Willow Valley Computer Club

Member of
apcug An International Association of Technology & Computer User Groups

Project Upskill II

Do You Really Know What You're Agreeing To?

Unpacking Privacy Policies

Al Williams   **June 5, 2025**

Information isn't a luxury –
it is the very basis of our survival.

...[we] need information to:
    live;
    understand and adapt to our environment;
    maintain relationships and cooperate with others; and
    make wise decisions that further our interests.

The control of our information isn't a luxury – it is the very basis of our survival.

We need to control the information about ourselves to ensure our safety and autonomy.

Source: *Privacy Is Power – Why and How You Should Take Back Control of Your Data*, Carissa Veliz, (Melville House, 2021)

Source: *Why Privacy Matters*, Neil Richards, (Oxford University Press, 2022)

Source: *Nothing to Hide – The False Tradeoff between Privacy and Security*, Daniel J. Solove, (Yale University Press, 2011)

Why We Need to Control Access to Our Information

Maintaining autonomy and agency

Protecting against harm

Preserving privacy and dignity

Ensuring security

Fostering trust and relationships

Empowering informed decision-making

Maintaining Autonomy and Agency

When our personal information is exposed or misused, it can limit our choices and manipulate our behavior. Controlling our data helps us maintain our independence and make decisions free from undue influence.

Protecting Against Harm

In the cybersecurity context, the lack of control over personal information can lead to direct harm, such as
identity theft,
financial fraud,
reputational damage, and even
physical threats in certain situations (e.g., doxxing – publishing private or identifying information on the Internet with malicious intent)

Preserving Privacy and Dignity

Unwanted exposure of personal details can violate our sense of privacy and dignity. Controlling what is known about us allows us to maintain a sense of personal space and boundaries.

Ensuring Security

Limiting the amount of personal information available online reduces our attack surface for cybercriminals and malicious actors.

Fostering Trust and Relationships

Knowing that our personal information is protected can foster greater trust in online interactions and platforms. Conversely, breaches of trust due to data leaks can damage relationships and erode confidence.

Empowering Informed Decision-Making

Understanding what data is being collected and how it's being used allows us to make more informed decisions about the services we use and the information we share.

Why We Need to Control Access to Our Information

Maintaining autonomy and agency ✔

Protecting against harm ✔

Preserving privacy and dignity ✔

Ensuring security ✔

Fostering trust and relationships ✔

Empowering informed decision-making ✔

How Do We Protect Our Information?

Prevention or Mitigation

Detection

Response

Why Project Upskill?

The effective protection of personal information depends upon:
best practices,
effective software and hardware products, and an
effective cybersecurity architecture.

The Cybersecurity Architecture

Defense in Depth

Least Privilege

Separation of Duties

Secure by Design

Keep It Simple Stupid

~~Security by Obscurity~~

Why Project Upskill?

The Cybersecurity & Infrastructure Security Agency (CISA) collaborated with other US and International partners to create Project Upskill, cybersecurity guidance for high-risk communities.

Project Upskill provides users with simple steps to improve their cybersecurity.

Why Project Upskill?

While none of these steps will offer complete protection against cyber intrusions, this combination of best practices will make it harder to target high-risk individuals and organizations.

They will also limit opportunities for attackers that leverage common techniques such as ransomware or malware.

Why Project Upskill II?

Anyone over 55 who uses a computing device (iPhone, laptop, etc.) is at higher-risk due to data breaches revealing our ages.

The Willow Valley Computer Club's Project Upskill II extends CISA's Project Upskill to include illustrations, examples, additional material, suggestions, and recommendations.

After completing Project Upskill II, you should feel more confident that you can implement basic cybersecurity practices.

Risk Analysis and Risk Tolerance

Risk analysis is the process of identifying potential threats, evaluating their likelihood of occurrence, and estimating their potential impact, enabling informed decision-making and minimizing negative outcomes.

Risk tolerance is about knowing yourself.

Threat modeling considers both risk analysis and risk tolerance.

Risk Tolerance Considerations

Confidentiality – Ensuring that information is accessible only to authorized individuals, entities, or processes.

Integrity – Maintaining the accuracy and completeness of information and ensuring that it is not altered or corrupted.

Availability – Ensuring authorized users have timely and reliable access to information and resources when needed.

Source: *Cybersecurity Architecture: Fundamentals of Confidentiality, Integrity, and Availability*, Jeff Crume, IBM Technology, https://www.youtube.com/watch?v=EqNe55IzjAw, June 7, 2023

Our Recommendations

We understand that choosing new software or hardware can be overwhelming if you're unfamiliar with the topic and do not have the time to research the details.

Think of our recommendations as we helping you based on our knowledge of what works well with effective cybersecurity.

Our recommendations assume that your risk tolerance is low.

You are not required to use our recommendations.

Clarifying Our Cybersecurity Recommendations

An understanding of computer concepts will clarify our recommendations.

Exploring our source notes (on most slides) will help you build this foundation.

For hands-on experience, try our workshops (e.g., Bitwarden).

Small learning steps will go a long way in protecting your digital life with confidence.

The Project Upskill II Series – Where we're going.

Your Personal Information and Other Risks

We often focus on the visible risks to our data, like device security. However, hidden risks, such as overlooked privacy policies, can be just as damaging. This privacy-oriented presentation sheds light on this crucial area with suggested solutions.

Protecting Your Personal Information on Your Devices

To ensure the security of your personal data on your computing devices, we provided a layered security approach including:
implementing basic cybersecurity,
preventing account breaches, and
ensuring the protection of your stored data.

Three classes

Protecting Your Personal Information Out There

To ensure the security of your personal data that isn't on your computing devices, we provide ways to

protect your data in transit,

secure your home Wi-Fi,

manage your privacy and security online, and

use Virtual Private Networks (VPNs) appropriately.

Four classes

Your personal information is valuable.

Which personal information?

Your identifying information
  Name, address, date of birth, Social Security Number, etc.

Your financial information
  Bank accounts, investment accounts, credit cards, etc.

Other information of a personal nature

We unknowingly simultaneously
give our personal information away
while
working to protect it

We give away a lot of
identity and financial information.

I'll provide examples to illustrate the scope.

I'll also drill down deeper to show how identity and financial information can be used to harm us.

This presentation identifies ways in which your personal information is disclosed, either legally or illegally, through your own choices.

This presentation sets the stage for the next seven presentations, showing how to significantly reduce personal information exposure or loss due to physical access or cybersecurity breaches.

Updated Project Upskill II Classes

- Unpacking Privacy Policies
- Basic Cybersecurity for Personal Computers and Mobile Devices
- Protecting Your Accounts from Compromise
- Protecting Data Stored on Your Devices
- Protecting Data in Transit
- Securing Your Home Router
- Unseen Access: Dealing with Intruders
- Virtual Private Networks

When you watch TV or read the news, you frequently hear about data breaches that reveal millions of people's personal information, such as birth dates, cell phone numbers, email addresses, etc.

Your personal information has likely been exposed.

Perhaps you know people who have been scammed, lost money, had credit cards stolen, lost access to accounts, or had similar experiences.

Perhaps you've been scammed.

Whether your information has been exposed or you've been scammed, we all deal with scammers, criminals, and organizations that want our personal information.

How Did We Get to Where We Are?

In 1993, the software and protocols that made the world wide web accessible were released

It was a time of rapid growth and change.

Users enthusiastically embraced social media platforms like Facebook, using them to share a wide range of personal details with family and friends.

How Did We Get to Where We Are?

Most users choose software apps based mainly on the features and how convenient they are to use

Users are usually unaware of possible personal information disclosure.

Users typically do not want to pay for apps, but software developers need money to cover their costs, and they began selling personal information.

Is this use of our personal information legal?

Supreme Court Rulings – Third-Party Doctrine

In 1976 (*United States v. Miller*) and 1979 (*Smith v. Maryland*), the Supreme Court affirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

Source: *The Third-Party Doctrine and the Fourth Amendment*, Dmitry Gorin, https://www.thefederalcriminalattorneys.com/third-party-doctrine, December 08, 2023

Executive Order 12333

President Ronald Reagan signed *Executive Order 12333, United States Intelligence Activities*, on December 4, 1981, to provide for the effective conduct of US intelligence activities and the protection of constitutional rights.

2.3 *Collection of information*. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures ...

2.3 (a) Information that is publicly available or collected with the consent of the person concerned;

The issue is the use of our personal information when it is
publicly available or given by consent.

There are some laws
which put limits on the Third-Party Doctrine
thereby protecting some use of
our personal information.

Many organizations
have privacy policies
which ask for our consent
to use our personal information

The European Union's
General Data Protection Regulation (GPDR)
requires
privacy policies

Google's Privacy Policy

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"

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."

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."

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."

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"

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."

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."

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."

WhatsApp's Privacy Policy

WhatsApp

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

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..."

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)."

Your car and your privacy

Your Car and Your Privacy

How does my car collect data about me?
      Microphones, cameras, and sensors
      Connected services in your car
      Devices you connect to the car

Source: *What Data Does My Car Collect About Me and Where Does It Go?*, Mozilla Foundation, https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go//, September 6, 2023

Your Car and Your Privacy

What data does my car collect about me?

       What you do,

       Where you go,

       What you say, and

       How you move your body

       Nissan collects sexual activity, genetic information, etc.

Source: *What Data Does My Car Collect About Me and Where Does It Go?*, Mozilla Foundation, https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go//, September 6, 2023

Your Car and Your Privacy

"All 25 car brands we researched earned our "Privacy Not Included warning label – making cars the official worst category of products for privacy that we have ever reviewed."

1. They collect too much personal data (all of them)
2. Most (84%) share or sell your data
3. Most (92%) give drivers little or no control over their personal data
4. We couldn't confirm whether any of them meet our Minimum Security Standards (including whether personal data is encrypted)

Source: *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, Mozilla Foundation, https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy , September 6, 2023

Your Car and Your Privacy

Honda says they collect "Personal Information" [which] means anything that identifies, relates to, describes, or is capable of being associated with a particular individual including, but not limited to his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

Source: *What Data Does My Car Collect About Me and Where Does It Go?*, Mozilla Foundation, https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go//, September 6, 2023
Source: *Honda*, Privacy Not Included, Mozilla Foundation, https://www.mozillafoundation.org/en/privacynotincluded/honda/, August 15, 2023

Your Car and Your Privacy

"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

Your Car and Your Privacy

The 2024 Honda CR-V offers users a data-sharing option, but if you turn off data-sharing because you want to turn off location tracking, you also turn off desirable services

This collected
personal information
is sometimes known as
Commercially Available Information (CAI)

Office of the Director of National Intelligence

Senior Advisory Group

Panel on Commercially Available Information

27 January 2022

Declassified 9 June 2023

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

Who Sells Commercially Available Information?

"…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…

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
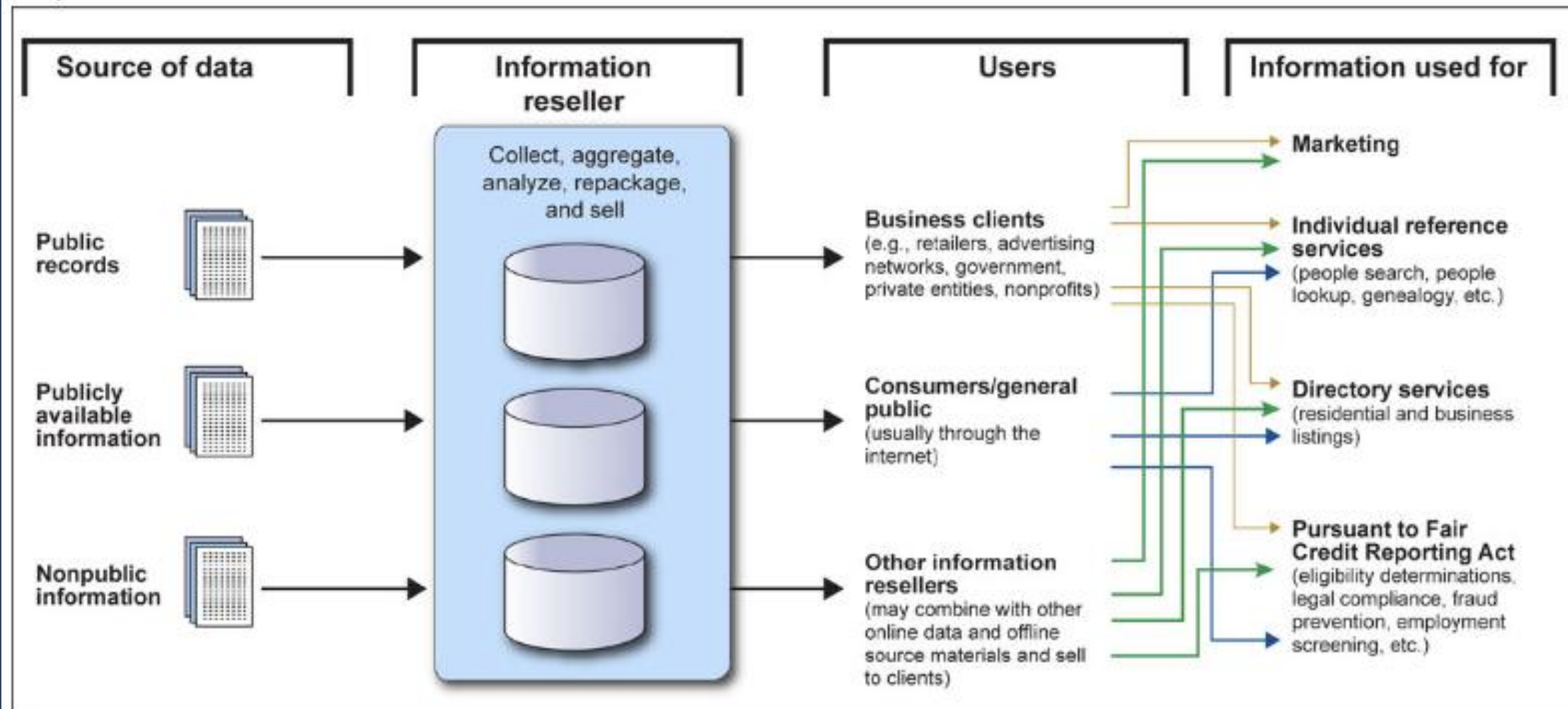
Identifying Individuals Using CAI

"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."

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

Misuse of Identity & Financial Information

When data breaches occur, our identity and financial information can be used by another person for:

Financial identity theft – for financial gain

Medical identity theft – to obtain medical services

Criminal identity theft – giving your identity to law enforcement

Synthetic identity theft – to merge identity information to create a new identity

We can reduce
the collection of our personal information
by apps and websites
by limiting the information we give and
through non-consent to privacy policies.

What is the Most Valuable Personal Information?

The geolocation information is the single most valuable piece of commercially available data

To deliver targeted advertising based on location (nearby)

To measure the responsiveness of nearby people

For planning and investment decisions

And for surveillance

Source: *Means of Control: How the Hidden Alliance of Tech and Government is Creating a New American Surveillance State*, Byron Tau, (Crown, 2024), Kindle edition, pages xxi - xxii

What could be done with
our personal location information?

Cell phone tracking

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

Cell Phone Location Tracking

Someone hired data broker *Near Intelligence* to collect the locations of over 200 cell phones that went to and from Jeffrey Epstein's island.

The data showed the location of each phone to within centimeters.

Source: *We Tracked Every Visitor to Epstein Island*, Dhruv Mehrotra, https://www.wired.com/video/watch/we-tracked-every-visitor-to-epstein-island, (Wired, 11/2/2024)

Source: *We Tracked Every Visitor to Epstein Island*, Dhruv Mehrotra, https://www.wired.com/video/watch/we-tracked-every-visitor-to-epstein-island, (Wired, 11/2/2024)
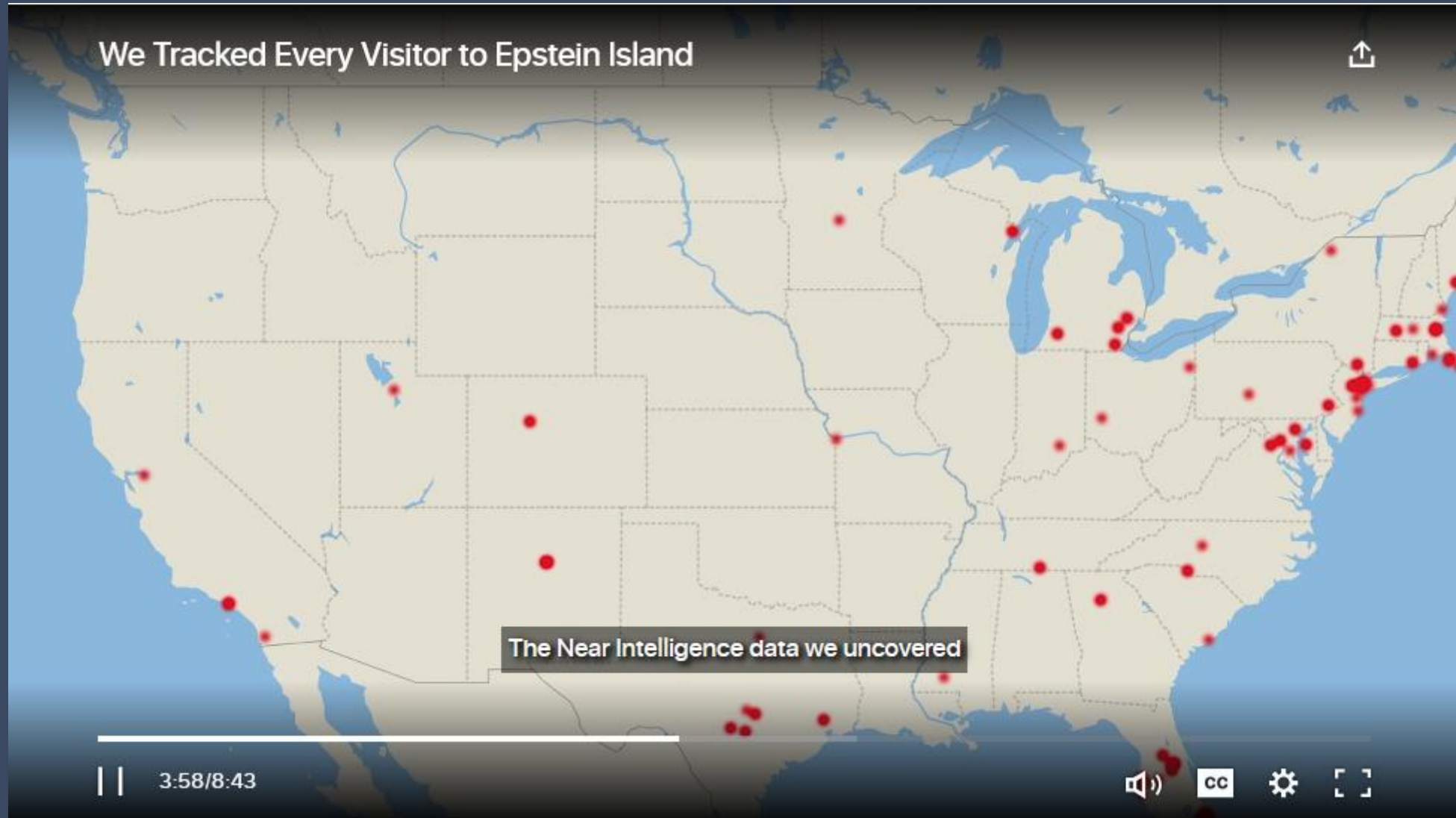
Cell Phone Location Tracking

GPS-enabled smartphones are typically accurate to within a 4.9-meter (16-foot) radius under open sky.

Apple's iPhone 15 Pro Max with GPS, GLONASS, Galileo, QZSS, and BeiDou is accurate to within 2 meters under open sky.

Source: *GPS Accuracy*, https://www.gps.gov/systems/gps/performance/accuracy/, last updated February 2025.

Source: *Best Gps Cell Phones for Accurate Navigation,* Ramsey Cole, Tools and Ideas, https://toolsandideas.com/best-gps-cell-phones/, June 11, 2025.

Source: *We Tracked Every Visitor to Epstein Island*, Dhruv Mehrotra, https://www.wired.com/video/watch/we-tracked-every-visitor-to-epstein-island, (Wired, 11/2/2024)

Cell Phone Location Tracking

The Pentagon used targeted ads to find Vladimir Putin (and other targets) – down to the foot

Putin did not have a cell phone. His aides and support staff did.

If anyone does not have a cell phone – or is using an RFID sleeve to block cell phone transmissions – but is traveling with someone who does, they can be tracked.

Source: *How the Pentagon Learned to Use Targeted Ads to Find Its Targets – and Vladimir Putin*, Byron Tau, https://www.wired.com/story/how-pentagon-learned-targeted-ads-to-find-targets-and-vladimir-putin, (Wired, Feb 27, 2024)

You can control access to location services on your phone. Here are possible choices:

- Do not allow any app access.
- Allow an app access while the app is being used.
- Allow an app access at all times.
- Allow all apps access at all times.

RFID Bag/Sleeve

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

They make

bags	clutch purses
phone sleeves	wallets
credit card wallets	passport wallets
jackets and pants	

Source: https://slnt.com

Summary

You can reduce giving away personal information by
reading privacy policies,
reviewing privacy reviews,
choosing the apps you will use,
limiting the personal information you provide, and
controlling location services.

In our upcoming
Project Upskill II
presentations…

Scammers are stepping up their attacks

Windows Defender and Malwarebytes are more effective

Using longer passwords is more effective

The attacks continue to focus on phishing emails

The attacks now focus on getting users to install malicious browser extensions, enable scripts in their browsers, or click on malicious links. This malicious software is called InfoStealers.

Extensions, Scripts, and Links Source: *What is a Drive-By Compromise Attack?*, Packetlabs, https://www.packetlabs.net/posts/heres-how-you-can-defend-against-drive-by-compromise-attacks, June 2, 2023

Threat Actors are Manipulating Network Traffic

China has ordered its network equipment manufacturers to report all vulnerabilities in their equipment to the government but not to anyone else.

Chinese threat actors are using home routers, network-attached storage (NAS), and devices such webcams and DVRs to create botnets and attack critical infrastructure

The threats are real and constantly changing

We're going to give you choices of solutions to handle privacy threats so you can pick the ones that best protect you based on your assessment of the risks

We're going to address physical, cybersecurity, and additional consent threats

We need several sessions to cover everything because there are so many different kinds of threats and ways to deal with them.

The classes are based on the CISA's Project Upskill training modules.

Why Does Project Upskill Exist

CISA, through the Joint Cyber Defense Collaborative (JCDC), created Project Upskill to provide high-risk communities with simple steps to improve their cybersecurity.

Project Upskill's series of lessons will break down threat actors' varied avenues of attack to help users understand the steps they can take to mitigate risk. After completing Project Upskill, users should feel more confident that they can implement basic cybersecurity protections.

Who Can Benefit From Project Upskill?

"While Project Upskill was developed as part of the JCDC High-Risk Communities Protection planning effort, **this guidance will benefit *any* individual seeking to improve their personal cybersecurity posture**. If you are someone without a technical background looking for straightforward ways to protect your privacy and security, Project Upskill is for you."

Seniors are being targeted. Therefore, we recommend that you implement the Project Upskill II guidance.

Improved Posture Source: https://www.cisa.gov/audiences/high-risk-communities/projectupskill Retrieved 8/7/2024

Our Application of Project Upskill

CISA's Project Upskill does not recommend or suggest hardware or software products, but the Willow Valley Computer Club's version, Project Upskill II, does.

Other threat categories beyond high-risk

Highly targeted individuals

Senior Government Leaders, Senior Political Leaders, CEOs, Celebrities

Extreme privacy

Those who fear for their life or just want maximum privacy

Highly Targeted Individuals Source: *https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf*, Retrieved January 14, 2025

Extreme Privacy Source: *Extreme Privacy: What It Takes to Disappear, 5th Edition*, Michael Bazzell, Self Published, 2024

Updated Project Upskill II Classes

- Unpacking Privacy Policies
- Basic Cybersecurity for Personal Computers and Mobile Devices
- Protecting Your Accounts from Compromise
- Protecting Data Stored on Your Devices
- Protecting Data in Transit
- Securing Your Home Router
- Unseen Access: Dealing with Intruders
- Virtual Private Networks

Carpenter v. United States, the Stored Communications Act, & the Third Party Doctrine in the Digital Age
Beatrice Neilson
The Princeton Legal Journal

Articles

For the latest cybersecurity information, these are accurate and reliable sources:

Ars Technica   arstechnica.com
Bleeping Computer   bleepingcomputer.com
CISA   cisa.gov
Forbes   forbes.com
Proton Blog   proton.me/blog
Proton VPN Blog   protonvpn.com/blog

Books

Beginner's Introduction to Privacy, Naomi Brockwell, (Independently Published, 2023)

Means of Control: How the Hidden Alliance of Tech and Government is Creating a New American Surveillance State, Bryon Tau, (Crown, 2024)

Your Face Belongs to Us: A Tale of AI, A Secretive Startup, and the End of Privacy, Kashmir Hill, (Crown, 2024)

Extreme Privacy: What It Takes To Disappear, 5th Edition, Michael Bazzell, (Independently Published, 2024)

Firewalls Don't Stop Dragons, 5th Edition, Carey Parker, (Apress, 2024)

YouTube Channels

David Bombal, [Cybersecurity, Privacy, IT] https://www.youtube.com/@davidbombal

Naomi Brockwell TV, [Privacy]
https://www.youtube.com/channel/UCSuHzQ3GrHSzoBbwrIq3LLA

PC Security Channel, [Cybersecurity, Malware]
https://www.youtube.com/channel/UCKGe7fZ_S788Jaspxg-_5Sg

Questions?