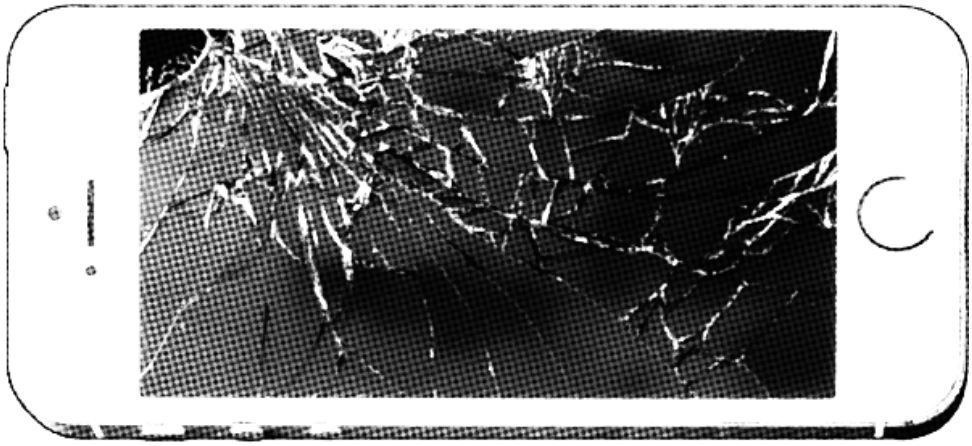
Smash all phones!

How To Protect Yourself From the Snitch in Your Pocket



Smash All Phones! How To Protect Yourself From the Snitch in Your Pocket

Original text in English
r2klegal.protestarchive.org/docs/smashallphones.pdf

Layout
No Trace Project
notrace.how/resources/#smash-phones

Contents

Data Extracted From the Phone 3
Emotional Fallout 6
Ten Steps to Consider 7
Resources and Further Reading 9

Data Extracted From the Phone

Tech savvy folks have a name for one of the safer ways to transfer data without the risk of snoops dipping into the information being sent while it's in transit: the sneakernet. Save data onto a portable drive, and walk it over to where it needs to go (wearing sneakers, of course!).

Recently I received two USB drives by sneakernet from my lawyer. I had been arrested at a protest months earlier,[1] and despite my original plans to the contrary, had my unencrypted Android smartphone on me during the arrest. Many articles and zines address electronic safety and precautions you can take to keep data safe while communications are being sent or received.[2] The purpose of this text is to inform you of the kind of data cops can easily take from your phone if they have physical access to it, and what you can do to mitigate that, so you can keep yourself and loved ones safe in a wider range of scenarios.

The USB drives I received contained all the data the cops took from my phone using a system created by a company called Cellebrite.[3] Cellebrite contracts with individual police departments, cities, companies, and militaries around the world. Among the products they sell are machines to which cell phones can be connected. They have "field models" which can be carried around in police cars, advertising their ability to "directly extract passwords, disable or bypass user locks and decode data from more than 1,500 mobile applications in minutes" so as to "increase conviction rates with accuracy and speed." According to the information on the drives, my phone was connected for about 45 minutes to extract its information.

I had only had my phone for 5 months at the time it was taken from me, but because it was signed in to a Gmail account that had been active for 11 years, the information they were able to gain was enormous.

Below is a list of all the information I received in one massive easy-to-search and sort spreadsheet. They also gave me an almost 8,000 page document with the same information.

---

[1] *No Trace Project (N.T.P.) note:* The author was arrested at a protest against the 2017 presidential inauguration of the 45th United States President, Donald Trump.

[2] See resources at the end of this text.

[3] cellebrite.com

- A list of all contacts, including phone numbers and emails that contacted me that were not stored in my phone, with a count of how many times I called, messaged, or emailed them or was called, messaged, or emailed by them.
- How many emails I received, sent, and drafted to specific email addresses and how many shared calendar events I had with those email addresses. How many incoming/outgoing/missed calls from each number and if they were in my contacts and how long total calls were between me and a number. Whether they were in my contacts, and if so what nickname I call them in my phone.
- How many SMS texts received/sent/drafted to a number. The content of all texts, even if and whether they were deleted, including drafts.
- Whatsapp contacts and their "username" (i.e., the phone number attached to their account) and how many chats/calls between me and them.
- All apps and when they were installed/deleted/last used/"purchased", and what permissions they had.
- Audio files that were stored in Google Drive, any podcasts, voice memos, and ringtones. Timestamps for their creation/deletion/modification/last access.
- All calendar events, attendees invited, location tags, etc.
- Traditional call log info you might expect.
- Date and time of cell towers my phone had ever connected to[4] and their location, conveniently linked to Google Maps. A world map marking all cell towers accessed by my phone.

---

[4]When a cell phone is on (and sometimes when you think it's off!), it is constantly looking for signal from a cell tower. So as long as your phone has service, it is in communication with a cell tower. If signal strength from 3 cell towers is known, your location can be determined highly accurately (sometimes within a few meters). For more on this, see "The Problem with Mobile Phones", in further reading.

[5]At the time of the arrest I did not know about disappearing messages on Signal, although I do not know if this would have changed the outcome of what could be obtained with physical access to my phone. Remember that Signal is designed to keep anyone from reading your messages in transit and to avoid people pretending to be

- "Chats" from Signal,[5] WhatsApp, SMS, Google Hangouts,[6] TextSecure, GroupMe, Google Docs; a list of all participants in those chats; text body content; whether it was read or unread, timestamp for sent and read; if it was starred; if it was deleted; all attachments. These chats were also from years ago, way longer ago than when I even had a smartphone.
- All information for all my contacts, including whether the contact was deleted or not.
- Web browser cookies.
- Any document ever opened on my phone, including text documents, attachments, Google Docs files, and those created by apps.
- Emails and email drafts, including all sending information, entire text content, and up to 16 attachments.
- Images/photos/videos along with their created/accessed timestamp and any metadata.
- 96 random tweets from one of my twitter accounts, some from as far back as 2013.
- A list of all Wi-Fi networks that my phone ever connected to, their passwords, hardware identifiers, and when I connected to them.
- The last 5 times my phone was turned on, including twice 2 months after I lost access to it.
- Web history and web and Play Store search history.
- A list of every word ever typed into my phone and how many times that word was typed, including email addresses as words, including words I added to the dictionary so they wouldn't be continued to be autocorrected to something else.

---

someone else, not to keep someone who physically has your phone from obtaining the messages. [*N.T.P. note:* Indeed, someone with physical access to a phone may be able to access deleted Signal messages.]

[6]There were bits of time when I had used Google Hangouts with OffTheRecord ("OTR") encryption (not to be confused with the option in Google to not save "conversation history", which Google then still has access to). All OTR messages were still encrypted and just showed up in my cell data as jibberish, because they had not been stored or accessed by my phone.

- What they call my "timeline": every action (texts, calls, emails, web history, app usage including maps searches, connections to Wi-Fi networks or new cell towers, etc.) with timestamp to be easily sorted.

Co-defendants of mine who also had their phones taken have told me that the data they received back also included:

- Facebook Messenger chats/drafts.
- Data from a phone before it was factory reset.[7]

Emotional Fallout

This wasn't as bad as it could have been, but was worse than I'd been hoping for. I knew that the government could get all this information, but when I was able to see all my personal data together like this in one big spreadsheet, I felt an existential dread that I didn't have words for, because not enough people have been able to feel it yet. What did I have of myself, to myself? The dystopian realization set in that my powerful enemies have so much of my identity: my fingerprints, my retinas, the appearance of my face, intimate emails to and from my friends and lovers through more than a decade, the late night political debates over chat apps that helped shape my values and convictions, documents framing out my life goals, the words and writing patterns I use, the groups that I'm part of that organize via email, how I relate to those groups, the responsibilities I take on in those groups, applications strangers had written to live in my home… The invasiveness felt total and it all hit me at once in a visceral tsunami.

My immediate reaction was to think that nothing was worth this level of intrusion. But I realized that any reason I might be targeted for this kind of privacy violation stemmed from my participation in projects so important to the continuing development of my values, and figuring out how to live my life to align with those values, that I could never regret engaging with them. If you are reading this, it is very likely that these are risks you do or should take seriously. We are fighting against powerful systems of destruction and death, for new possibilities and alternative

[7] A factory reset does not wipe and rewrite over the phone drive enough times that data from before isn't recoverable.

visions of how we can be together with each other and the rest of this earth. To me, those possibilities make this kind of targeting worth it. If you aren't already, it's time to get serious about tech security.

Ten Steps to Consider

This probably makes you want to smash your phone into tiny bits, and by all means, please do. But there are measures you can take to protect your personal data in situations like these. And remember, it's not just your own data, but its information about and between all the contacts stored in your phone as well. Keep your friends and networks safe.[8]

1. If you have a smartphone, encrypt it, NOW. All my codefendants who had encrypted phones had no information taken from them except for their phone numbers.[10] This option should be found in the settings of all Android phones. It is very simple, and just requires an extra password when accessing your phone. The encryption process might take a few hours, so plug in to a safe spot and leave it for awhile. iPhones are generally encrypted automatically.

---

[8] *N.T.P. note:* For our own recommendations on digital security, see our Threat Library's digital best practices.[9]

[9] https://notrace.how/threat-library/mitigations/digital-best-practices.html

[10] *N.T.P. note:* Whether or not Cellebrite devices with physical access to a given encrypted phone are able to extract the phone's unencrypted data is a complex issue. It depends on the state of the phone when accessed (turned off, turned on and locked, or turned on and unlocked), the phone operating system (and whether the operating system is up-to-date), the phone model, and the strength of the encryption password. For example, according to leaked internal Cellebrite documents,[11] as of July 2024, if a phone is accessed when turned on and locked…

- …and it runs stock Android (the default operating system installed on Android phones), Cellebrite devices **can almost always** extract its unencrypted data, no matter the strength of the encryption password.
- …and it is a recent Google Pixel phone running GrapheneOS[12] (an operating system you can install to replace stock Android), Cellebrite devices **cannot** extract its unencrypted data.

We recommend using GrapheneOS for phones.

[11] https://discuss.grapheneos.org/d/14344-cellebrite-premium-july-2024-documentation

[12] https://grapheneos.org

2. Don't bring your phone with you to places or events that have a higher chance of the government getting your phone! We don't always know when we're going to fall into the clutches of our enemies, but we can take precautions if we know there's a high risk. If you do get arrested with your phone, you might want to weigh the option of destroying your phone if you have the chance.
3. Create an email account to only connect to Google Play in Android phones or iTunes for Apple phones. Do not ever connect an email account you use regularly to your phone. If you need to, check your email using a private browser from your phone, rather than through an app.
4. Don't store your contacts' physical or mailing addresses in your phones. Think about the name you use for them in your phone: you may not want to put their full legal name even if you know it. Or it may be worse off for them if you use an identifying code name that connects them to a certain phone number or email address. Is it more helpful or risky to call someone by a name that associates them to a group they work with or the event where you met?
5. Use a private web browser on your phone like Firefox Focus. Orbot is a web browsing app that allows you to use TOR on an Android phone for added anonymity.
6. Don't use the calendar function on your phone. If you do, don't invite others to calendar events or put the physical address of events in the calendar.
7. It is better to connect to social media through private web browsers than through the apps themselves. You may want to consider only connecting to social media through computers instead.[13]
8. A dumb phone might be preferable in some respects, but remember that there is no encryption possible on a dumb phone, both with the information stored on the phone itself and communication

[13]Computers are only safer because you are less apt to have them on your person when being arrested, and therefore it's more difficult for the government to have access to them. The hard drives of your personal computers should also be encrypted for maximum security, especially if you carry a laptop with you often. [*N.T.P. note:* The hard drives of your personal computers should always be encrypted, with strong passwords.]

in transit. Many dumb phones don't even have passwords, so no information (contacts, etc) is even slightly secure.

9. Make a pouch to keep your phone in while not in use lined with aluminum foil. It sounds wingnutty, but your phone cannot connect to cell towers (and thus your location can't be stored) through foil. Just remember to put your phone in airplane mode or switch it off so it doesn't waste battery searching for cell towers while it's in the pouch! Alternatively, you can obtain a fancy case/pouch for your phone called a Faraday cage, which is the same thing just more expensive.[14]
10. If a contact of yours has their phone data collected in this way, you may want to consider changing your phone number.

Luckily, only one of my email accounts had been synced to my phone, and I live a life where I connect with people and groups without technology often. Interestingly and mysteriously, there was some information not present that I expected to be there. And of the many thousands of emails sent and received in the past 11 years, only several thousand were there. I know I am much more than what my phone can give to anyone, and we are always growing and changing through our experiences. While the data they have about me and my communities tells them about my past, I still have control over what information they can obtain going forward. It is definitely worth fighting against their ability to gather more.

For more information about the case, see "We've Got Your Back: The Story of the J20 Defense".[15]

Resources and Further Reading

- Threat modeling is a way to help you find a balance between complete paranoia and having all your info out in the open: ssd.eff.org/module/your-security-plan.

[14] *N.T.P. note:* It can be very difficult to make a pouch that fully blocks phone signals. It can be safer to buy one from a reputable company.

[15] https://crimethinc.com/2019/01/30/weve-got-your-back-the-story-of-the-j20-defense-an-epic-tale-of-repression-and-solidarity

- Step-by-step tutorials for setting up and using digital security tools like encryption from Front Line Defenders: securityinabox.org.
- The Problem with Mobile Phones: ssd.eff.org/en/module/problem-mobile-phones.

I had been arrested at a protest months earlier, and despite my original plans to the contrary, had my unencrypted Android smartphone on me during the arrest. […] The purpose of this text is to inform you of the kind of data cops can easily take from your phone if they have physical access to it, and what you can do to mitigate that, so you can keep yourself and loved ones safe in a wider range of scenarios.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.