Part 3 –
Invasive Species –
Collecting Our Personal Information

July 6, 10:30am, Cultural Center Theater

Part 3 –
Dealing With Invasive Species –
Protecting Our Personal Information

July 6, 10:30am, Cultural Center Theater

Executive Summary

Many organizations, government and private, want our personal information for a variety of reasons

We can’t hide, we must provide some personal information in order to function in society

Artwork: OpenClipart-Vectors, pixabay

Executive Summary

We all have some personal information that we want to keep private, sharing only with those we trust

There are ways to keep that personal information private when sharing

Artwork: OpenClipart-Vectors, pixabay

Many organizations, government and private, want our personal information for a variety of reasons

Office of the Director of National Intelligence

Senior Advisory Group

Panel on Commercially Available Information

27 January 2022

Declassified 9 June 2023

Source: https://s3.documentcloud.org/documents/23843212/odni-declassified-report-on-cai-january2022.pdf

Why Was The Report To The DNI Written?

"Given the increasing volume of data that is commercially available, I … asked them to make recommendations … regarding how and under what circumstances the IC [Intelligence Community] should use commercially available information, and … to reflect on … ensuring the protection of privacy and civil liberties…"

Source: ODNI News Release No. 15-23 June 14, 2023

What Is Commercially Available Information?

"… CAI is information that is available commercially to the general public … [and] is a subset of publicly available information (PAI)… "

Source: Report on CAI, Executive Summary, page 1

What Is Publicly Available Information?

"PAI is … information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer (but not amounting to physical surveillance), is made available at a meeting open to the public, or is observed by visiting any place or attending any event that is open to the public."

Source: Report on CAI, Background on CAI, page 2

Who Sells CAI?

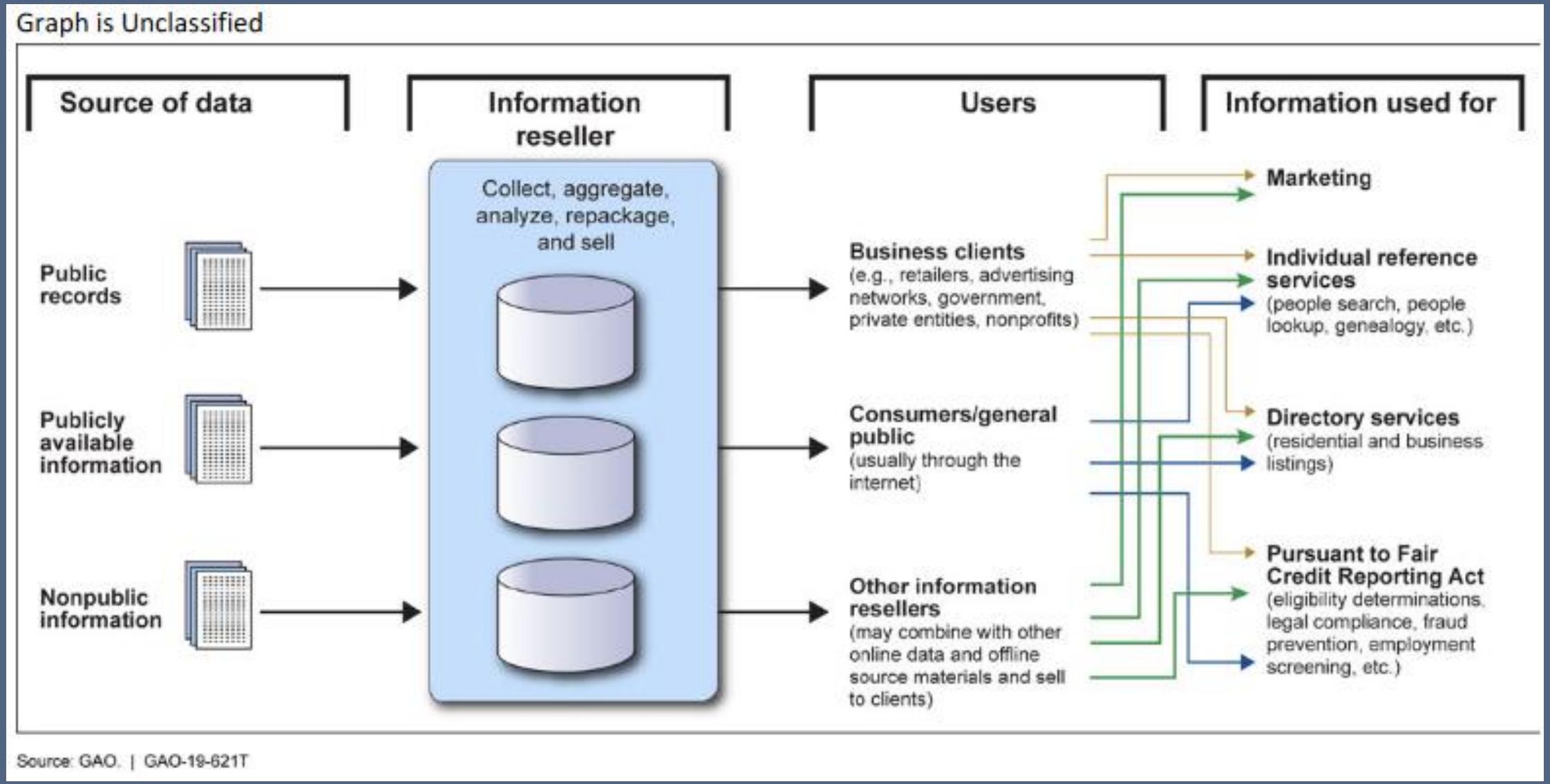
"…CAI..is often sold or otherwise made available by commercial entities…often referred to as "data brokers" or "information resellers." [They] maintain large, sophisticated databases with consumer information that can include credit histories, insurance claims, criminal records, employment histories, incomes, ethnicities, purchase histories, and interests...

Source: Report on CAI, Background on CAI, page 2

What Information Do Data Brokers Collect?

"Data brokers collect data from commercial, government, and other publicly available sources. Data collected could include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions."

Source: Report on CAI, Background on CAI, page 3



Source: Report on CAI, Background on CAI, page 3

Identifying Individuals Using CAI

"The volume and sensitivity of CAI … have expanded in recent years … due to the advancement of digital technology, including location-tracking and other features of smartphones and other electronic devices, and the advertising-based monetization models … Although CAI may be "anonymized," it is often possible (using other CAI) to deanonymize and identify individuals, including U.S. persons."

Source: Report on CAI, Executive Summary, page 1

Potential Misuse of CAI

"CAI can reveal sensitive and intimate information about the personal attributes, private behavior, social connections, and speech of U.S. persons and non-U.S. persons. It can be misused to pry into private lives, ruin reputations, and cause emotional distress and threaten the safety of individuals. … CAI can increase the power of the government's ability to peer into private lives to levels that may exceed our constitutional traditions or other social expectations…"

Source: Report on CAI, Background on Commercially Available Information, page 11

Has The Supreme Court Ruled In This Area?

In *Carpenter v. United States*, a case about accessing cell-site location information without a warrant, the Supreme Court ruled in 2018, the "data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' These location records 'hold for many Americans the 'privacies of life.'"

Summary: The Supreme Court ruled that accessing cell phone location records requires a warrant under the Fourth Amendment. The Court also identified sensitive personal information

Source: Report on CAI, Background on CAI, page 12

Source: https://americandragnet.org/

Center on Privacy & Technology's Summary

"When you think about government surveillance in the United States, you likely think of the National Security Agency or the FBI. You might even think of a powerful police agency, such as the New York Police Department. But unless you or someone you love has been targeted for deportation, you probably don't immediately think of Immigration and Customs Enforcement (ICE)."

Source: https://americandragnet.org/

Center on Privacy & Technology's Summary

"This report argues that you should. Our two-year investigation … reveals that ICE now operates as a domestic surveillance agency. Since its founding in 2003, ICE has not only been building its own capacity to use surveillance to carry out deportations but has also played a key role in the federal government's larger push to amass as much information as possible about all of our lives… "

Source: https://americandragnet.org/

Center on Privacy & Technology's Summary

"… In its efforts to arrest and deport, ICE has – without any judicial, legislative or public oversight – reached into datasets containing personal information about the vast majority of people living in the U.S., whose records can end up in the hands of immigration enforcement simply because they apply for driver's licenses; drive on the roads; or sign up with their local utilities to get access to heat, water and electricity… "

Source: https://americandragnet.org/

Cell phone tracking

Carpenter v. United States

... A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user. …

Source: https://constitutioncenter.org/the-constitution/supreme-court-case-library/carpenter-v-united-states

How Is An Individual's Information Collected?

When we use hardware or software, we agree to abide by that hardware's or software's privacy policy which states what information will be collected and how it will be used.

Tracking Your Phone

Each phone has a unique hardware ID:
International Mobile Equipment Identity (IMEI)

The IMEI is used to track phones

It is very difficult to change most phone's IMEI

Source: https://www.kicksecure.com/wiki/Mobile_Phone_Security#Data_Harvesting_by_Most_Phones

How Do I Avoid Phone Tracking?

Get a phone that is not connected to your identity

- burner cell phone

Burner Cell Phone – Getting One and Using It

Leave your cell phone home!

Purchase a burner phone with cash – Walmart, etc

Put the burner phone in an RFID bag/sleeve before getting into your car

Never turn on your burner phone and cell phone in the same location at the same time

Source: https://www.kicksecure.com/wiki/Mobile_Phone_Security#Data_Harvesting_by_Most_Phones

RFID Bag/Sleeve

The company with the highest reputation for RFID shielding is Silent Pocket at slnt.com

They make

- bags
- sleeves
- credit card wallets
- clutch purses
- wallets
- passport wallets

Source: https://slnt.com

Burner Cell Phone – Using It

If you want to use your burner phone, leave your cell phone home!

Take your burner phone out of the RFID bag/sleeve only after you are several miles from home – approximately 3 miles

Put the burner phone back in the RFID bag/sleeve when approximately 3 miles from home

Source: https://www.kicksecure.com/wiki/Mobile_Phone_Security#Data_Harvesting_by_Most_Phones

Hacking Your Phone's Bluetooth

Coffee shops, fast food restaurants, etc.

Bluesnarfing can happen without your knowledge – up to 300 feet away

Can access and steal contact information, emails, calendar entries, passwords, photos, and other Personally Identifiable Information

Turn Bluetooth OFF in these settings or use an RFID bag/sleeve

Sources: https://www.makeuseof.com/keep-bluetooth-secure/?newsletter_popup=1

Hacking Your Phone's Bluetooth

Bluebugging is the most malicious Bluetooth hack. The hacker can get full access and control of the device without your knowledge.

Can listen to and make phone calls, read and reply to text messages, and gain access to online accounts or apps

Turn Bluetooth OFF in these settings or use an RFID bag/sleeve

Sources: https://www.makeuseof.com/keep-bluetooth-secure/?newsletter_popup=1

Accessing Credit Cards and Passports

Passports have an RFID feature that can be read by others

Credit cards with the tap-to-use feature can be read by others

Use an RFID bag, sleeve, wallet, purse, etc to protect them

Source: https://www.kicksecure.com/wiki/Mobile_Phone_Security#Data_Harvesting_by_Most_Phones


SLNT

Car location tracking

Tracking Your Car's Location

"… personally identifiable information collected, generated, recorded, or stored in … in vehicles … can be retrieved by or on behalf of Honda…"

Source: https://www.honda.com/privacy/connected-product-privacy-notice

Tracking Your Car's Location

"…The Privacy Principles provide additional, heightened protections for the most sensitive types of consumer in-vehicle data, such as geo-location, driver behavior, and biometric data."

Source: https://www.honda.com/privacy/connected-product-privacy-notice

Tracking Your Car's Location

"We cooperate with government and law enforcement officials and private parties to enforce and comply with the law. We may use and disclose Covered Information and any other information about you to government or law enforcement officials or private parties if, in our discretion, we believe it is necessary or appropriate to respond to legal requests (including court orders, investigative demands and subpoenas), to protect the safety, property, or rights of ourselves, consumers, or any other third party, to prevent or stop any illegal, unethical, or legally actionable activity, or to comply with law."

Source: https://www.honda.com/privacy/connected-product-privacy-notice

Tracking Your Car’s Location

Honda does not provide any way to turn off location tracking

Source: https://www.honda.com/privacy/connected-product-privacy-notice

Many Of Us Use Google
Gmail, Chrome, Google Docs, etc.

What Information
Does Google Collect?

Google Collects

"The activity information we may collect include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services

Source: https://policies.google.com/privacy#infocollet Effective July 1, 2023

Google Collects

"We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos."

Source: https://policies.google.com/privacy#infocollect Effective July 1, 2023

Google Collects

"If you use our services to make and receive calls or send and receive messages, we may collect call and message log information like your phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages."

Source: https://policies.google.com/privacy#infocollect Effective July 1, 2023

Google Collects

"We collect information about your location when you use our services, which helps us offer features like driving directions, search results for things near you, and ads based on your general location."

Source: https://policies.google.com/privacy#infocollect Effective July 1, 2023

We must provide some personal information in order to function in society

Personal Information

Personal preferences

Personal attributes

Personally identifying information (PII)

Personally sensitive information

Personal Information

Personal preferences –

- styles
- colors

Personal attributes –

- clothing sizes
- shoe size

Personally Identifiable Information (PII)

Public

Semi-Private

Private

Public PII

- Your name
- Your U.S. mail address
- Your email address
- Your home phone
- Your cell phone

Semi-Private PII must be provided to

Obtain services such as health care

Pay taxes

Hold a job

Do online shopping

Be allowed to drive or fly

Semi-private PII includes

- Your date of birth
- Your place of birth
- Your Social Security number
- Your driver’s license number
- Your mother’s maiden name
- Your photograph
- Your race
- Your religion
- Your bank account numbers
- Your credit card numbers
- Your passwords
- Your Medicare number, if applicable

Semi-private PII also includes

Your taxpayer identification number

Your health insurance numbers

Your professional associations

Your educational achievement

Your trade associations

Your hobby associations

Private PII includes

- Your DNA
  - Unless you provided it to a genealogy site
- Your biometric data
  - Fingerprints, retina scans, voice signatures, facial geometry
  - Unless you are required to provide it to your employer or law enforcement

We can protect our personal information when we
use reputable websites and
a privacy focused browser

Use Reputable Websites

Don’t browse aimlessly

Don’t check out websites that might be interesting

Have a purpose for going to a website

Browsers

There are many browsers. Many do not respect your privacy

Chrome is very popular

It feeds everyone's personal information to Google

The most respected browser for privacy is Firefox

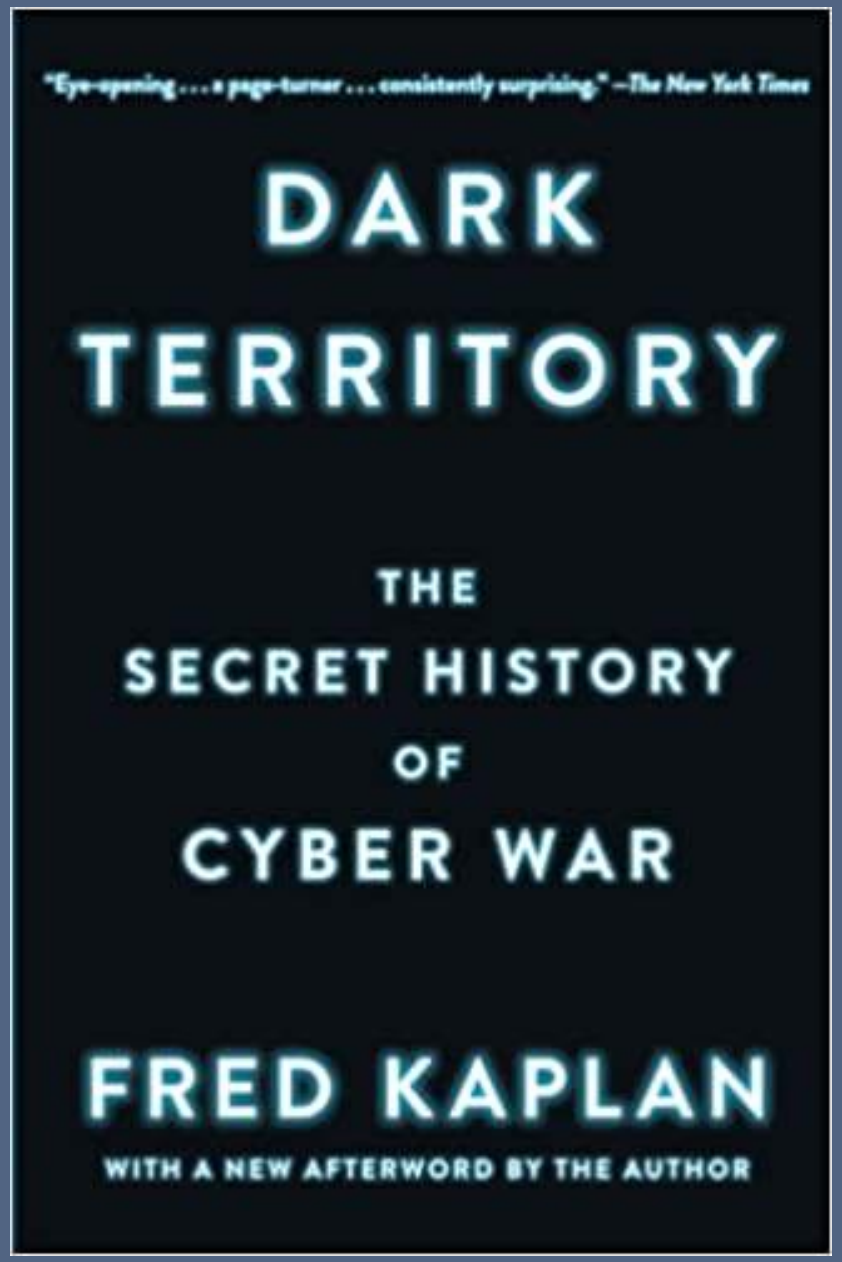
On iPhones, Safari should be used. Apple restricts the features that Firefox may offer on an iPhone.

Browsers - Firefox

Although many extensions are available for Firefox, for most users only one is needed: uBlock Origin

uBlock Origin blocks ads and other content

We can protect our personal information by using reputable hardware
and ensuring that the settings protect us



Simon & Schuster Paperbacks, Trade Edition, 2017

The Internet' Beginnings

In the late 1960's, the Department of Defense started the ARPANET project.

In April 1967, Willis Ware of Rand Corporation recognized the security problems and wrote a paper "Security and Privacy in Computer Systems" in which he laid out the risks.

ARPANET's chief scientist convinced ARPANET's deputy director not to add security requirements at that time but to add it later.

Source: *Dark Territory*, pages 7-9

The Current Internet

The Internet has a lot of security holes

Most websites, especially banks and investment firms, use software to protect their customers and visitors from those holes

- Secure information transmission
- Authenticators such as Authy
- Hardware security keys
- Passwordless authentication

Major Nation-State Actors

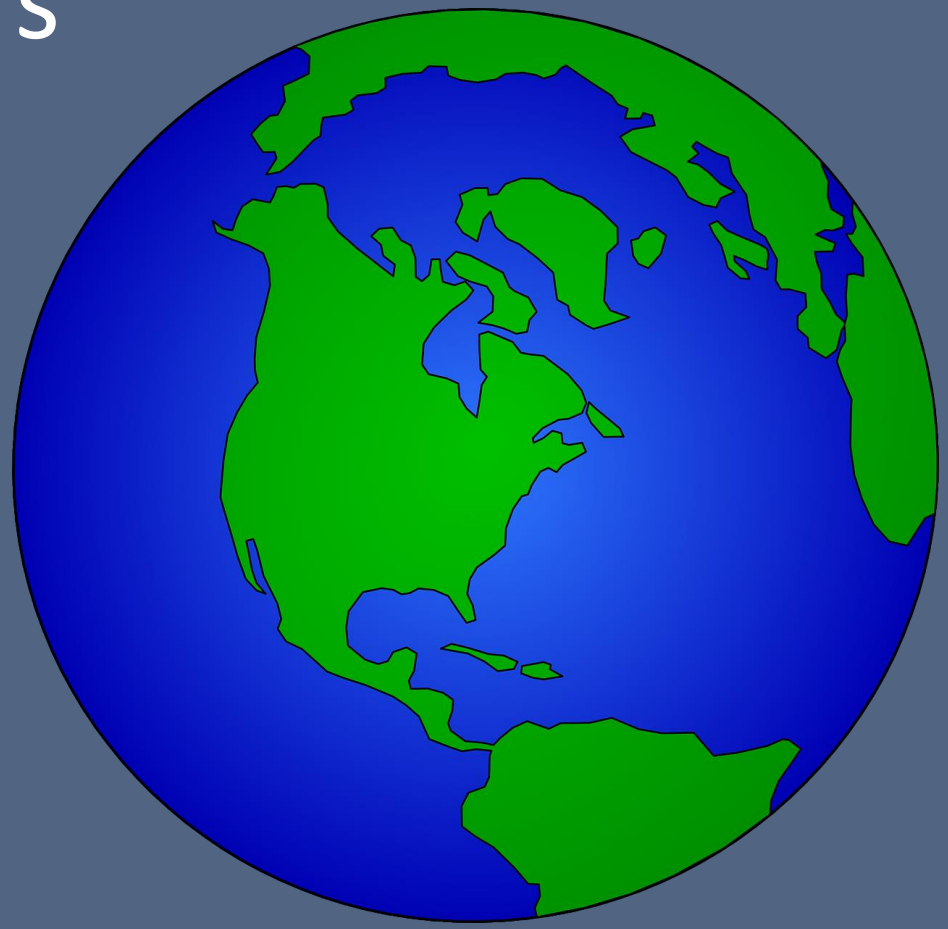
China

Iran

North Korea

Russia

U.S.A



Pixabay.com

Are These Actors A Threat To Individuals?

- They tend to be interested in sets of individuals
- In June, 2015, the Office of Personnel Management suffered a data beach which exposed 21.5 million individuals with federal security clearances
- The breach included Social Security Numbers and information related to background investigations

Are These Actors A Threat To Individuals?

However, there is a Chinese actor:

"…Volt Typhoon tries to blend into normal network activity by routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware... "

https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

What Is Volt Typhoon Doing?

"… Microsoft has confirmed that many of the devices, which include those manufactured by ASUS, Cisco, D-Link, NETGEAR, and Zyxel, allow the owner to expose … management interfaces to the internet... "

https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

What Can I Do?

Log into your router and turn off Remote Management

- If you have Comcast, you likely won't be able to turn this off

While logged in, turn off Universal Plug and Play (UPnP)

- If Comcast allows you to turn off UPnP, do so

If you use your cell phone at other Wi-Fi locations, turn your phone off and then on after you leave that location

What Can I Do?

Don’t purchase hardware (PC, laptop, phone, modem, router) made by companies headquartered in China

Most hardware is reliable for 5 to 7 years. Replace unwanted hardware at the end of its reliable life.

Many companies have a supply chain that uses companies in China. Brand reputation will force those companies to ensure that their products do not contain malicious hardware.

We all have some personal information that we want to keep private, sharing only with those we trust

Personally Sensitive Information

Familial

Political

Professional

Religious

Sexual Association

We select the personal information
we want to keep private

I want to keep financial, medical, and
user account information (username and password) private

There are ways to keep personal information private when sharing

Text Messages – iPhone and Android

- Text messages are sent between phones
- Text messages are not encrypted in transit when sent between
  - iPhone and Android
  - Android and Android
- These text messages provide no privacy

Text Messages – iPhone to iPhone

- iMessages are encrypted in transit
- If Standard data protection (default) is used, iMessages are stored encrypted in iCloud and the encryption keys are sent to Apple
- If Advanced Data Protection for iCloud is selected (available in iOS 16.2 and later), iMessages are stored encrypted in iCloud but the encryption keys remain on your phone

Source: https://support.apple.com/en-us/HT202303

We need to be aware of what information is collected by the software we are using

WhatsApp

Provides encrypted text messages, calls, photos, videos, voice messages, documents, and status updates

Source: https://faq.whatsapp.com/820124435853543

WhatsApp Privacy Policy

"We collect device and connection-specific information when you install, access, or use our Services. This includes information such as hardware model, operating system information, battery level, signal strength, app version, browser information, mobile network, connection information (including phone number, mobile operator or ISP), language and time zone, IP address, device operations information, and identifiers…"

Source: https://www.whatsapp.com/legal/privacy-policy

WhatsApp Privacy Policy

We collect and use precise location information from your device with your permission when you choose to use location-related features… Even if you do not use our location-related features, we use IP addresses and other information like phone number area codes to estimate your general location (e.g., city and country).

Source: https://www.whatsapp.com/legal/privacy-policy

Signal

All messages, attachments, voice calls, and video calls are encrypted at all times. They are never collected and are stored locally [on your device].

Source: https://support.signal.org/hc/en-us/articles/360007059412-Signal-and-the-General-Data-Protection-Regulation-GDPR-

Signal Privacy Policy

You register a phone number when you create a Signal account. Phone numbers are used to provide our Services to you and other Signal users. You may optionally add other information to your account, such as a profile name and profile picture. This information is end-to-end encrypted.”

Source: https://signal.org/legal/

Signal – Grand Jury Requests For Data

Signal knows only

- the date and time the account was created and
- the last date and time the account was accessed

Source: https://signal.org/bigbrother/

Interview About ProtonMail

"Andy Yen, Proton's CEO, told me that he doesn't expect you to quit Gmail or whatever email provider you're using.

"Yen imagines Proton as the place for communications that you want to keep private, like those among your friends and family or email related to your finances and health.

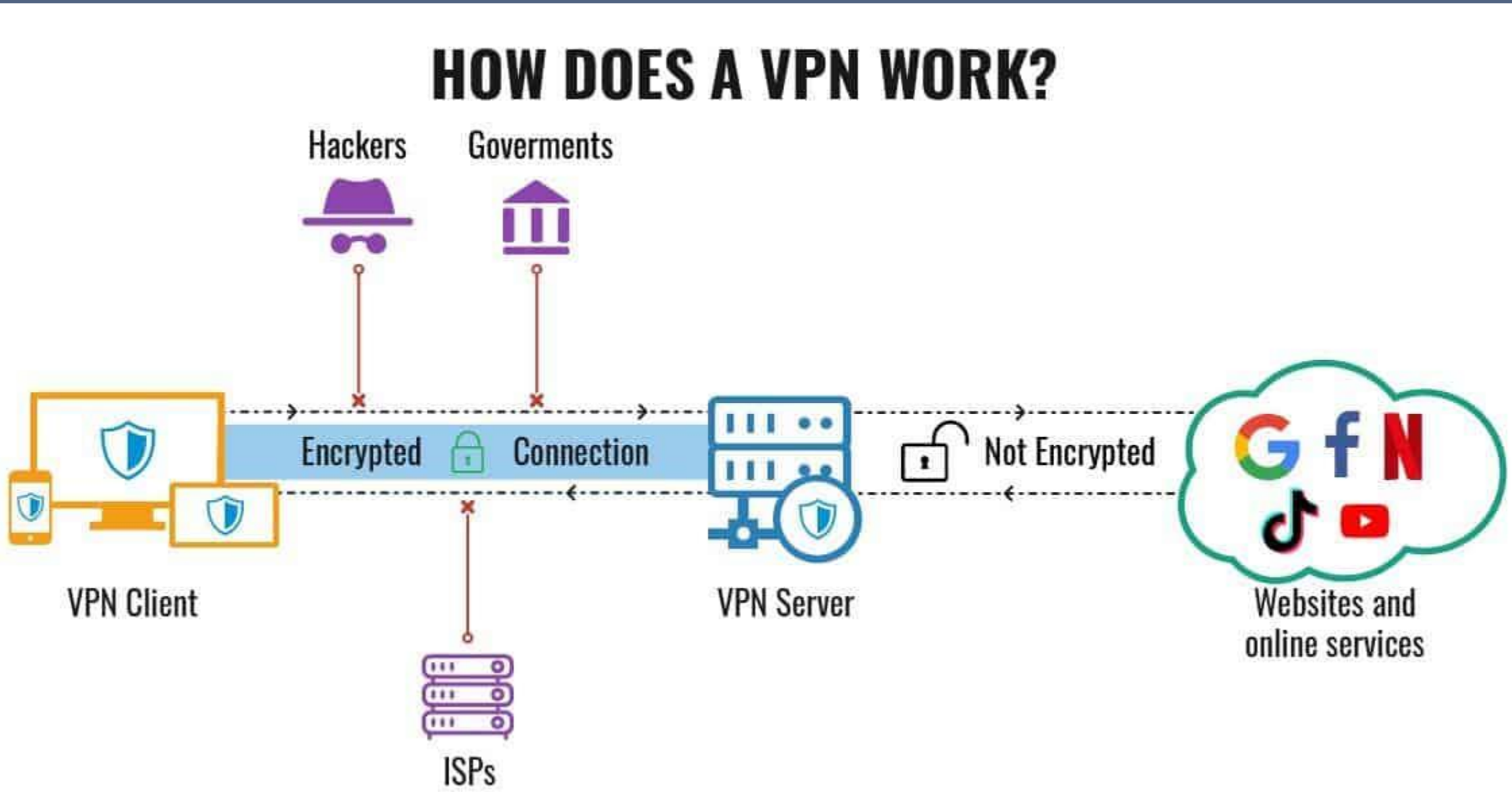
"'Our goal is not to be the only email account you use,' Yen said. 'It's to be the email account for things that matter.'"

Source: *The Tech Friend*, Shira Ovide, The Washington Post, June 26, 2023

ProtonMail Privacy Policy

Proton cannot see the contents of the encrypted message body

Source: https://proton.me/legal/privacy



Source: https://www.comparitech.com/blog/vpn-privacy/vpn-tunneling/

Why Would I Use A VPN?

To change your geo-location

To watch Netflix while out of the country

To prevent surveillance while in another country

Many VPN Providers Make Misleading Claims

A VPN does not prevent malware

A VPN does not prevent access to malicious websites

A VPN does not provide anonymity because a browser can be fingerprinted

Source: https://proton.me/legal/privacy & https://protonvpn.com/support/no-logs-vpn/

ProtonVPN Privacy Policy

Proton VPN is a no-logs VPN service… All of the Proton VPN servers are encrypted …

Source: https://proton.me/legal/privacy & https://protonvpn.com/support/no-logs-vpn/

Your Phone's Hotspot

You may use your phone's hotspot to avoid public Wi-Fi

You may want to use a VPN with the hotspot for privacy

The VPN software must be on your device that is connecting to the hotspot, not on your cell phone

- cell phones use one network for the phone
- and a separate network for the hotspot

Anonymity – Tor Browser

The Tor Browser is easy to use. It's just like any other browser except that it uses Tor.

The Tor Browser provides anonymity because your traffic is randomly routed through three servers

How To Geek has a guide:

How to Browse the Web Anonymously: A Simple Guide

Source: https://www.howtogeek.com/845566/how-to-browse-anonymously-a-simple-guide/

Summary

Data brokers collect our personal information and sell it

We must provide some personally identifying information in order to live in our society

There are apps which will protect our personally sensitive information

It is good practice to replace hardware made by companies headquartered in China

Questions?