Safer Passwords

- Rule of thumb: if you can remember your password, it's probably not secure!
- **Use a password manager**, such as **Bitwarden**, to securely store your strong passwords in one place so you don't need to remember them.
- Enable **2 Factor Authentication (2FA)** wherever possible.

Encrypted Messaging Platforms

- Encrypted messaging services such as **Signal** can help protect conversations.
- Limiting what you share and with who is the best course of action.
- Enable **auto-deleting messages** on Signal for an extra layer of protection. It doesn't matter if your connection was encrypted of you loose posession of your device.

Data Minimization

- Conducting regular audits of settings and services on your phone can help minimize data collection.
- Enable data collection only for services you need when you need them.
- **Disable location access** within apps whenever possible.
- Leaving phones at home when seeking care can limit exposure to location tracking.

Disabling Biometrics

- Police can compel you to open your phone with biometrics under different legal statue than with a password.

Where To Go From Here

https://ssd.eff.org/

https://www.stopspying.org/

https://nysee.nyc/

Safer Browsing: VPNs, TOR, and Other Tools

- **Virtual Private Networks (VPNs)** do not prevent websites you visit from "seeing" it's you, but they can prevent your internet provider from seeing which websites you visit; they should also encrypt your traffic
- **The Onion Router (TOR)** is free and open-source software for enabling anonymous communication. It directs internet traffic via a free, worldwide, volunteer overlay network that consists of more than seven thousand relays
- Tools from the **Electronic Frontier Foundation** like **Privacy Badger** and **Cover Your Tracks** can help minimize exposure to trackers and ad-tech

Insecure Messaging Platforms

Deleted DMs on social media apps are not deleted, but are simply tagged as such.

Those "deleted" DMs and messages on unencrypted platforms such as Facebook Messenger have been used to identify and build cases against abortion seekers, immigrants, protesters, and members of other targeted communities.

Geofences

Geofences are warrants allowing police to collect all phone data that passes through a specific area during a certain period of time. With almost no restrictions on the size or scope, these searches can sweep up huge numbers of people based on location alone.

Resist geofences by limiting the applications that can access your location data!

Ad Tech

Tracking URLs, tracking pixels, and cookies are used to collect data and insights about you and your behavior.

To make a quick buck application developers are all too eager to sell your data to the highest bidder; that often includes the government.

Location Tracking

Location data patterns can be used to identify an individual. If you know some places a person traveled, you can figure out where else they went by seeing who visited those known locations.

The government buys location data with very few restrictions, especially law enforcement. They examine most phone location data and supplement it with other tracking sources, including fingerprinting and ad tech.

IP Address & Browser Fingerprinting

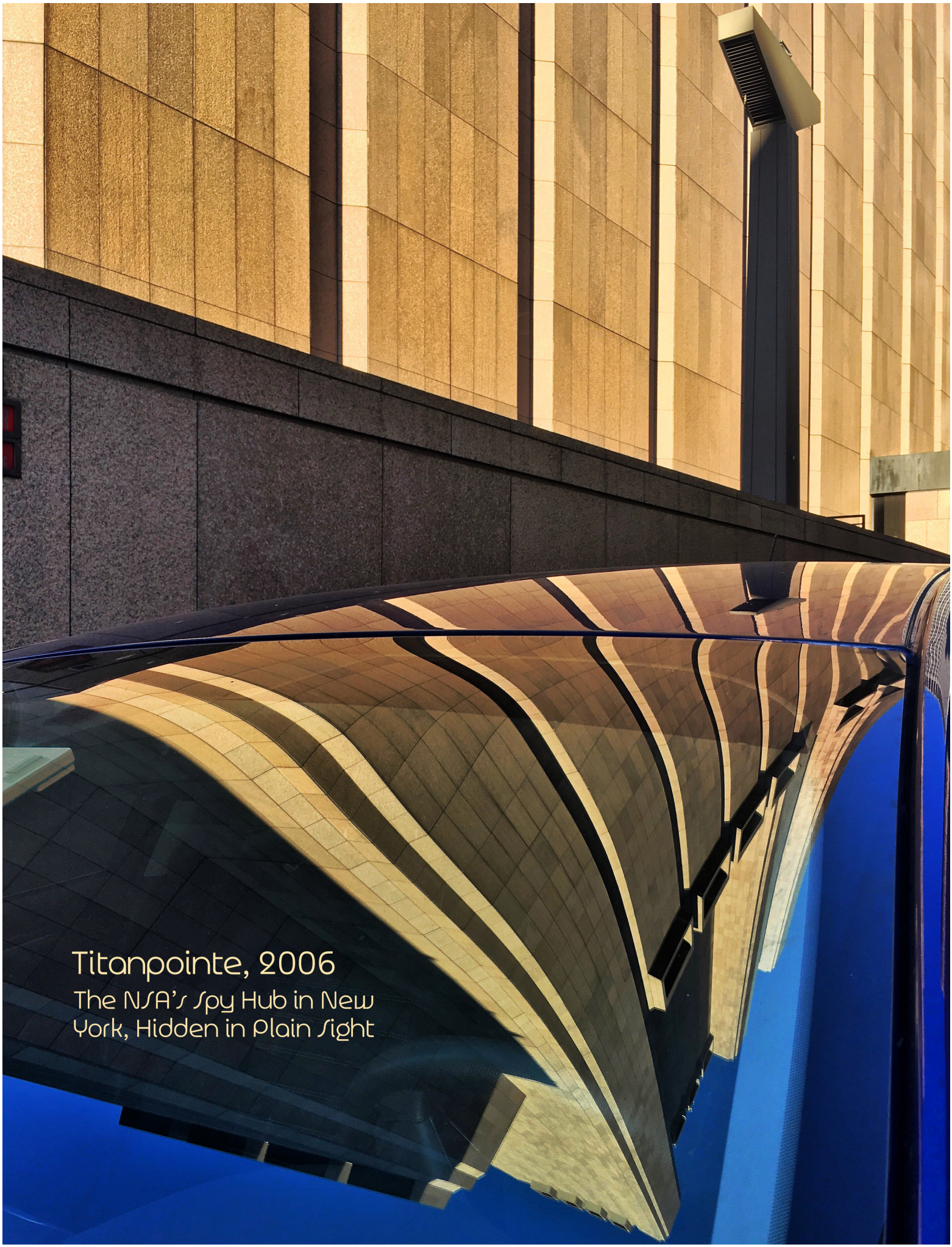
Trackers can see all kinds of details about your browser, and taken together these details often form a unique or near-unique pattern (like a fingerprint).

Companies with trackers across multiple websites can then recognize the pattern as you, and track your browsing habits.

S.T.O.P. created the **Intro to Cybersecurity: Surveillance Resistance Basics** guide to help individuals learn what surveillance looks like and how to protect themselves.

How is our data collected and who has access to it? How do we avoid tracking, hacking, and phishing?

This guide answers these questions and more, sharing surveillance resistance best practices. It has been extended slightly as afforded by the **Creative Commons CC BY-NC** license it was published with.



Titanpointe, 2006

The NSA's Spy Hub in New York, Hidden in Plain Sight