soldiers move around them.

https://www.bbc.com/news/technology-42853072

So where do you live?





Iot war it’s just at the beginning

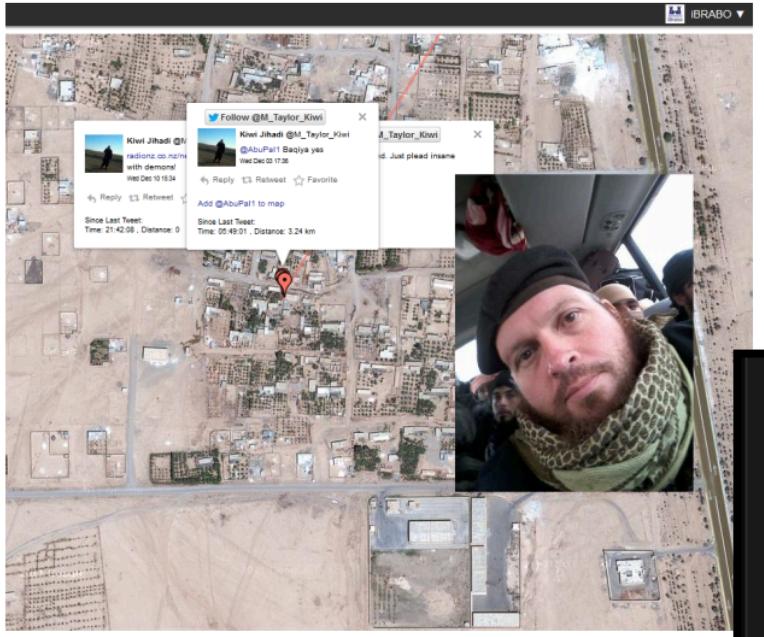
“DJI drones automatically tag GPS imagery and locations and register **facial recognition** data even when the system is off, and access users’ phone data.

Additionally, the applications capture user information including email addresses, full names, phone numbers and other credentials. And, of course, **images and video captured by the drones are also collected and transmitted back to cloud-based servers operated by DJI in Taiwan, China, and Hong Kong**. DHS said that the Chinese government “most likely has access” to the data stored on those servers.

SIP Los Angeles assesses with high confidence a foreign government with access to this information could easily coordinate physical or cyber attacks against critical sites.

https://publicintelligence.net/ice-dji-china/

So you forgot to remove the geo-tag ?



NEW ZEALAND JIHADIST DELETES TWEETS AFTER DISCOVERING HE LEFT GEOTAGGING ON

Feds Use Instagram To Arrest Over 350 Drug Dealers & Seize $7 Million In One Weekend?!

APRIL 05, 2014 WORD ON DA STREET 0 COMMENTS

SMH…these idiots just never learn!? The DEA used drug dealer's narcissistic need to post all their incriminating pictures on Instagram for "likes" to their advantage this weekend and made a record-breaking number of arrests and seizures. One drug dealer was even dumb enough to brag about how police would never catch him, yet geotagged the exact location of his drug warehouse so that police where easily able to find him! Read the rest of this not-so-bright criminal's story below…..

The Federal Government has no problem using every tool at its disposal to catch criminals in action. After noticing an extremely large number of criminals using *Instagram* to show off their drugs, money, and expensive purchases, the Drug Enforcement Agency (DEA) teamed up with the Federal Bureau of Investigations (FBI) to set up sting operations to take down criminals.

- https://ibrabo.wordpress.com/2014/12/30/new-zealand-jihadist-deletes-tweets-after-discovering-he-left-geotagging-on/
- http://wordondastreet.com/feds-use-instagram-arrest-350-drug-dealers-seize-7-million-one-weekend/

Connecting dots…

- This image, which was provided by an analyst who prefers not to be named publicly (but whose identity we have independently verified), shows an Uber receipt addressed to a user called ‘Qiang’ (强) and bears the e-mail address 420192[at]qq.com, an account that we believe to be used by APT10 actor Gao Qiang.

https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/

Knowing the attackers: APT28

Compile Times Align with Working Hours in Moscow and St. Petersburg

Of the 140 malware samples that we have attributed to APT28 so far, over 89% were compiled between 0400 and 1400 UTC time, as depicted in Figure 10. Over 96% were compiled between Monday and Friday. This parallels the working hours in UTC+0400 (that is, compile times begin about 8AM and end about 6PM in this time zone). This time zone includes major Russian cities such as Moscow and St. Petersburg.

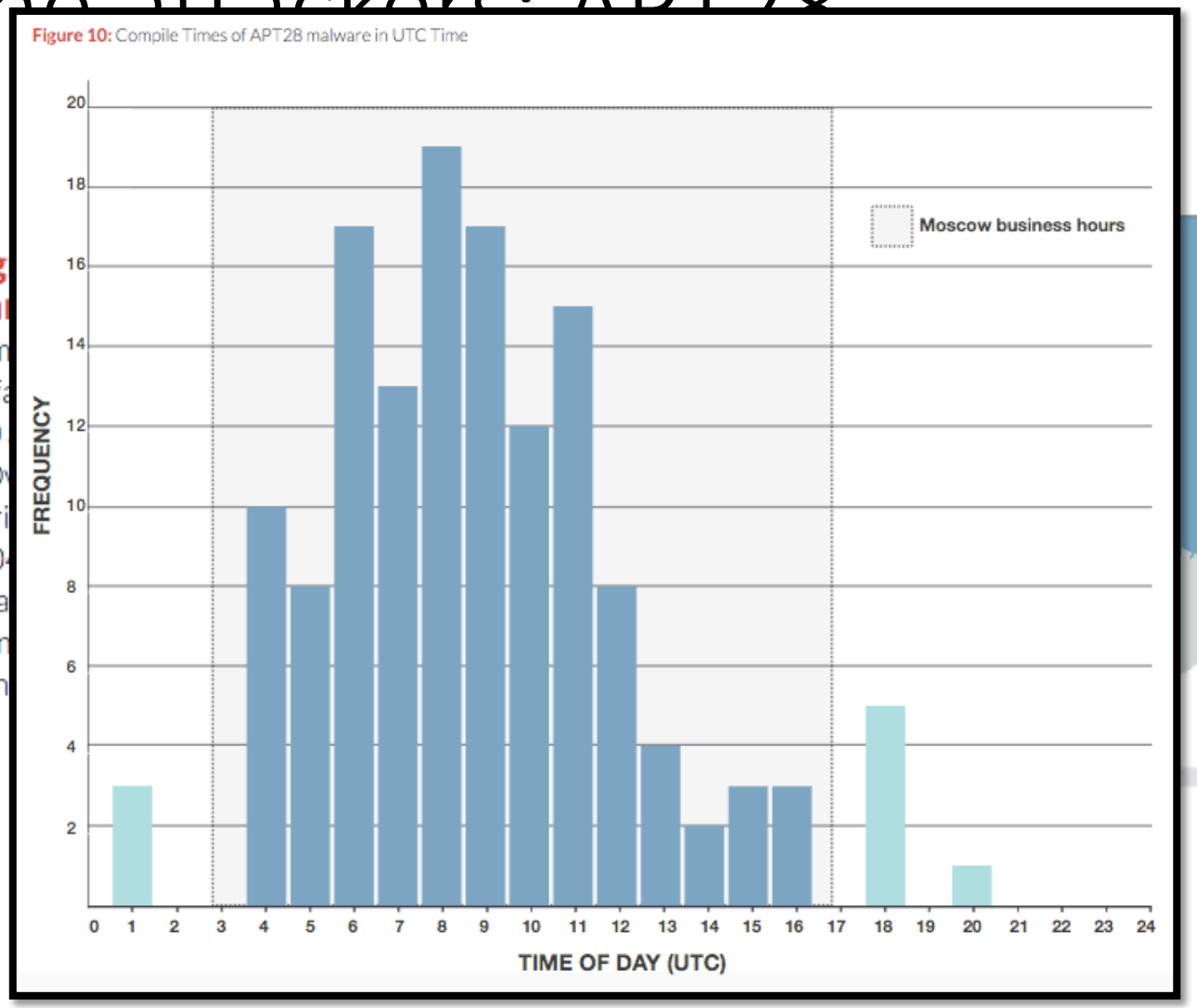
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

Knowing the attackers: APT28

Compile Times Alig
Hours in Moscow a

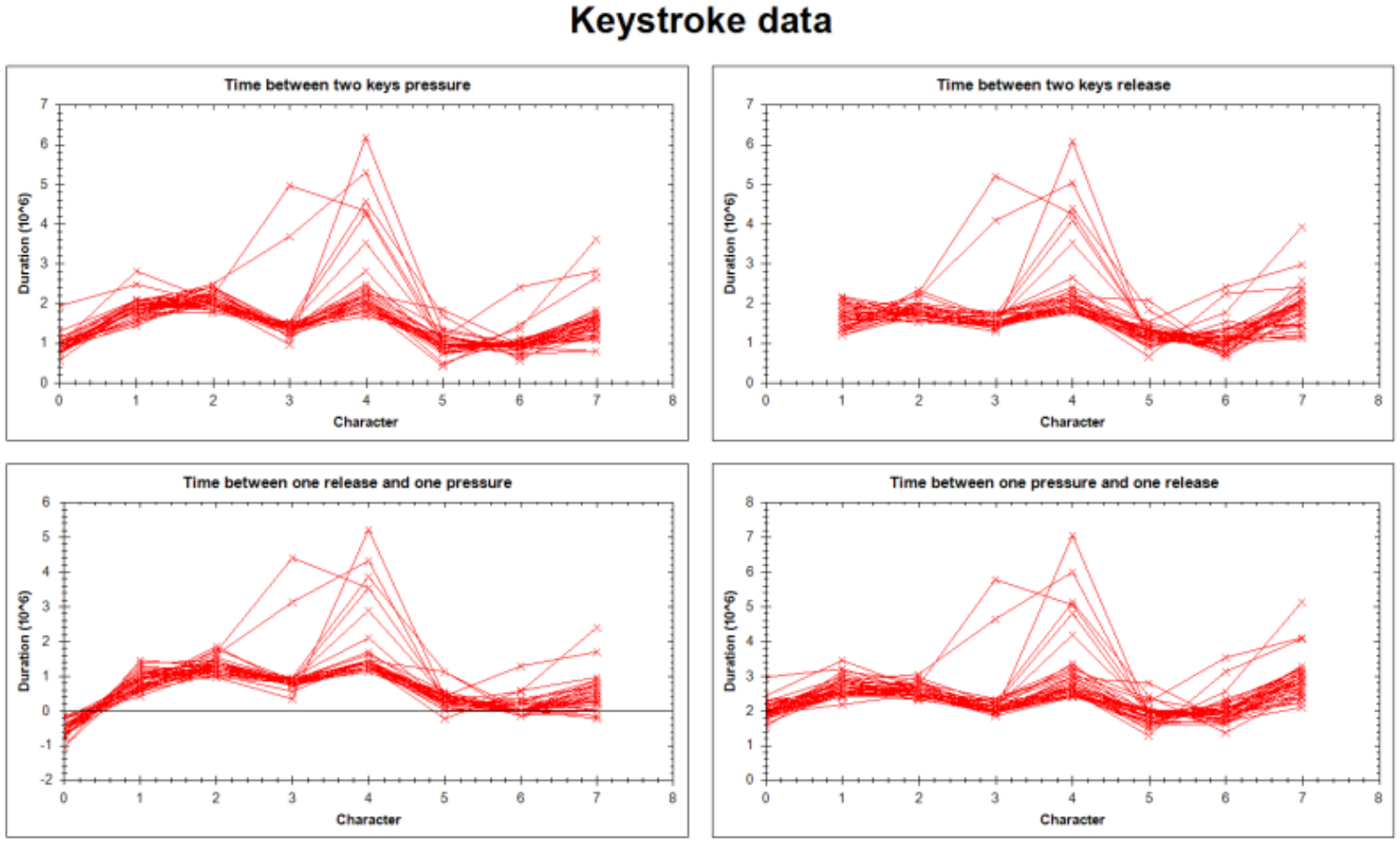
Of the 140 malware sam
attributed to APT28 so f
compiled between 0400
depicted in Figure 10. O
between Monday and Fri
working hours in UTC+0
times begin about 8AM a
time zone). This time zon
cities such as Moscow an

Figure 10: Compile Times of APT28 malware in UTC Time



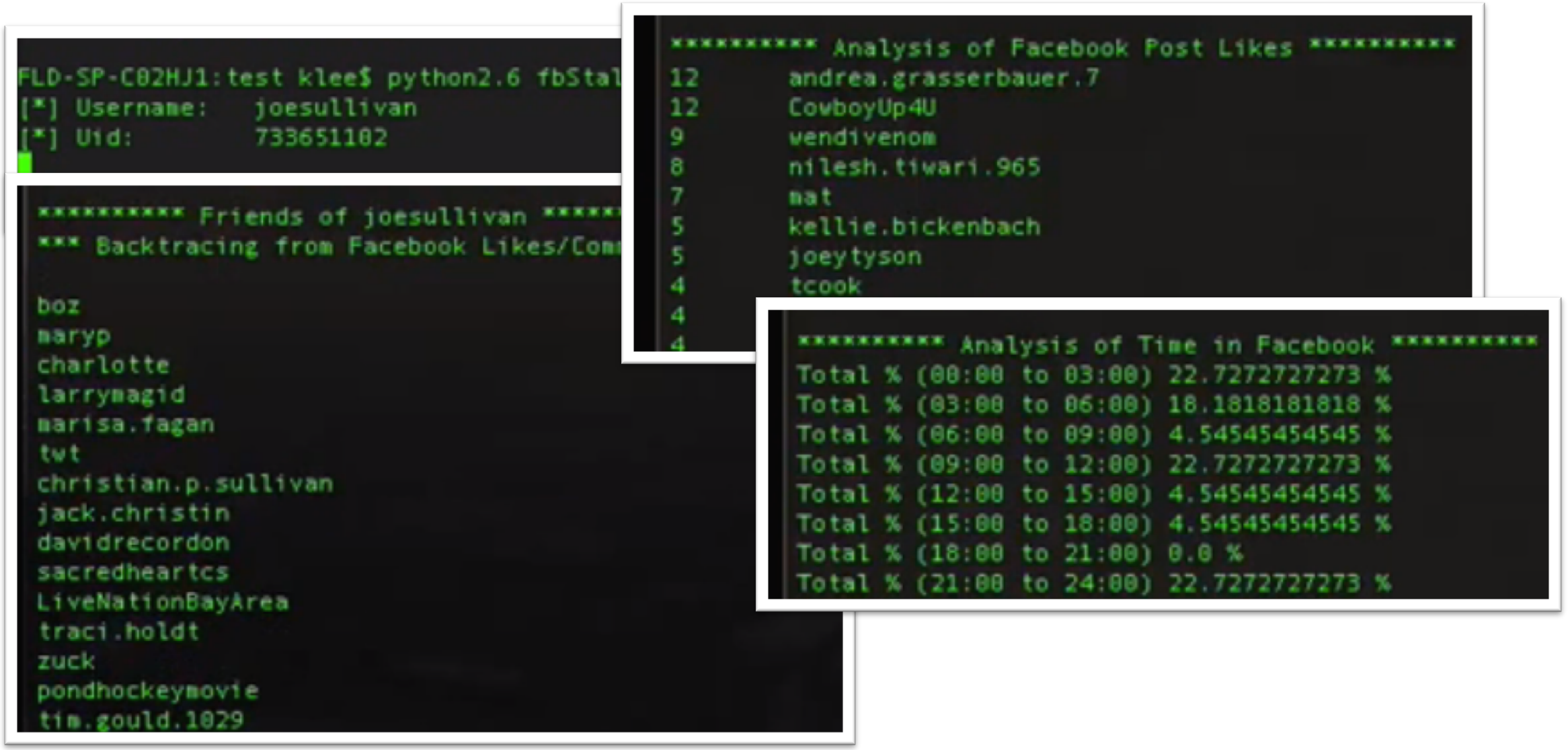
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

How the way you type can shatter anonymity



http://arstechnica.com/security/2015/07/how-the-way-you-type-can-shatter-anonymity-even-on-tor/

Fbstalker

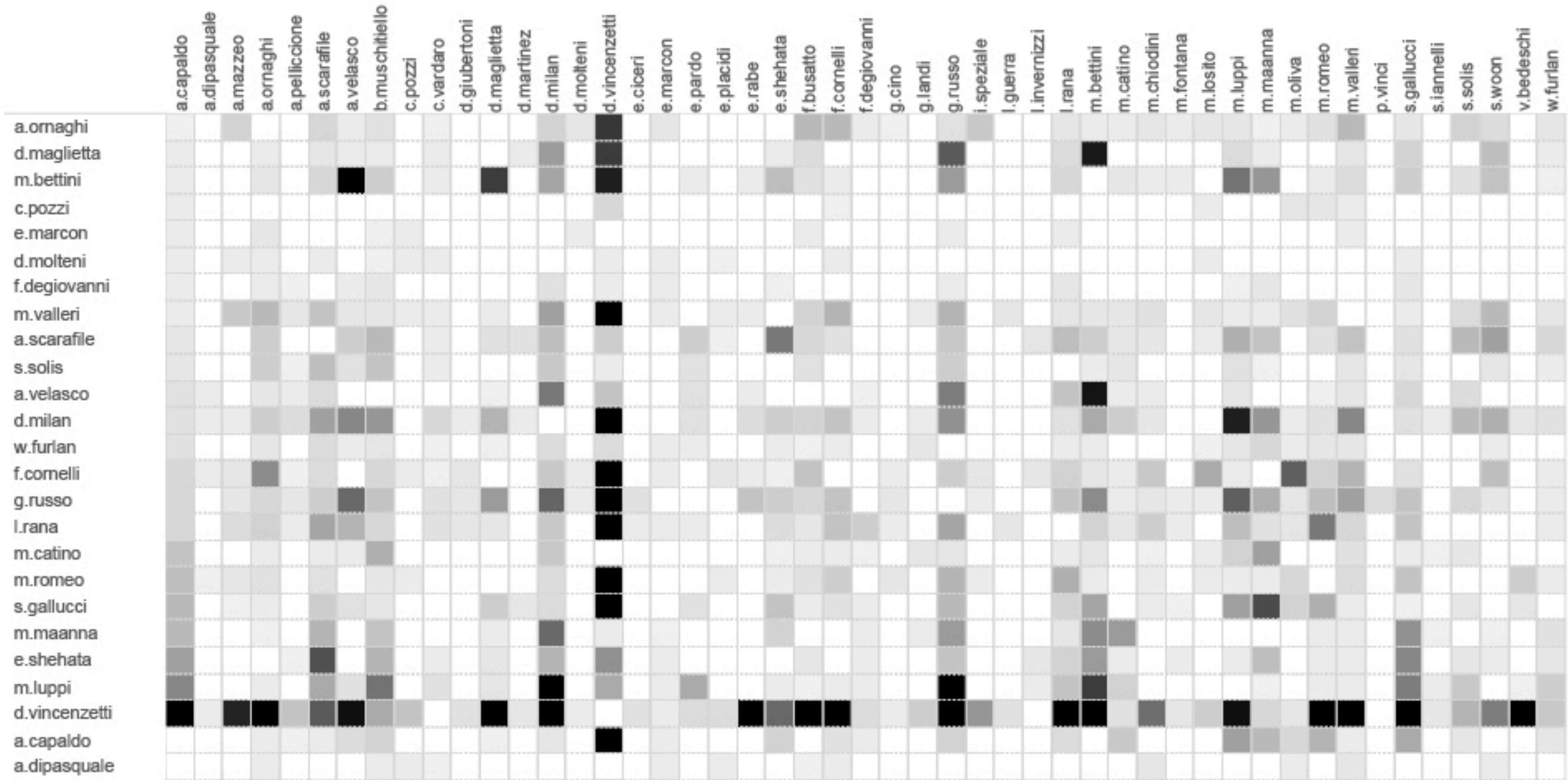

FLD-SP-C02HJ1:test klee$ python2.6 fbStal
[*] Username: joesullivan
[*] Uid: 733651102
********** Friends of joesullivan ******
*** Backtracing from Facebook Likes/Com
boz
maryp
charlotte
larrymagid
marisa.fagan
twt
christian.p.sullivan
jack.christin
davidrecordon
sacredheartcs
LiveNationBayArea
traci.holdt
zuck
pondhockeymovie
tim.gould.1029
********** Analysis of Facebook Post Likes **********
12 andrea.grasserbauer.7
12 CowboyUp4U
9 wendivenom
8 nilesh.tiwari.965
7 mat
5 kellie.bickenbach
5 joeytyson
4 tcook
4
4
********** Analysis of Time in Facebook **********
Total % (00:00 to 03:00) 22.7272727273 %
Total % (03:00 to 06:00) 18.1818181818 %
Total % (06:00 to 09:00) 4.54545454545 %
Total % (09:00 to 12:00) 22.7272727273 %
Total % (12:00 to 15:00) 4.54545454545 %
Total % (15:00 to 18:00) 4.54545454545 %
Total % (18:00 to 21:00) 0.0 %
Total % (21:00 to 24:00) 22.7272727273 %

https://labs.rs/en/metadata/

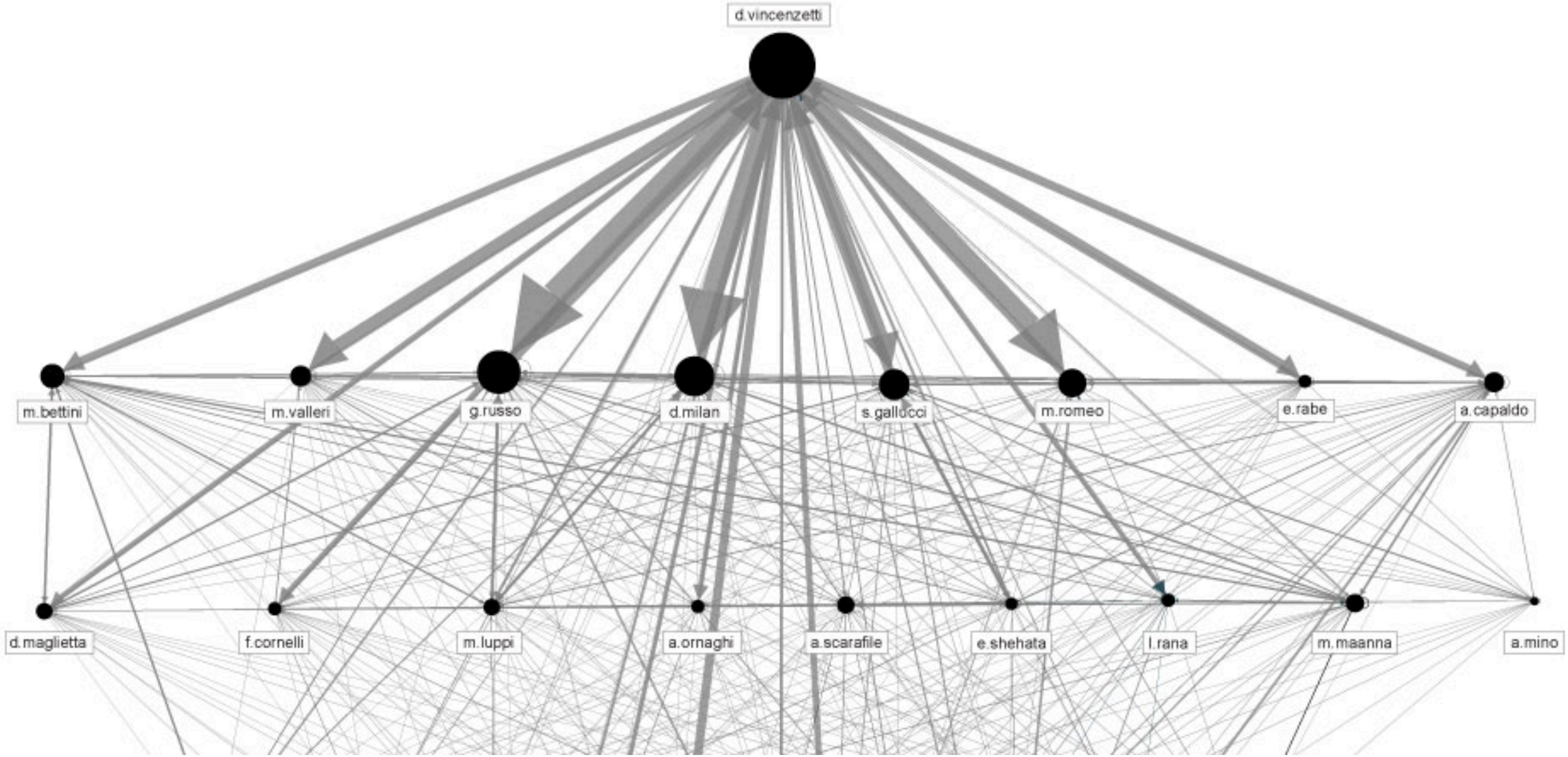
Share Lab is a newborn child of the Share Foundation – a research and data investigation lab for exploring different technical aspects of the intersections between technology and society.

"*Once online, our every movement, every click, sent or received email, our every activity produces a vast amount of invisible traces. These traces, once collected, put together and analysed, can reveal our behavioral patterns, location, contacts, habits and most intimate interests. They often reveal much more than we feel comfortable sharing.*"

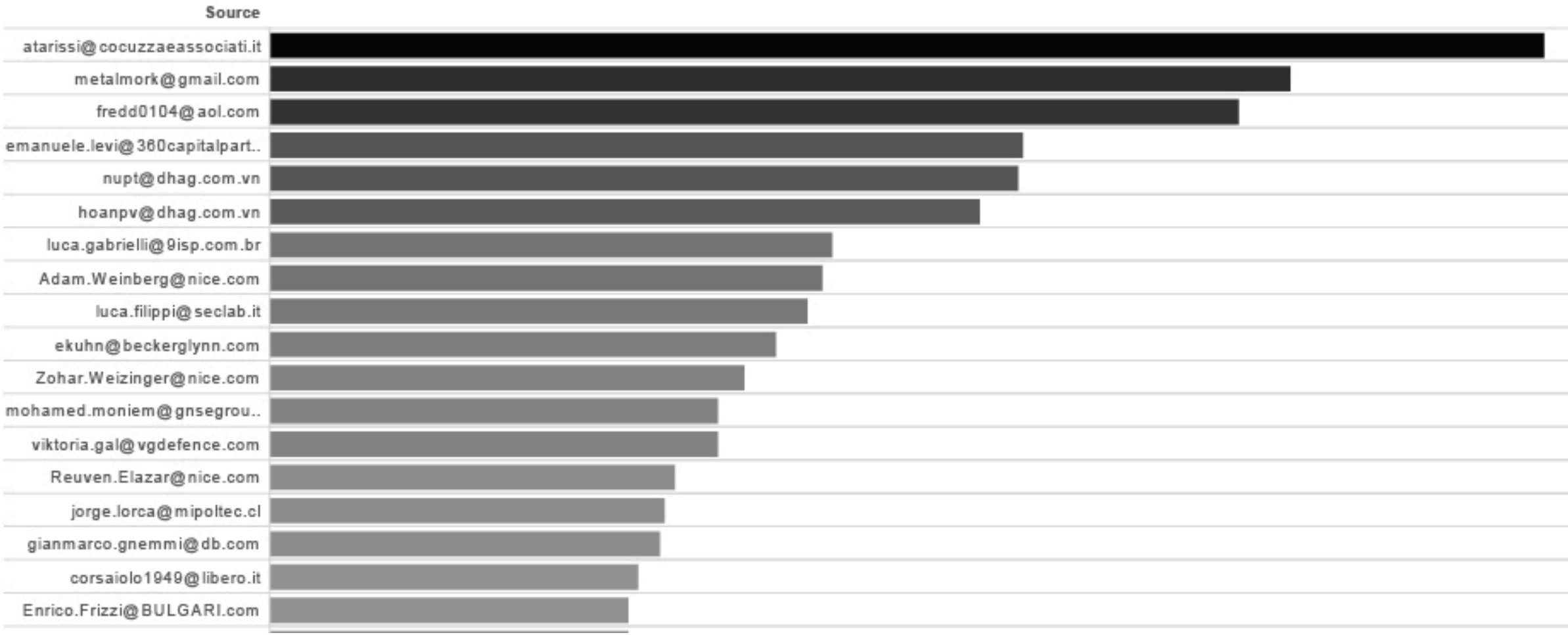
HEAT-MAP OF INTERNAL COMMUNICATION



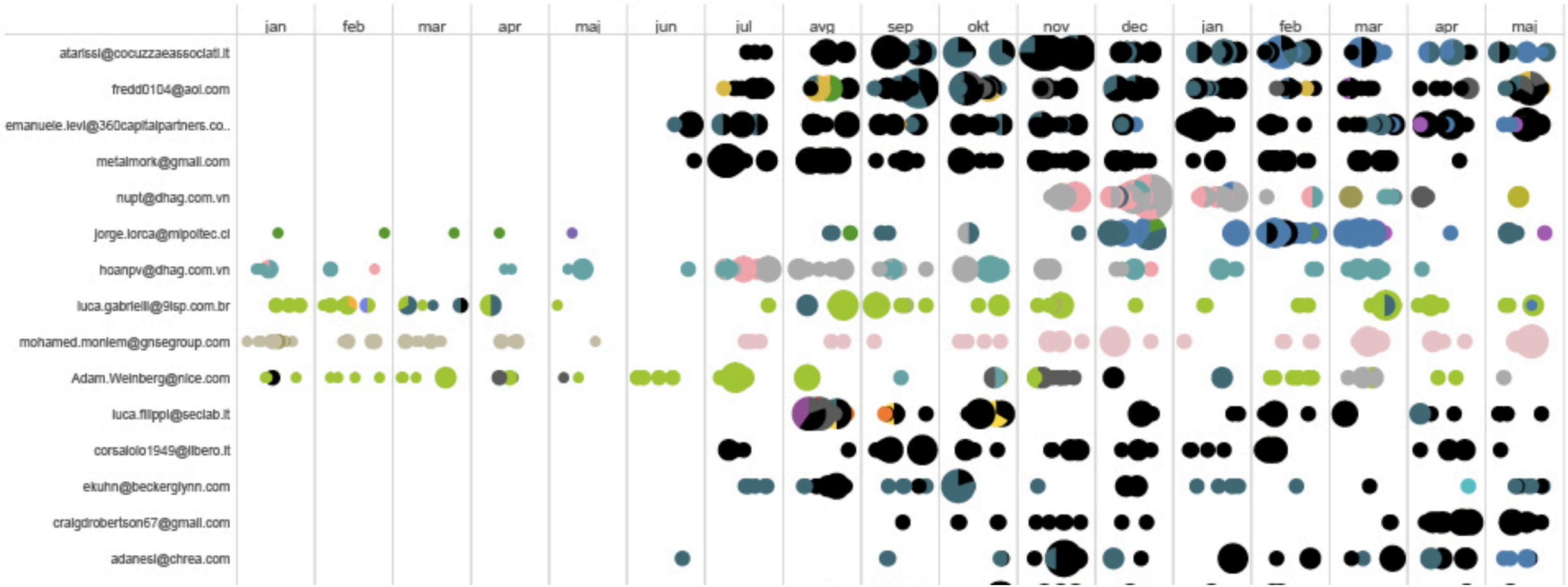
POTENTIAL ORGANISATIONAL STRUCTURE BASED ON THE LEVEL AND DIRECTION OF COMMUNICATION



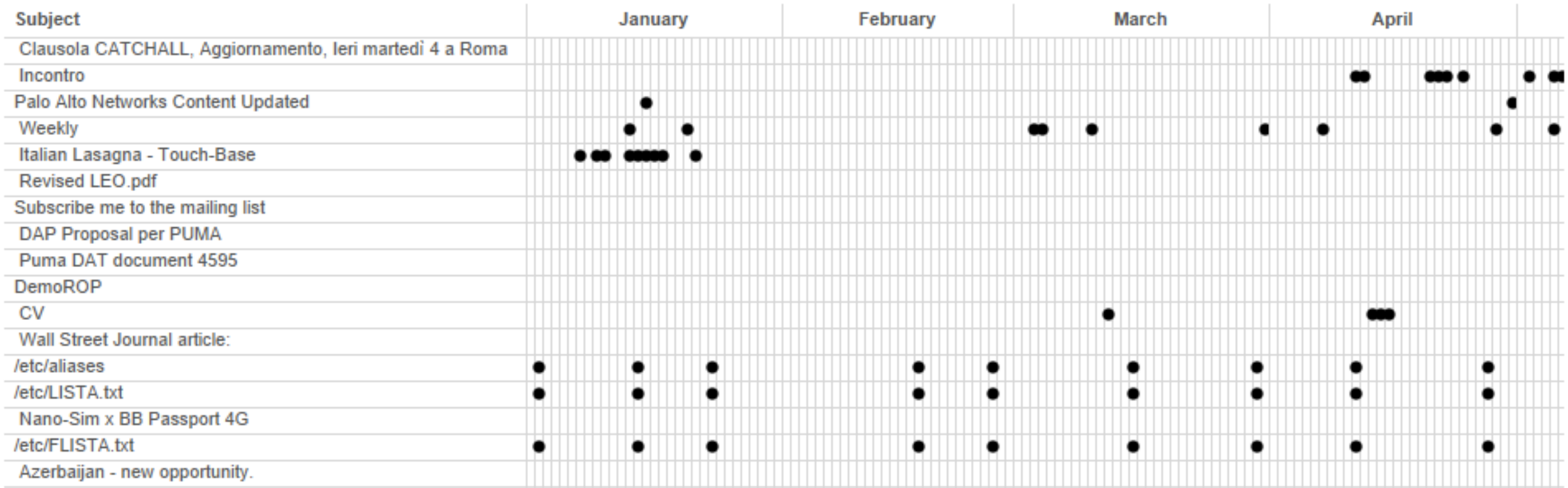
EXTERNAL CONTACTS WITH MORE THAN 50 EMAILS EXCHANGED WITH HT EMPLOYEES (2014-2015)



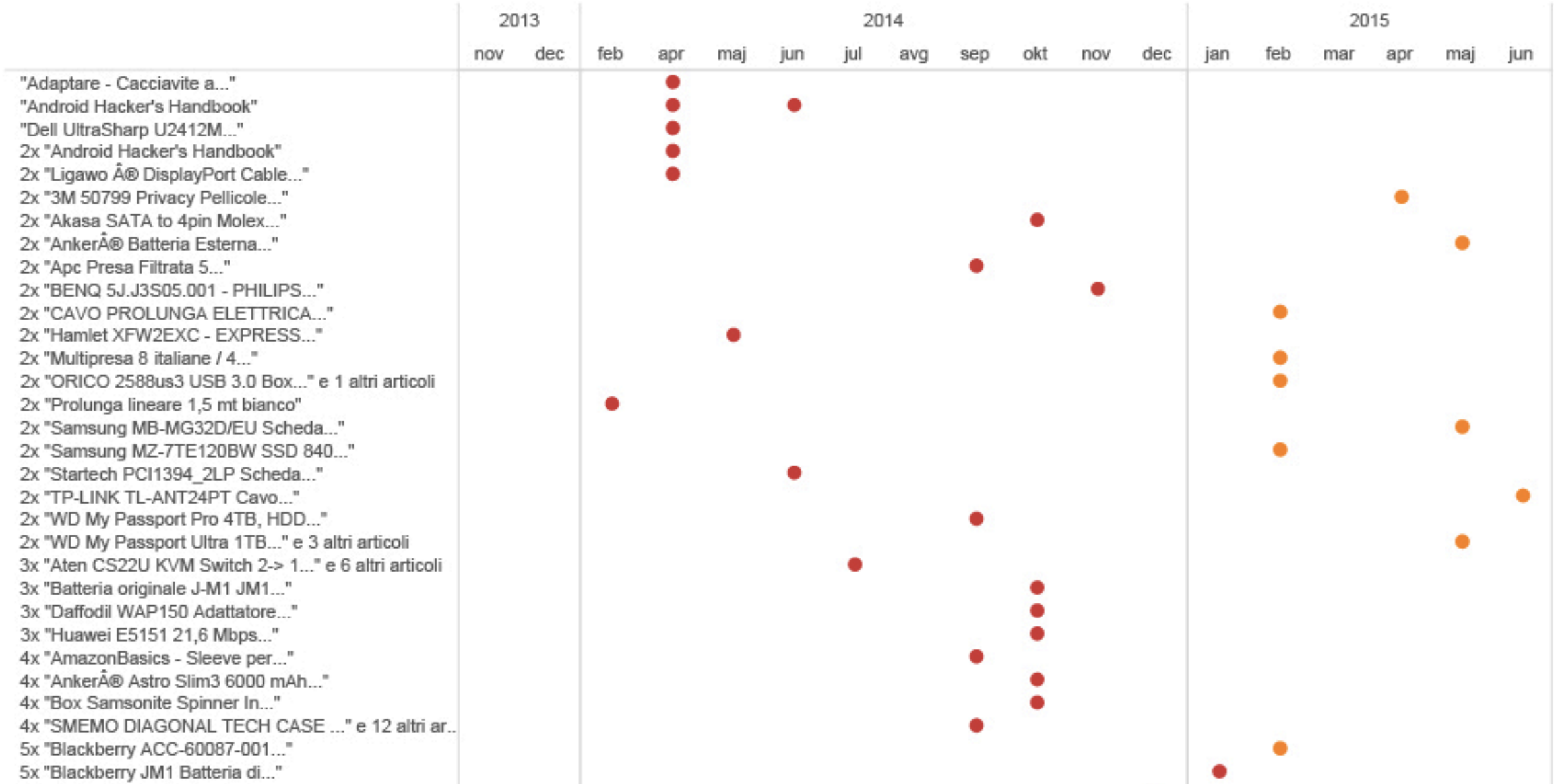
TIMELINE OF INDIVIDUAL COMMUNICATION OF EXTERNAL CONTACTS AND HT EMPLOYEES (2014-2015)



TIMELINE OF SUBJECT LINES (2014)

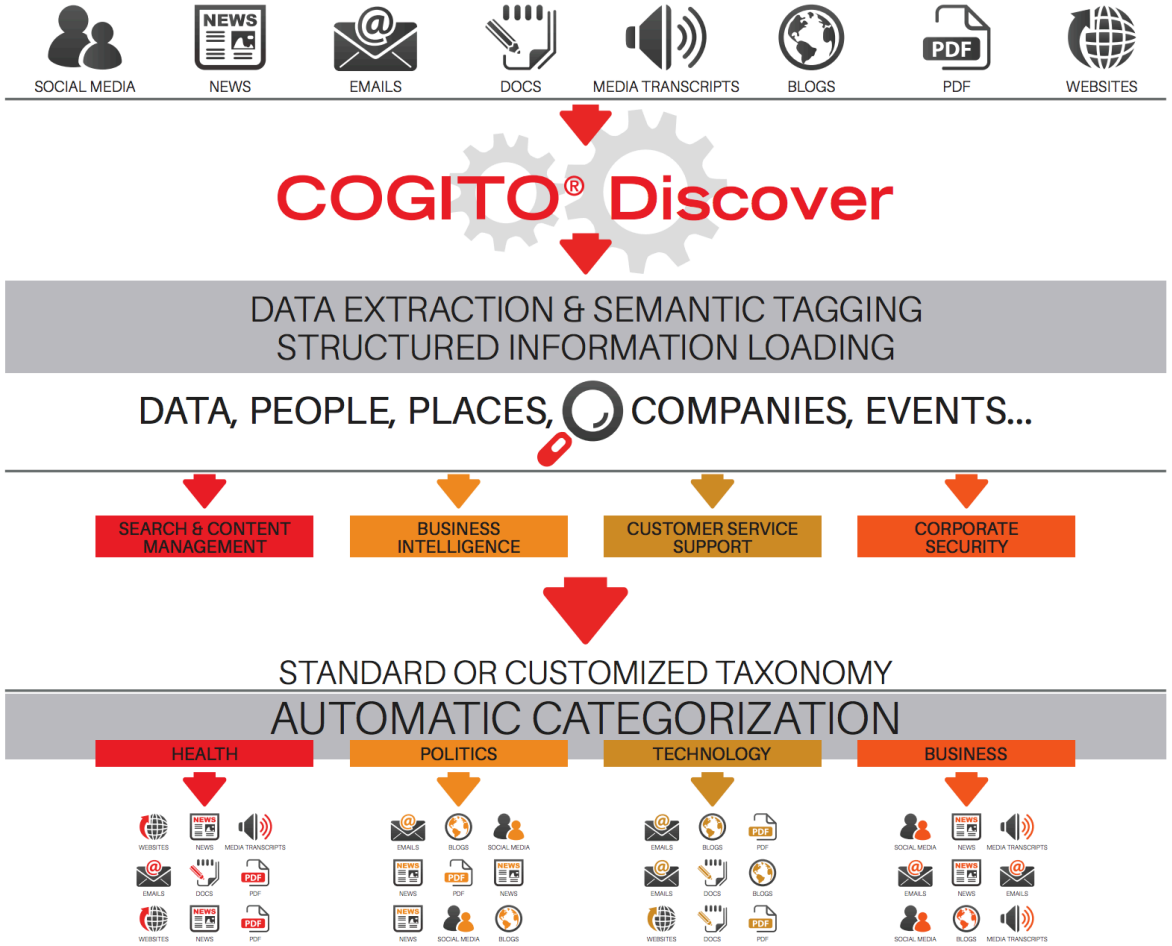


TIMELINE OF EMAILS WITH SUBJECTS FROM AMAZON.IT



MAP OF HT EMPLOYEES FLIGHTS BASED ON CWT EMAILS SUBJECT LINES

So much data so little time



https://www.mintpressnews.com/geofeedia-student-surveillance/249107/
https://cdn2.hubspot.net/hubfs/2037777/Brochure_Cogito%20Discover.pdf

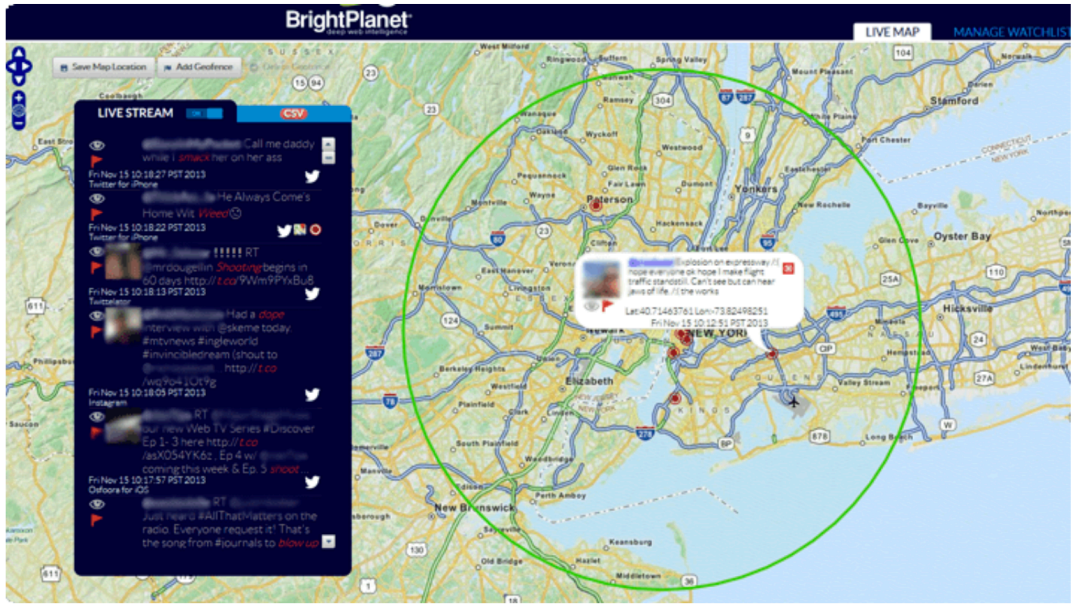
Cities under surveillance 1/2

THE POLICE OFFICER'S NEW TOOLS

As Police Monitor Social Media, Legal Lines Become Blurred

February 28, 2014 · 8:39 PM ET
Heard on All Things Considered

MARTIN KASTE



BlueJay, a tool by social media monitoring company BrightPlanet, shows the locations of tweeters who have left their geotagging option activated.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

POLICY —

First Chicago robber caught via facial recognition gets 22 years

With more cops using facial recognition tech, questions of efficacy remain.

CYRUS FARIVAR - 6/9/2014, 8:10 PM

https://www.npr.org/sections/alltechconsidered/2014/02/28/284131881/as-police-monitor-social-media-legal-lines-become-blurred?t=1559804031972
https://arstechnica.com/tech-policy/2014/06/first-chicago-robber-caught-via-facial-recognition-gets-22-years/

Cities under surveillance 2/2

New York school district's facial recognition system sparks privacy fears

Plan for cameras to track students in Lockport's schools called 'unprecedented invasion of privacy' and 'colossal waste of money'

▲ A display shows a facial recognition system at an industry conference in Washington DC. Photograph: Saul Loeb/AFP/Getty Images

CHICAGO 10/26/2012 03:29 pm ET

ShotSpotter Gunshot 'Listening' Technology Comes To Chicago Police Force

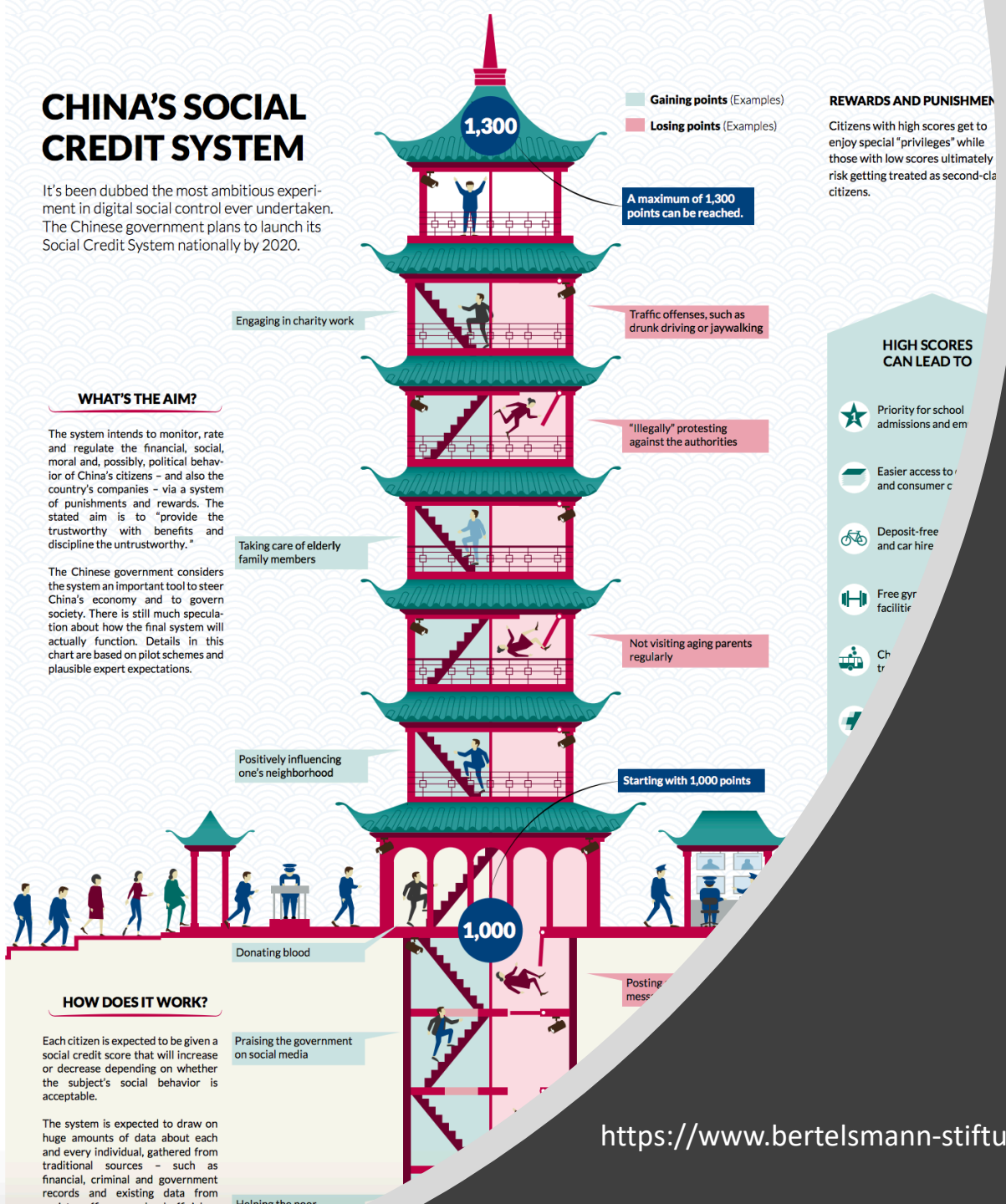
Chicago police are using a new technology that can listen for gunshots and help the responding officers pinpoint where they were fired. The technology, called ShotSpotter, relies on an acoustics-based, GPS-equipped system to feed police the location of a gunshot

https://www.huffpost.com/entry/shotspotter-gunshot-liste_n_2025220
https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york-privacy-fears

Tracking is valid also for non-digital contents like books

- **What is the USA PATRIOT Act?**
  - On October 25, 2001, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT) Act. The act broadly expands law enforcement's surveillance and investigative powers, with Sections 214-216 applying to libraries and bookstores.
- **How is SFPL responding to the USA PATRIOT Act?**
  - The USA PATRIOT Act is law, and the Library will comply with it. However, both the Library Commission and the San Francisco Board of Supervisors have formally opposed the Act, including Sections 214-216.
- **What are Sections 214-216 of the USA PATRIOT Act?**
  - These sections of the Act give law enforcement **agencies expanded authority to obtain Library records**, secretly monitor electronic communications and prohibit libraries and librarians from informing users of such monitoring or information requests.

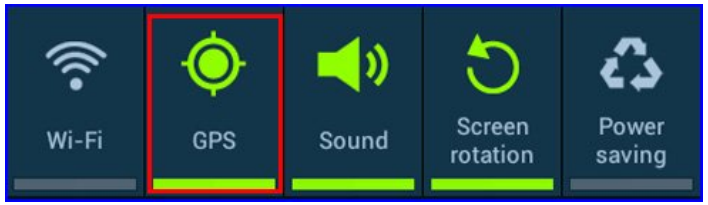
https://sfpl.org/?pg=2000060501



Yeah, but what's the impact on me?

https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf

How to share less metadata*



- Avoid Geo-Tagging when possible on all the devices and socials apps.

  PS: even if you disable the Location tracking in FB, the app, might use your IP address in order to track your location.

- Use software to delete Exif or other metadata.

  PS: do not upload your photos on sites with exif metadata deletion capabilities ☺

*Main suggestions in no specific order and not comprehensive

How to share less metadata*

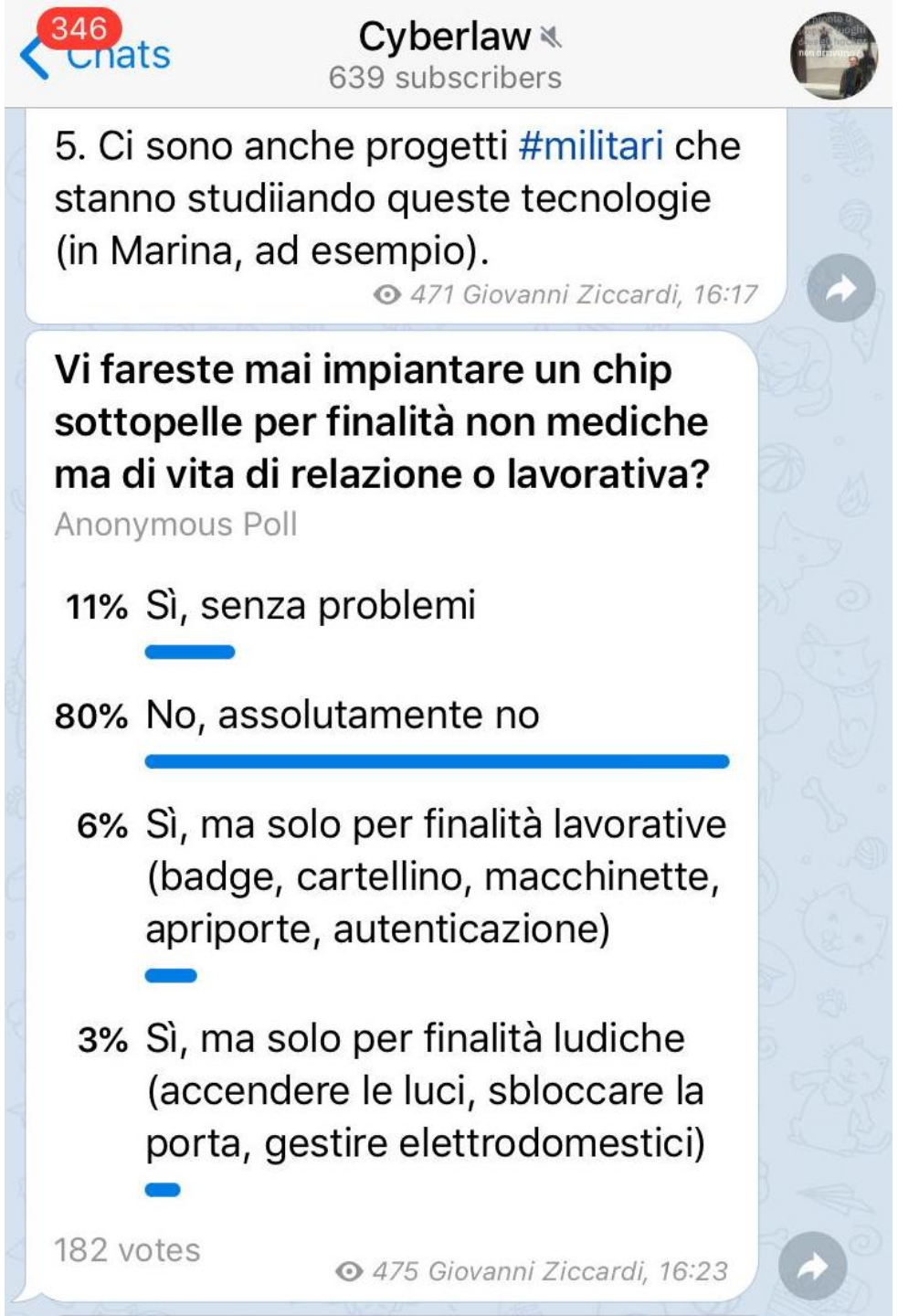
- Using a fake name on social it’s not that useful (your likes and your friends will be still real).
- Nicknames are usually unique, pay attention how you use it (emails, socials etc..).
- Avoid to fill the “subject” in the emails or use generic strings like: info, slides, details, opportunity etc… same thing for the attachments.
- Digital payments concerns (e.g. pay cash critical “things”?).
- Check terms & conditions and avoid registering on sites with T&C not updated: very likely the proper controls on your data and medata is low.
- Avoid using vocal messages.

*Main suggestions in no specific order and not comprehensive

How to share less metadata*

- Avoid having Wifi and Bluetooth always enabled (quite hard!)
- Follow privacy hardening guides at least for the main products you use (maps, FB, Whatsapp, Google services etc…)
- Remember that you location might be known due to usage of taxi apps, food delivery apps etc..
- T-shirt anti-face recon (?)
- Cancel cookies frequently
- Go at the e-privacy conference
- Stay updated on the topic
- Etc…

*Main suggestions in no specific order and not comprehensive



A «new» usage method?

Yiqin Fu @yiqinfu · 28 mag

A Germany-based Chinese programmer said he and some friends have identified 100k porn actresses from around the world, cross-referencing faces in porn videos with social media profile pictures. The goal is to help others check whether their girlfriends ever acted in those films.

Traduci il Tweet

Thanks!

Stay in touch @infoshaker