

BURNER PHONE 101

BROOKLYN PUBLIC
LIBRARY
AUGUST 2025

PRESENTED BY
REBECCA WILLIAMS



**HELLO!
MY NAME IS
REBECCA
WILLIAMS**



ABOUT ME

I am a writer, lawyer, and artist exploring how technology shapes power, government, and our relationships with one another. My work asks how we can resist surveillance and extraction while building systems that support collective care and self-determination.

REBECCAWILLIAMS.INFO

(1) SECRET GOALS

WHY ARE YOU HERE?

(2) KNOW YOUR RISKS

WHAT ARE YOU AFRAID
OF?

(3) SMART PHONES

HOW CAN WE IMPROVE
YOUR BAD PHONE?

(4) BURNER PHONES

WHAT ARE ALL YOUR
"OFF THE GRID"
OPTIONS?

(5) NO PHONES

WHEN SHOULD YOU
AVOID PHONES
ALTOGETHER?

(6) Q&A/LIVE SETUP

WHAT CAN WE STILL
LEARN FROM EACH
OTHER?

SECRET GOALS

(1)

WHY ARE YOU HERE?

BURNER PHONE 101

GOALS

LEARN HOW TO SET UP A
"BURNER" PHONE

EXPERIENCE A KIND &
JOYFUL WORKSHOP

SECRET GOALS

LEARN THE LIMITS OF
(BURNER) PHONES & MORE
ABOUT DIGITAL PRIVACY

TELL YOUR LOVED ONES

ANTI GOALS

ANY DIVULGING OF SENSITIVE
INFORMATION

ANY PROMOTING OF HARM OR
ABUSE

KNOW YOUR RISKS

(2)

WHAT ARE YOU AFRAID
OF?

RISK MODELING



WHAT ARE YOU
TRYING TO
PROTECT?



WHO ARE YOU
TRYING TO
PROTECT IT
FROM?



WHAT
HAPPENS IF
IT FAILS?

WHY IS “RISK MODELING” SO IMPORTANT?

BECAUSE YOUR'RE NOT
GOING TO DO IT
UNLESS IT IT'S THAT
IMPORTANT TO YOU

AND BECAUSE IT
WON'T WORK WHEN
YOU MOST NEED IT

GEORGE FLOYD, GENERAL WARRANTS, AND CELL-SITE
SIMULATORS

Brian L. Owsley*

ABSTRACT

The Fourth Amendment was enacted to prevent the government from utilizing general warrants. Instead, the government must obtain a warrant that is based on the specificity or particularity of the person, place, or thing to be searched. This approach evolved from a property-centric approach to safeguarding Fourth Amendment rights to one that is based on reasonable expectations of privacy.

Technology has long been a factor in law enforcement and balancing Fourth Amendment rights. As technology embeds itself in more of our lives, its constitutional impact also grows. Law enforcement periodically uses a device called a cell-site simulator to obtain personal information and data from cell phones. Essentially, a cell-site simulator works by mimicking a cell phone tower. All cell phones in a certain radius then attempt to register with the cell-site simulator for purposes of assuring that they can receive and send calls and data.

In law enforcement's gathering of data from a large number of cell phones, law enforcement essentially has a general warrant that violates the Fourth Amendment. The history of general warrants in England demonstrates the problem of gathering this data. This history, focusing on notable developments in England and America, demonstrates the problem. Regardless of whether one applies a property-centric approach or an expectation of privacy analysis, cell-site simulators pose a significant threat to those of general warrants.

There are reports that cell-site simulators have been used at protest rallies in Chicago. Similarly, there were reports of the protests over Freddie Gray's death in Baltimore. In the summer of 2020 over George Floyd's death, there was a response by law enforcement. This Article seeks to explore how cell-site simulators constitutes a search based on United States Supreme Court the handful of decisions that address cell-site simulators.

* Associate Professor of Law, University of North Texas Dallas College of Law; B.A., University of Notre Dame, J.D., Columbia University School of Law, M.I.A., Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. The author appreciates the assistance of Dean Felecia Epps and the UNT Dallas College of Law in support of this article. Similarly, the author owes much gratitude to the 2020 SEALS Criminal Law & Criminal Procedure Workshop, including Terrence Cain, Ngov Eang, Adam Gershowitz, Nicholas Kahn-Fogel, Corinna Lain, Suparna Malempati, Jennifer Moore, and Melanie Wilson. Finally, the author wants to thank Professor Christina Masso for her amazing assistance in editing and her numerous suggestions that enhanced this article.



EXAMPLE: PROTEST

WHAT ARE YOU
TRYING TO
PROTECT?

Location and protest
communications.

WHO ARE YOU
TRYING TO
PROTECT IT
FROM?

Government and corporate
surveillance.

WHAT HAPPENS
IF IT FAILS?

Police or corporations knew
you were at the protest and
your movements; they can
retaliate, categorize you as a
threat, or criminalize your
activity.

NOTE: With protest, consider your full risk profile
(social media data, etc.) & the risks of those around
you. Always ask for consent before posting images of
others.

EXAMPLE: ICE RAID

WHAT ARE YOU TRYING TO PROTECT? Phone content as evidence and identities of undocumented people.

WHO ARE YOU TRYING TO PROTECT IT FROM? ICE and corporate surveillance.

WHAT HAPPENS IF IT FAILS? Exposes videos/contacts, can put *others* at risk, leading to detainment or worse.



FILMING IMMIGRATION ENFORCEMENT

BE SAFE. BE ETHICAL. BE EFFECTIVE.

Filming encounters with immigration enforcement can expose human rights abuses, deter violence, substantiate reports and serve as evidence. But if the footage isn't captured safely and ethically, there can be unintended harm to both the person being filmed and the person filming.

Your first priority should be to do no harm. Exposing someone's identity could put them at greater risk. Always assess the risks before you hit "record" and consider other ways to respond if filming is unsafe (e.g. alert support networks and/or write down details after the incident).

KNOW YOUR RIGHTS

- It is legal to film immigration and law enforcement in public in the United States, as long as you don't interfere.
- Be aware that agents may falsely identify themselves as police officers or lie in the course of enforcement, but you should not lie.

MORE RIGHTS INFO

Immigrant Defense Project

- immigrantdefenseproject.org/ice-home-and-community-arrests/

American Civil Liberties Union

- bit.ly/ACLU_Right2Record
- bit.ly/ACLU_KYR_Immigrants
- bit.ly/ACLU_KYR_Border



BE SAFE

- Avoid locking your phone with fingerprint, face, and pattern ID. Law enforcement can't force you to give up your passcode without a warrant or court order, but they can ask or coerce you to unlock your phone with your fingerprint.
- Have a legal support number and/or a trusted contact's info handy.
- Encrypt your phone, regularly back it up, and delete sensitive data like images of or contact information for anyone at risk of deportation or arrest.
- Be aware that immigration agents and police care mainly about their safety, not yours. Moving quickly or suddenly to get a phone or reaching into your pocket could escalate the situation.





FILM THE DETAILS

- If possible, film key details such as law enforcement badges, uniforms (or lack thereof), license plates, weapons, communications between agents/officers, signage, property damage, border fences/walls, surveillance and body cameras, and cameras or other individuals filming. Document all agencies working together.
- Stay focused on law enforcement activity instead of civilians. Make targets and/or protesters harder to identify by filming very wide shots and/or filming people's feet or backs.
- Make it easier for investigators, journalists, and lawyers to verify your video by filming street signs, buildings and landmarks. If filming inside or outside someone's home, don't expose details of their living situation without consent. Doing so could put other members of their family at risk.

ANTI-DOXING GUIDE FOR ACTIVISTS



EXAMPLE: HARRASSER

WHAT ARE YOU
TRYING TO
PROTECT?

Phone number, accounts,
social graph.

WHO ARE YOU
TRYING TO
PROTECT IT
FROM?

Abusive partner or family
member, stalker, doxxer.

WHAT HAPPENS
IF IT FAILS?

Harasser gains account
information or location leaks,
putting your physical safety,
mental health, or employment
at risk.

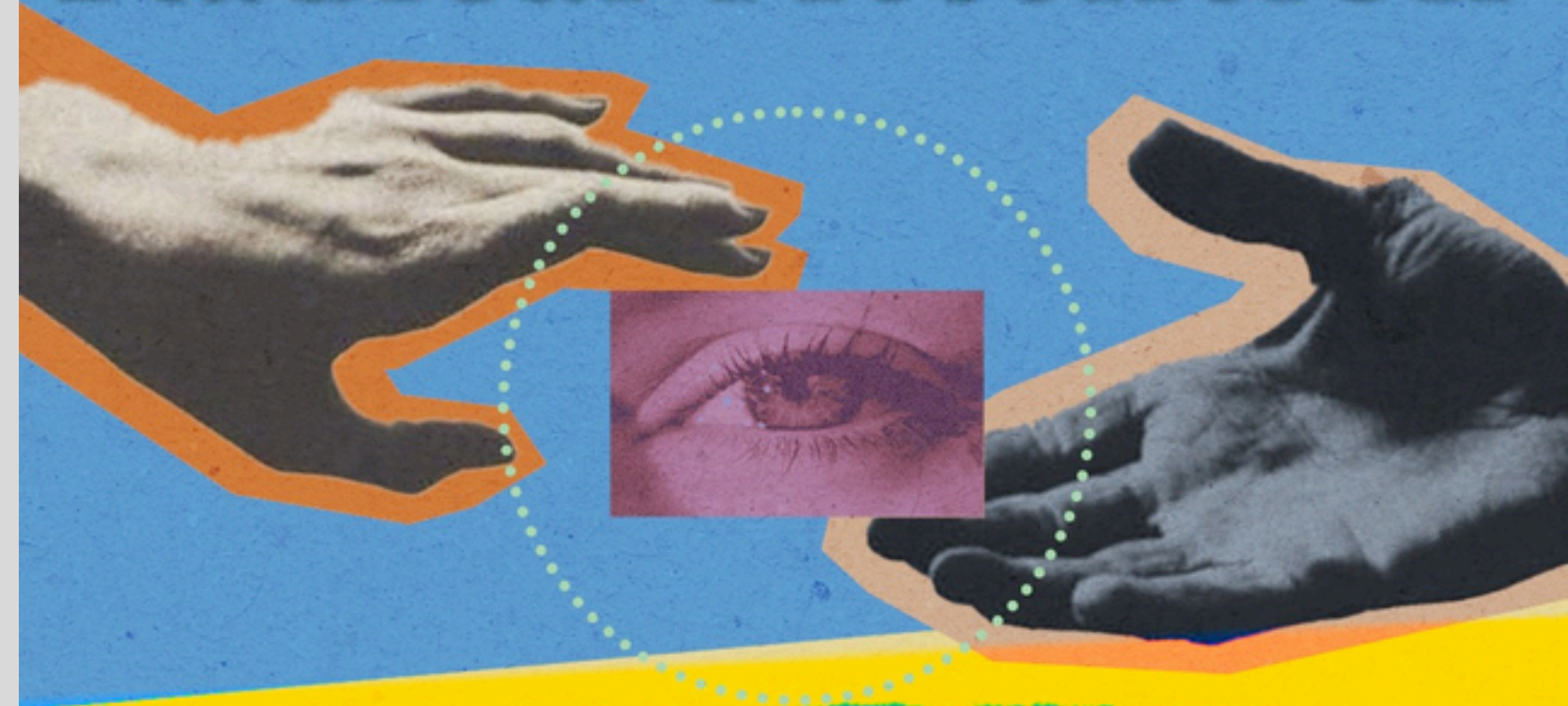
EXAMPLE: YOURSELF

WHAT ARE YOU TRYING TO PROTECT? Your attention, mental health, and time offline.

WHO ARE YOU TRYING TO PROTECT IT FROM? Yourself, constant reach, ad tech.

WHAT HAPPENS IF IT FAILS? Relapse into overuse.

Strother School of Radical Attention



ATTENTION ACTIVISM 101

Thursdays, 8:00 – 9:45pm


July 24 – August 7

Online via Zoom

Online Seminar



SMARTPHONES

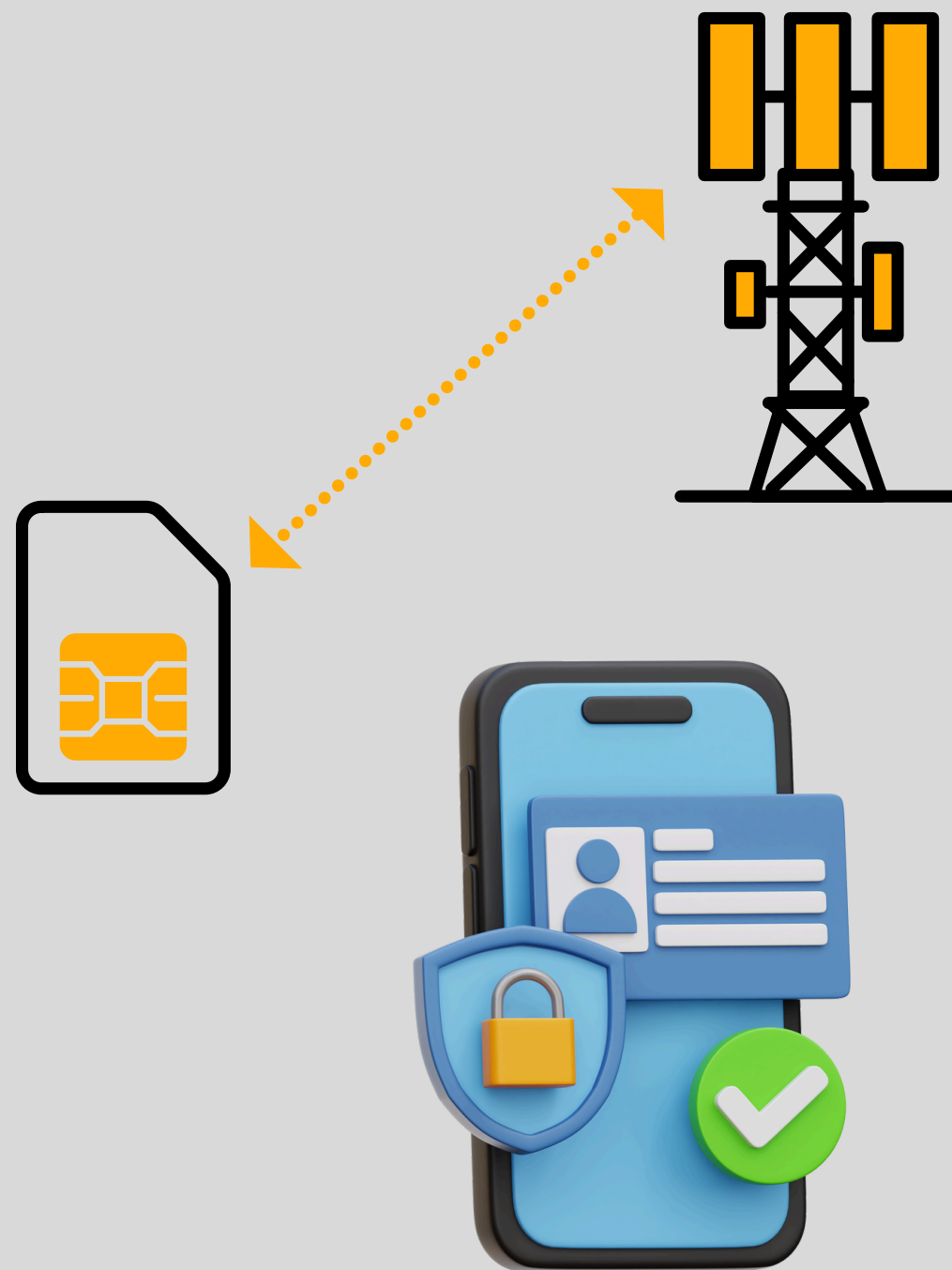


(3)

HOW CAN WE IMPROVE
YOUR BAD PHONE?

-

IDENTITY & FINANCE



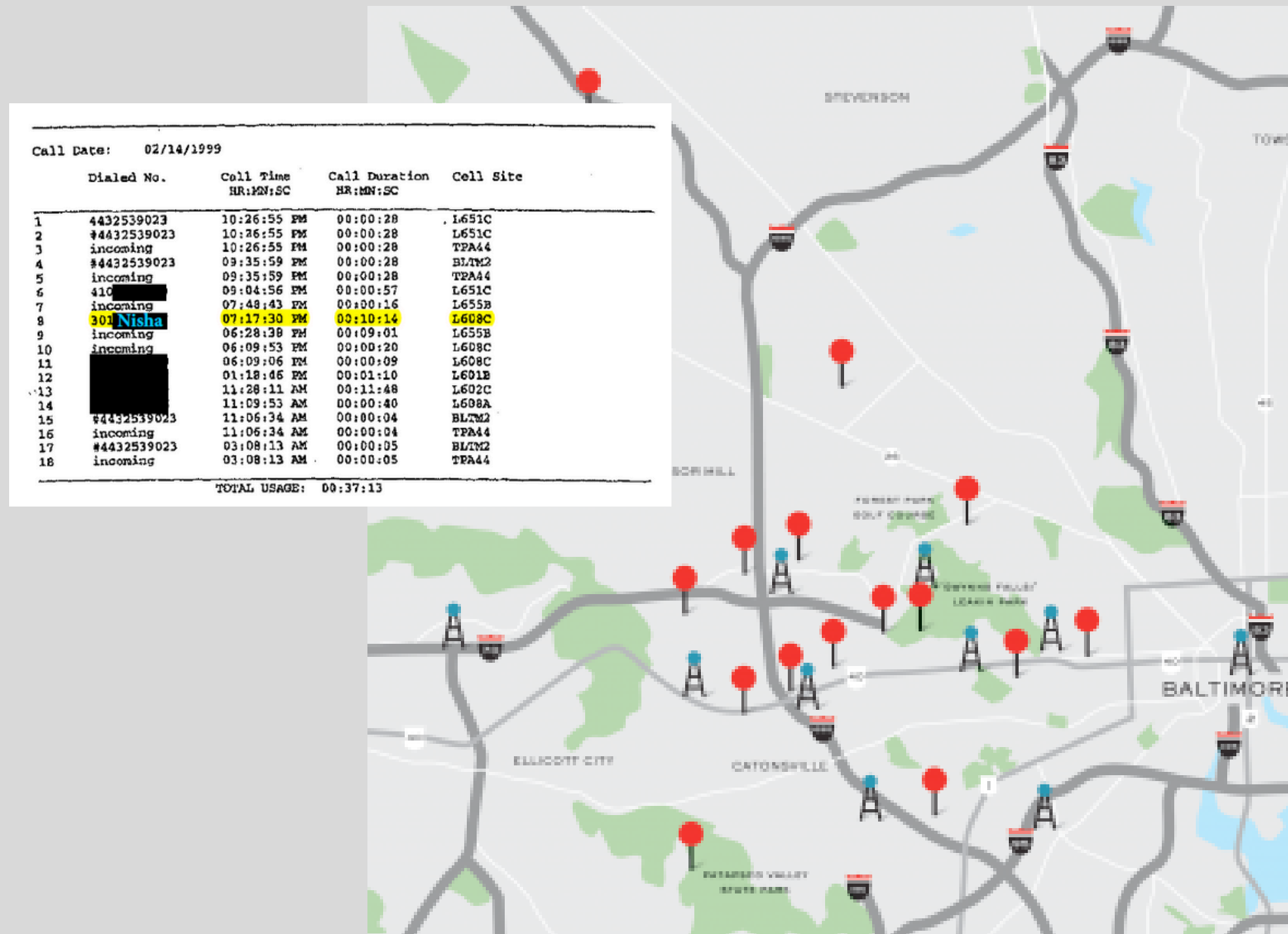
DEVICE IDS MAKE TRUE PHONE ANONYMITY NEARLY IMPOSSIBLE !!!

- IMSI TIED TO YOUR SIM & CELL TOWER ACCESS &
- IMEI TIED TO YOUR HARDWARE

IDENTIFIERS: PAYMENTS/ CONTRACTS, PHONE NUMBER, DIGITAL ID.

EXPOSED BY: CARRIERS, SIM REGISTRATION, TOWER LOGS, BIOMETRICS.

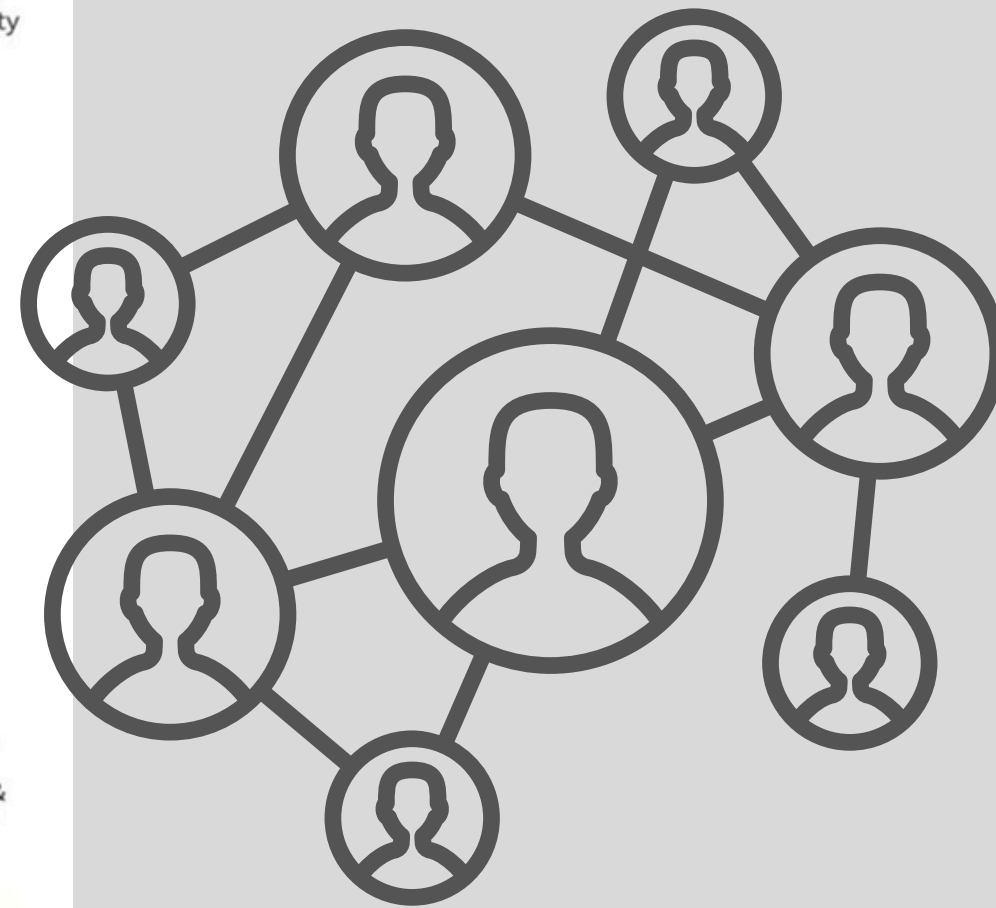
LOCATION & MOVEMENT



IDENTIFIERS: GPS,
WI-FI, BLUETOOTH,
CELL TOWERS,
SENSORS.

EXPOSED BY:
SPYWARE,
STALKERWARE, TOWER
DUMPS & DATA
BROKERS.

COMMS & SOCIAL GRAPH



IDENTIFIERS: CALLS, TEXTS, MESSAGING LINKS, CONTACTS.

EXPOSED BY: SPYWARE, STALKERWARE, PHONE BREAKING SOFTWARE, DATA BROKERS.

CONTENT & STORAGE

Table 2: Android OS Access Support Matrix – Locked devices 7.69.1

Vendor (Chipset)		Section 1: COLD - turned off (Secure startup or FBE)		Section 2: HOT (AFU or FDE without secure startup)		Comments and exceptions	
		BFU extractions (for FBE devices)	Brute-Force Password to get the user data (CE) decrypted	All Extractions (Even without BF)	Brute-Force password (not needed for extraction)		
Samsung (Exynos / MTK / Qualcomm)	Android 6	✖	✖	✓	✓		Fully Supported
	Android 7-14	✓	✓	✓	✓	Added BF support for QC S24, S24+, S24 Ultra	
Huawei (Kirin / Qualcomm / MTK)		✓	✓	✓	✓	P40 family is supported for Brute-force only up to ~04-2021 SPL	Huawei Kirin temporarily disabled.
Pixel	Pixel, Pixel XL	✓	✓	✓	✓		
	Pixel 3 - 5	✓	✓	✓	✓	Added AFU support for Android 14 Official and Pixel 8. BF support for Pixel 3-5 extended to latest SPLs	For Non-Samsung/Pixel, Qualcomm FBE devices, there may be a requirement for 24hr time of the device prior to brute force device. Affected devices: SM4350, I50 SM7150, I50 and newer
Non-Samsung Qualcomm Including Huawei, Motorola, Xiaomi, OnePlus and many others		✖	✖	✓	✖		

LISTEN TO THE 404 MEDIA PODCAST

404

ABOUT RSS SUPPORT/FAQ PODCAST FOIA FORUM ARCHIVE MERCH ADVERTISE THANKS PRIVACY

NEWS

Leaked Docs Show What Phones Cellebrite Can (and Can't)

The leaked April 2024 documents, obtained and verified by 404 Media, show Cellebrite could not unlock a large chunk of modern iPhones.

ADVERTISEMENT • GO AD FREE • HIDE

IDENTIFIERS:
ACCOUNTS, APPS,
PHOTOS, BACKUPS,
LOCAL FILES.

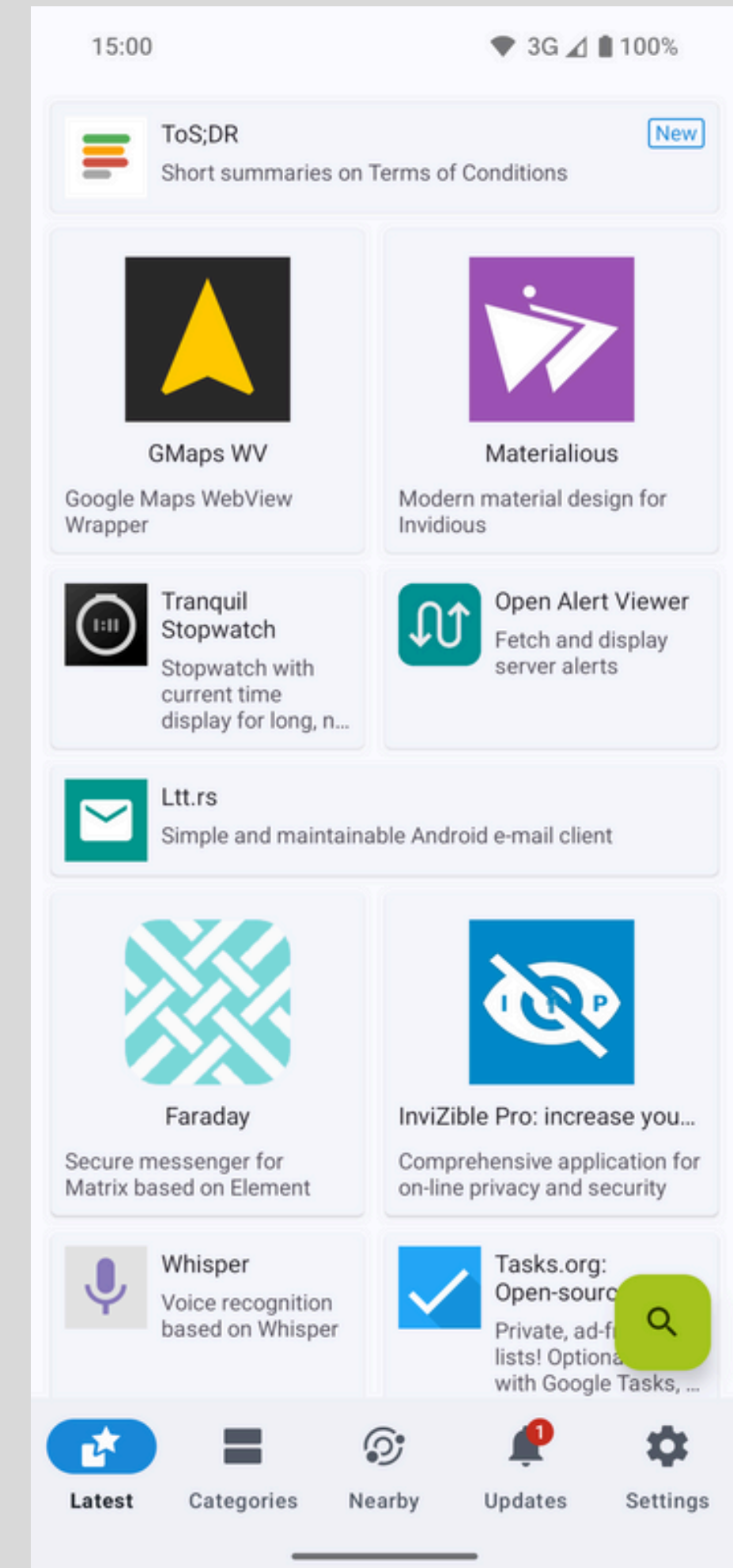
EXPOSED BY:
SPYWARE, FORENSIC
TOOLS (CELLEBRITE,
GRAYKEY), CLOUD
SUBPOENAS.

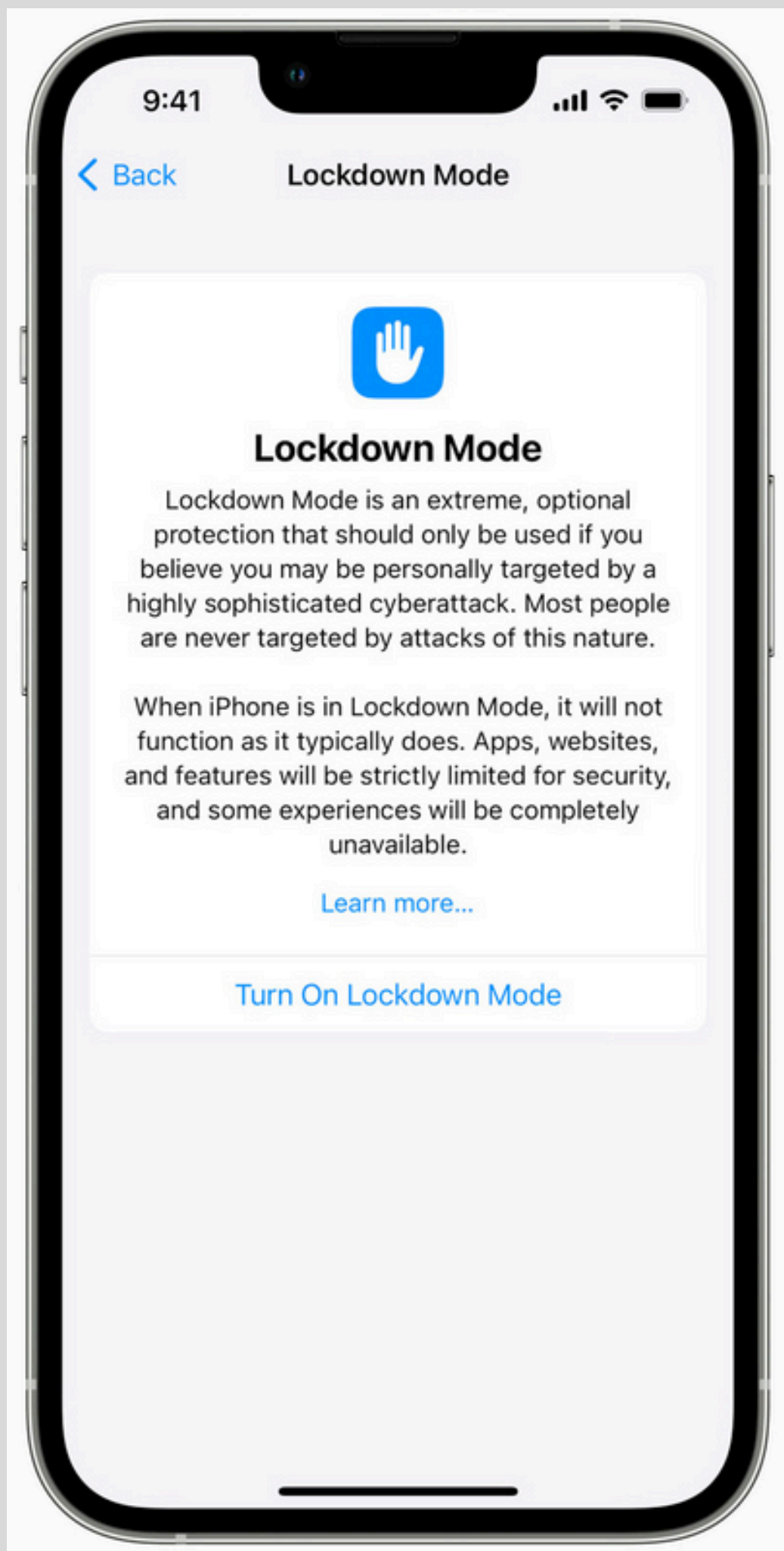
TIPS FOR ALL DEVICES

1. KEEP DEVICE & OS AS UPDATED AS POSSIBLE
2. STRONG PIN, NOT BIOMETRICS
3. DISABLE CLOUD BACKUPS / USE ENCRYPTED BACKUPS
4. INSTALL SIGNAL
5. ENFORCE STRICT APP PERMISSIONS (DENY MIC, CAMERA, LOCATION) UNLESS NEEDED
6. RADIOS OFF (GPS/WI-FI/BLEETOOTH) UNLESS NEEDED
7. STORE MINIMAL SENSITIVE DATA

ANDROID TIPS

- DISABLE GOOGLE LOCATION HISTORY AND AD PERSONALIZATION
- USE FIREFOX OR BRAVE INSTEAD OF CHROME
- RESTRICT GEMINI / GOOGLE ASSISTANT
- CONSIDER F-DROID FOR TRUSTED APPS
- CONSIDER HARDENED OS ALTERNATIVES LIKE GRAPHENEOS OR CALYXOS





IPHONE TIPS

- **ENABLE "ASK APP NOT TO TRACK"**
- **RESTRICT SIRI & APPLE INTELLIGENCE**
- **ERASE AFTER 10 FAILED PASSCODE ATTEMPTS**
- **USE LOCKDOWN MODE (IOS 16+) IF HIGH-RISK**

BURNER PHONES

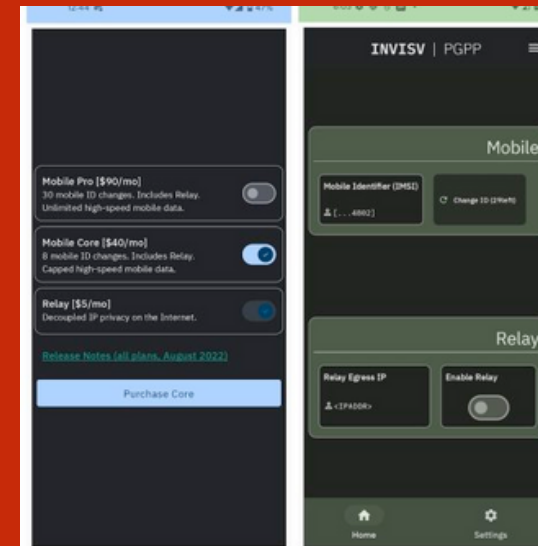
(4)

WHAT ARE ALL YOUR
"OFF THE GRID"
OPTIONS?

“BURNER PHONE” OPTIONS

A TAXONOMY OF WHAT IS COLLOQUIALLY CALLED A BURNER PHONE:

- Prepaid / Repurposed
- SIM-Swapping
- Minimal / Dumb Phones
- Device Disguises



UNIVERSAL BURNER SETUP

1. BUY PHONE & SERVICE IN CASH
2. DO NOT GIVE CARRIERS/CLERKS ANY PERSONAL INFO (EMAIL, PHONE, ID) WHEN ACTIVATING SERVICE
3. SET UP WITH PUBLIC WIFI
4. NO PERSONAL ACCOUNTS, NO CONTACT IMPORTS, NO BEING YOURSELF ON THE DEVICE
5. DO TIPS 1-7 FOR ALL DEVICES + MINIMIZE RADIOS/APP PERMISSIONS/PHOTOS AS MUCH AS POSSIBLE (OR YOU MAY COMPROMISE YOUR BURNER)
6. ROTATE YOUR SIM (PHYSICAL OR WITH PGPP; CARRIER ESIM CHANGES LEAVE A TRAIL)
7. TREAT AS DISPOSABLE

PREPAID OR REUSED PHONES

PROS

Cheap, easy, flexible.

CONS

Tower tracked, weak security, setup required.

OTHER CONSIDERATIONS

Prepaid (not automatically private, buy with cash, etc.) vs Old Unlocked (wipe required, best if you never used the phone before).



HOW TO SET UP A CLASSIC BURNER

PREPAID

1. BUY PHONE + MINUTES/PLAN IN CASH (BEST BUY, TARGET, WALMART, BODEGA).
2. DO NOT GIVE CARRIERS/CLERKS ANY PERSONAL INFO (EMAIL, PHONE, ID) WHEN ACTIVATING SERVICE.
3. THEN FOLLOW THE UNIVERSAL BURNER SETUP GUIDE.

USED/OLD

1. MAKE SURE THE PHONE IS FULLY WIPED/RESET AND UNLOCKED (TO AVOID TIES TO PAST CARRIERS).
2. INSERT A PREPAID SIM BOUGHT IN CASH (BEST BUY, TARGET, WALMART, BODEGA).
3. THEN FOLLOW THE UNIVERSAL BURNER SETUP GUIDE.

SIM ROTATING

PROS

Frequent new IMSI identities, PGPP automates.

CONS

IMEI still constant.

OTHER CONSIDERATIONS

Even with SIM rotation, your phone can still leak identifiers (Wi-Fi, Bluetooth, app logins).



HOW TO ROTATE YOUR SIM

MANUAL: ROTATE SIM CARDS

1. BUY PREPAID SIMS IN CASH (BEST BUY, TARGET, WALMART, BODEGA).
2. INSERT INTO UNLOCKED PHONE TO ACTIVATE.
3. SWAP OFTEN (DAILY/WEEKLY/AS NEEDED).
4. STORE USED SIMS IN A BAG OR DISCARD.

AUTOMATED: PGPP ROTATING ESIMS (ANDROID ONLY)

1. INSTALL THE PGPP APP.
2. BUY DATA/VOICE WITH A PREPAID CARD.
3. APP ISSUES NEW ESIM NUMBERS ON DEMAND OR SCHEDULE; NO NEED TO BUY OR SWAP PHYSICAL SIMS.

NOTE: ROTATING ESIMS DIRECTLY WITH YOUR CARRIER HELPS YOU GET A NEW NUMBER QUICKLY BUT IT IS NOT A GREAT OPTION FOR PRIVACY. EACH NEW ESIM ACTIVATION IS TIED TO YOUR ACCOUNT AND BILLING INFORMATION, LEAVING A PERSONAL TRAIL.





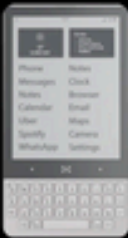




MINIMAL/DUMB PHONES

PROS

No apps/cloud, small attack surface.

CONS

Tower tracked, no encryption, limited functionality

9 DUMBPHONES TO HELP CURB YOUR SCREEN ADDICTION									Freethink*
									
	Light Phone II	Light Phone III	Lively Jitterbug Flip2	Mudita Pure	The Minimal Company Minimal Phone	Punkt. MP02	Greentouch Mindful	Sunbeam F1 Horizon	Techless Wisephone II
Cost	\$299	\$799	\$79.99	\$369.99	\$499	\$299	\$307	\$249	\$399
Availability	Now	February 2025	Now	Now	October 2024	Now	Now	Now	Summer 2024
Dimensions	3.77 x 2.20 x 0.34"	4.17 x 2.81 x 0.47"	4.30 x 2.19 x 0.75"	5.67 x 2.33 x 0.57"	5.59 x 3.07 x 0.34"	4.61 x 2.02 x 0.57"	5.60 x 2.60 x 0.41"	4.33 x 2.28 x 0.91"	6.37 x 3.02"
Features									
📞 Calls	✓	✓	✓	✓	✓	✓	✓	✓	✓
💬 Texts	✓	✓	✓	✓	✓	✓	✓	✓	✓
📷 Camera		✓	✓		✓		✓	✓	✓
🔔 Alarm	✓	✓	✓	✓	✓	✓	✓	✓	✓
📅 Calendar	✓	✓		✓	✓	✓	✓	✓	
📝 Notes	✓				✓	✓	✓		✓
🧮 Calculator	✓				✓	✓	✓		✓
🔦 Flashlight					✓			✓	✓
📍 Navigation	✓				✓			✓	✓
🎵 Music	✓				✓		✓	✓	✓
📶 Wifi	✓				✓	✓	✓	✓	✓
📶 Bluetooth	✓				✓	✓	✓	✓	✓



DEVICE DISGUISES

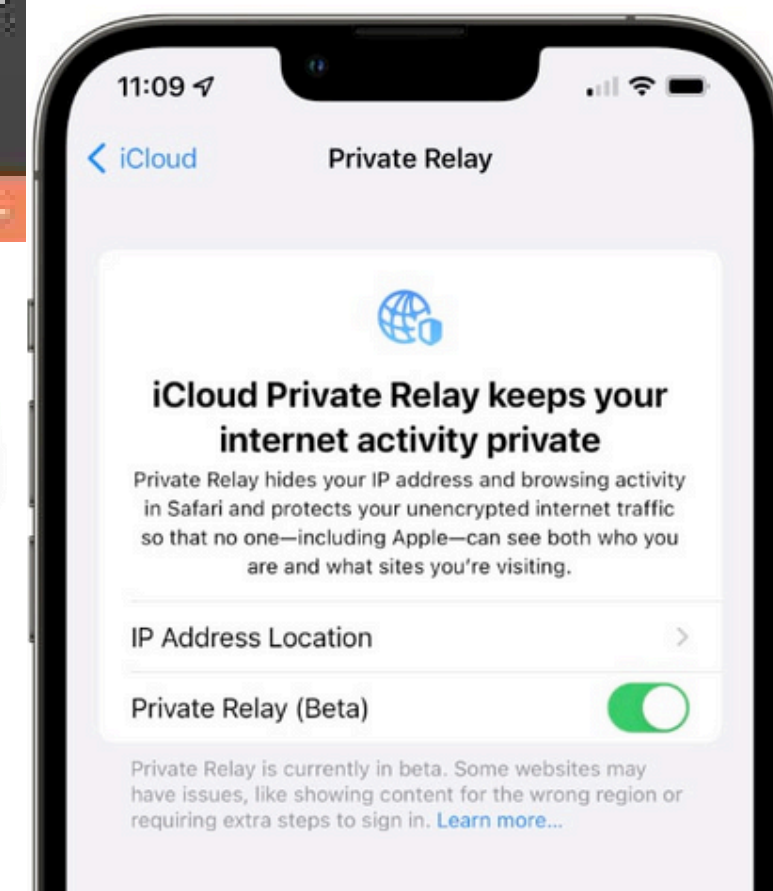
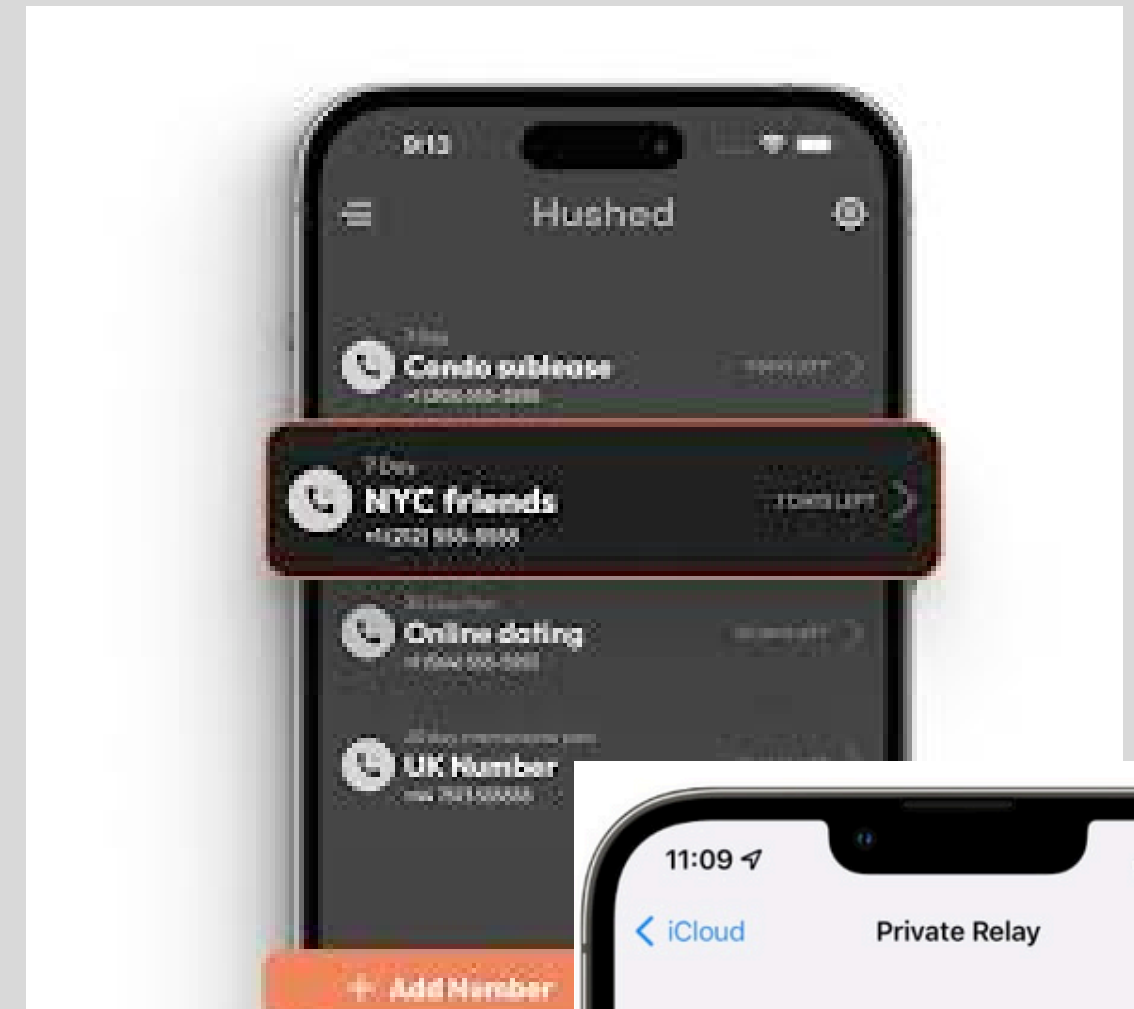
PHONE MASKING: VOICE OVER INTERNET PROTOCOL (VOIP)

IP MASKING: VIRTUAL PRIVATE NETWORK (VPN)

TOWER PING MASKING: MOBILE HOTSPOTS

PROS Obscure identifiers, avoid towers.

CONS Metadata trails, configuration still required.



BURNER 101 FINAL EXAM

THE SAFEST BURNER IS ONE BOUGHT IN CASH, LOCKED WITH A STRONG PIN (NOT BIOMETRICS), USING SIGNAL ONLY, WITH RADIOS KEPT OFF, A ROTATING SIM, NO PERSONAL ACCOUNTS OR PHOTOS, MINIMAL DATA STORED, AND THE DISCIPLINE TO TREAT IT AS DISPOSABLE.

NO PHONES

(4)

WHEN SHOULD YOU
AVOID PHONES
ALTOGETHER?



WHEN TO GO NO PHONE



WHERE LOCATION
TRACKING COULD
BE EVIDENCE



WHERE
CONFISCATION RISK
IS HIGH



WHEN YOU DON'T
WANT AN
ASSOCIATION TRAIL

HOW TO GO NO PHONE

- USE A PAPER OR SAVED PHOTO MAP AND KEEP CONTACTS WRITTEN DOWN.
- USE OFFLINE-ONLY DEVICES (CAMERA, NOTEPAD) IF NEEDED.
- ARRANGE PRE-SET MEETING POINTS/TIMES.
- USE AN IPAD (OR OTHER TABLET) ON PUBLIC WI-FI INSTEAD OF YOUR PHONE.
- BORROW OR USE A COMMUNITY/ROTATING DEVICE ONLY WHEN NECESSARY.

Q&A/LIVE SETUP

(6)



WHAT CAN WE STILL
LEARN FROM EACH
OTHER??