

ECE458/ECE750T27: Computer Security Privacy

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca



UNIVERSITY OF
WATERLOO

FACULTY OF
ENGINEERING



First, the news...

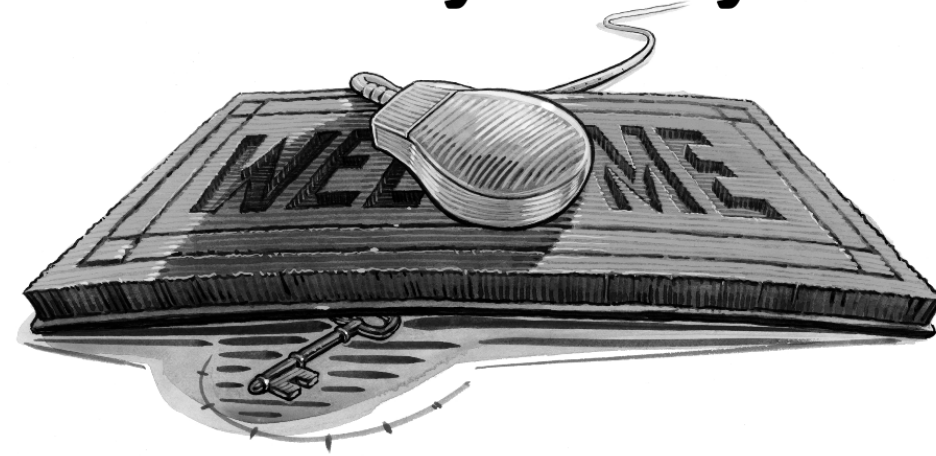
- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
 1. Some students show up late for various good reasons
 2. Reward students who show up on time
 3. Important to see real world examples

TRUST AND E-COMMERCE

Roll back time to the early 2000's

“In the rush to build Internet businesses, many executives concentrate all their attention on attracting customers rather than retaining them. That was a mistake. The unique economics of e-business make customer loyalty more important than ever.”

E-Loyalty



Your Secret Weapon on the Web

In the rush to build Internet businesses, many executives concentrate all their attention on attracting customers rather than retaining them. That's a mistake. The unique economics of e-business make customer loyalty more important than ever.

by Frederick F. Reichheld and Phil Schefter

LOYALTY MAY NOT BE THE FIRST idea that pops into your head when you think about electronic commerce. After all, what relevance could such a quaint, old-fashioned notion hold for a world in which customers defect at the click of a mouse and impersonal shopping bots scour databases for ever better deals? What good is a small-town virtue amid the faceless anonymity of the Internet's

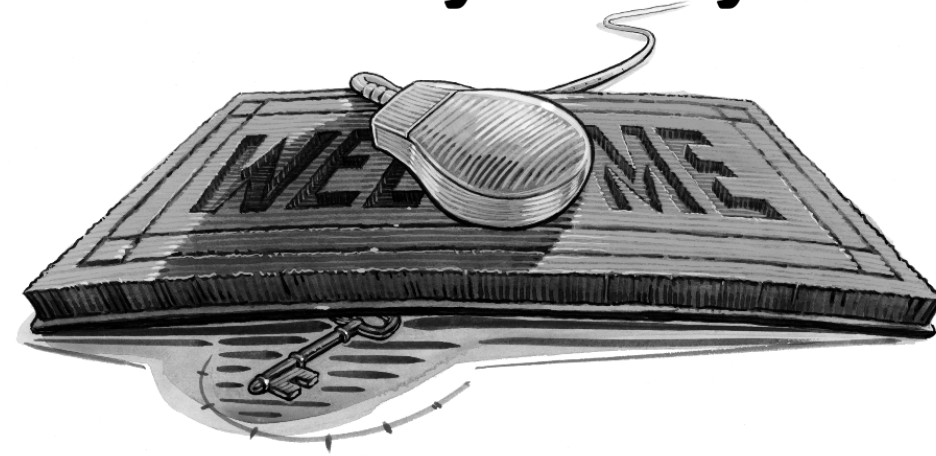
global marketplace? Loyalty must be on a fast track toward extinction, right?

Not at all. Chief executives at the cutting edge of e-commerce—from Dell Computer's Michael Dell to eBay's Meg Whitman, from Vanguard's Jack Brennan to Grainger's Richard Keyser—care deeply about customer retention and consider it vital to the success of their on-line operations. They know that loyalty

ILLUSTRATION BY DOUGLAS JONES

“On the Web ... business is conducted at a distance and risks and uncertainties are magnified... Customers can't look a salesclerk in the eye, can't size up the physical space of a store or office, and can't see and touch products. They have to rely on images and promises, and if they don't trust the company presenting those images and promises, they'll shop elsewhere.”

E-Loyalty



Your Secret Weapon on the Web

In the rush to build Internet businesses, many executives concentrate all their attention on attracting customers rather than retaining them. That's a mistake. The unique economics of e-business make customer loyalty more important than ever.

by Frederick F. Reichheld and Phil Schefter

LOYALTY MAY NOT BE THE FIRST idea that pops into your head when you think about electronic commerce. After all, what relevance could such a quaint, old-fashioned notion hold for a world in which customers defect at the click of a mouse and impersonal shopping bots scour databases for ever better deals? What good is a small-town virtue amid the faceless anonymity of the Internet's

global marketplace? Loyalty must be on a fast track toward extinction, right?

Not at all. Chief executives at the cutting edge of e-commerce—from Dell Computer's Michael Dell to eBay's Meg Whitman, from Vanguard's Jack Brennan to Grainger's Richard Keyser—care deeply about customer retention and consider it vital to the success of their on-line operations. They know that loyalty

ILLUSTRATION BY DOUGLAS JONES

Problem: How can we make people feel safe spending money online?

Trust transfer

- Inexperienced shoppers tend to transfer trust. One thing worked, so they look for something else that looks similarly trustworthy.
- Collective approaches
 - TRUSTe seal
 - Being part of a more trusted retail group
 - “well they would say that, wouldn’t they”...
- Individual site approaches
 - Hard to build trust on just one site.
 - Things like customer testimonials first require trust in the company that they are true



Problem: We need a trusted cross-site signal that users can trust.

Answer: Privacy policies

Federal Trade Commission Act of 1914 (USA)

The FTC is empowered, among other things, to:

- prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce;
- seek monetary redress and other relief for conduct injurious to consumers;
- prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices;
- conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce

Federal Trade Commission Act of 1914 (USA)

The FTC is empowered, among other things, to:

- **prevent** unfair methods of competition, **and unfair or deceptive acts or practices** in or affecting commerce;
- seek monetary redress and other relief for conduct injurious to consumers;
- prescribe **trade regulation rules defining** with specificity **acts or practices that are unfair or deceptive**, and establishing requirements designed to prevent such acts or practices;
- conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce

Federal Trade Commission (FTC)

- Unfair practices
 - Injure consumer
 - Violate established policy
 - Unethical
- Deceptive practices
 - Mislead consumer
 - Differ from reasonable consumer expectations

Roughly: The FTC declared that if an organization said it did X in its privacy policy, but then was shown to not be doing X, then the FTC could levy a large fine.

Also if it had no privacy policy, that was unfair, and the organization could be fined.

Morning Lecture Stopped Here

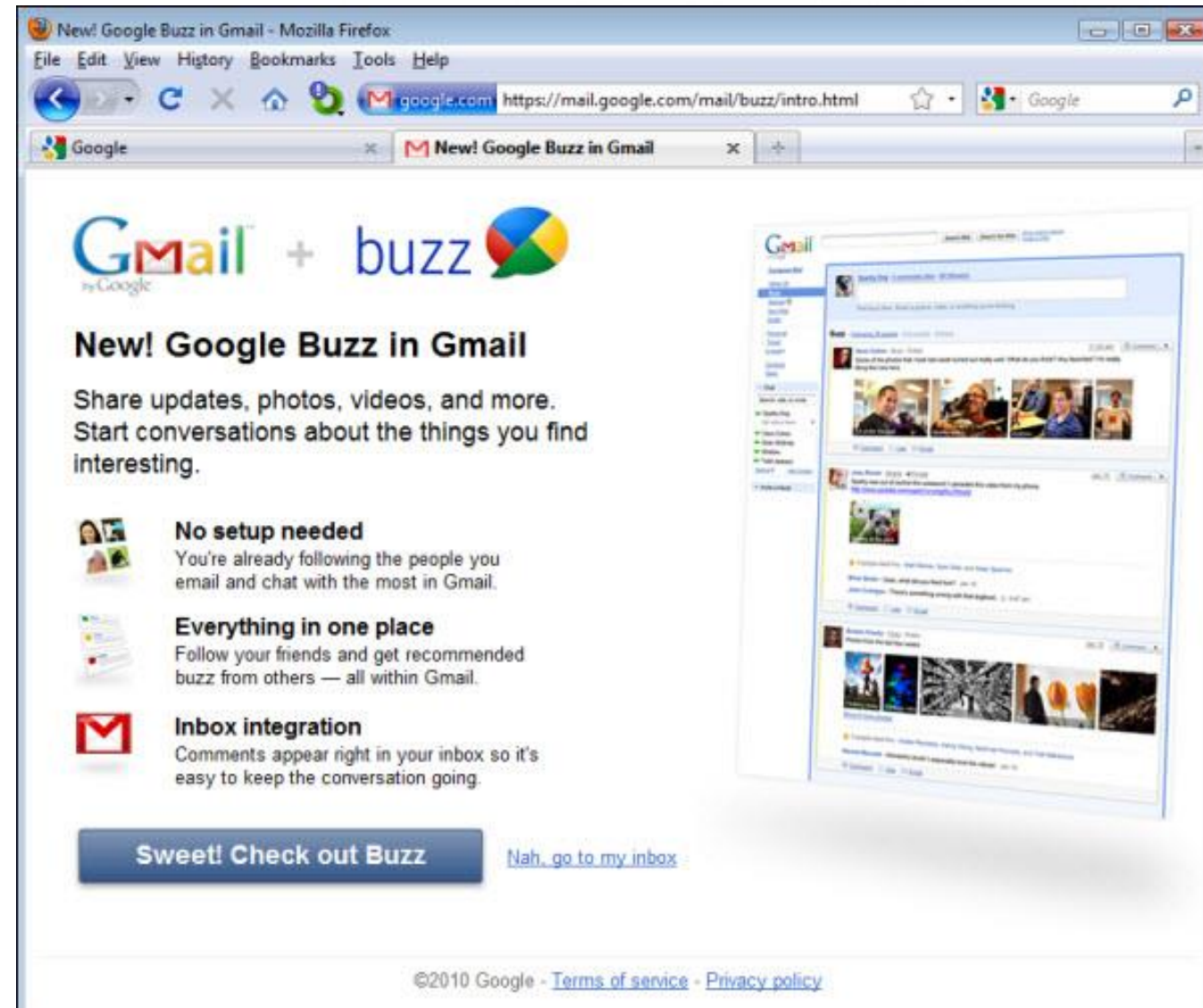
FTC vs Google Buzz

- When Google launched Buzz it wanted to use the network it already had in Gmail
- Gmail privacy policy (2004-2010):
 - “Gmail stores, processes and maintains your messages, contact lists and other data related to your account in order to provide the service to you”
- Google privacy policy (2005-2010)
 - “When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.”



FTC vs Google Buzz

- User first given options
- If they selected “Nah, go to my inbox”
 - They could still be followed on Buzz
 - Their Google profile listed them as a Buzz user
 - A link appeared on their UI and if they clicked it they were auto enrolled and data was copied over
- Contacts that users interacted with the most were listed on their profile



Office of the Privacy Commissioner of Canada

- Oversees compliance with:
 - Privacy Act - how federal government handles personal data
 - Personal Information Protection and Electronic Documents Act (PIPEDA) - private sector privacy law
- Activities like:
 - Investigation of complaints
 - Auditing
 - Public awareness
 - Advise parliament



The screenshot shows the official website of the Office of the Privacy Commissioner of Canada. At the top, there is a header with the Canadian coat of arms, the office's name in English ("Office of the Privacy Commissioner of Canada") and French ("Commissariat à la protection de la vie privée du Canada"), and a navigation bar with links for "For individuals", "For businesses", "For federal institutions", and "Report a concern". Below the header, the main heading "Office of the Privacy Commissioner of Canada" is displayed in a large, bold, purple font. Underneath, the sub-heading "Protecting and promoting privacy rights" is shown in a smaller purple font. The main text block explains the office's role: "The Office of the Privacy Commissioner of Canada provides advice and [information for individuals](#) about protecting personal information. We also enforce two [federal privacy laws](#) that set out the rules for how [federal government institutions](#) and certain [businesses](#) must handle personal information." It also includes a link to "Learn more about [our Office](#)." Below the text is a large image featuring a young girl looking at a smartphone, overlaid with three orange speech bubbles containing a white exclamation mark, a white checkmark, and a white question mark. At the bottom of the page, there is a purple footer with the text "Call for comments" and "Privacy and age assurance - Exploratory consultation".

Office of the Privacy Commissioner of Canada

Protecting and promoting privacy rights

The Office of the Privacy Commissioner of Canada provides advice and [information for individuals](#) about protecting personal information. We also enforce two [federal privacy laws](#) that set out the rules for how [federal government institutions](#) and certain [businesses](#) must handle personal information.

Learn more about [our Office](#).

Call for comments
Privacy and age assurance - Exploratory consultation

Office of the Privacy Commissioner of Canada: Home Depot Case

- Home Depot was using Facebook's "Offline Conversions" feature which measures effectiveness of Facebook ads.
- "Home Depot forwards the customer's hashed email address and off-line purchase details to Meta when the customer provides their email address to Home Depot, at check-out, to obtain an e-receipt"
- Facebook then provides statistics on how ads are impacting purchases
- Meta could use information for its own purposes

Investigation into Home Depot of Canada Inc.'s compliance with PIPEDA

PIPEDA Findings # 2023-001

January 26, 2023

Overview

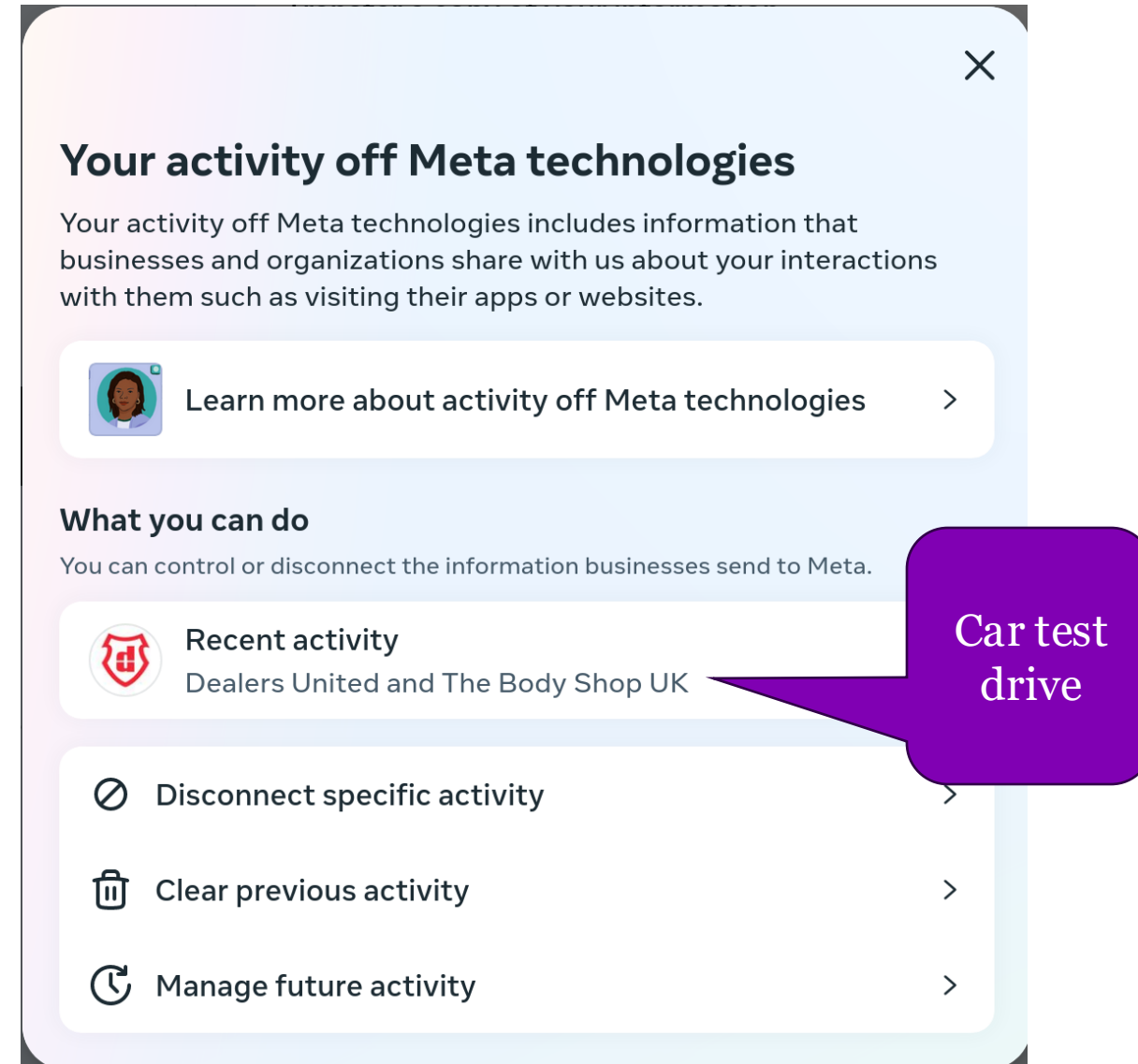
The Complainant alleged that Home Depot of Canada Inc. ("Home Depot") disclosed his personal information to Facebook (now Meta Platforms, Inc., "Meta") without his knowledge and consent. Specifically, the complainant claimed that while he was deleting his Facebook account, he learned that Meta had a record of most of his in-store purchases made at Home Depot.

Home Depot confirmed to our Office that it was in fact sending in-store customers' data to Meta through a business tool known as "Offline Conversions", which allows businesses to measure the effectiveness of Meta ads. Specifically, Home Depot forwards the customer's hashed ¹ email address and off-line purchase details to Meta when the customer provides their email address to Home Depot, at check-out, to obtain an e-receipt. Meta then matches the email to the customer's Facebook account. If the customer has a Facebook account, Meta compares offline purchase information to ads delivered to the customer on Facebook, to measure effectiveness of those ads, and provides results of that analysis back to Home Depot in the form of an aggregated report. Meta can also use the customer's information for its own business purposes, including targeted advertising, unrelated to Home Depot.

Contrary to Home Depot's assertion, neither its Privacy Statement nor that of Meta were sufficient to obtain implied consent for its disclosure to Meta of the personal information of in-store customers requesting an e-receipt. The Home Depot privacy statement would not have been readily available to customers at the time of purchase, and in any event did not provide a clear explanation of the practice in question. Furthermore, customers would have no reason to check Meta's privacy statement in the context

How did the Home Depot complaint come about?

- A user was deleting his Facebook profile and noticed Home Depot under "activity off Meta"
- They complained to OPC
- Investigation happened




I tried to disconnect "Dealers United"


- Out of curiosity I tried disconnecting "Dealers United" and got the dialog to the right
- In short, I can disconnect and face bad usability. But they will still keep collecting and using my data?





×


What you should know


 When you disconnect your future activity that businesses send us, your choices will be applied to all of your accounts you've linked in Accounts Center. [Learn more](#)


 You are disconnecting future activity from Dealers United.


 When you disconnect future activity that businesses send us, your choices will be applied to all of your accounts you've linked in Accounts Center.

 This will disconnect your future activity from the selected apps and websites. It may take 48 hours until it's fully disconnected from your account.

 If you're logged into any apps and websites with Facebook, disconnecting future activity may log you out. It will also prevent you from logging in with Facebook in the future.

 If you've connected your Instagram account to other apps and websites, disconnecting your future activity may stop your Instagram account from being connected to those businesses. It will also prevent you from connecting your Instagram account to those businesses in the future.

 We'll still receive activity from Dealers United. It may be used for measurement purposes and to make improvements to our ads systems, but it will be disconnected from your account.

 You may still see ads from Dealers United. Your ad preferences and actions you take on Facebook or Instagram will be used to show you relevant ads.

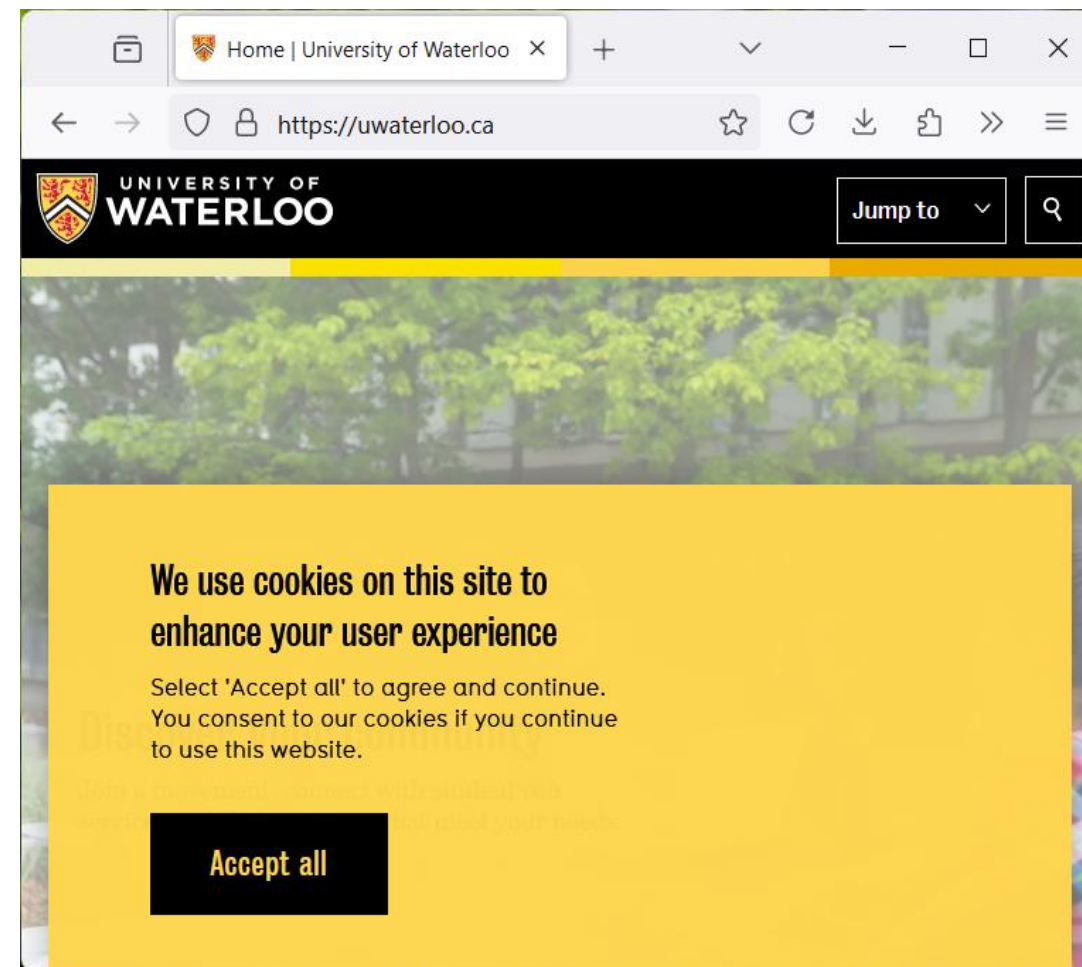
CancelConfirm

NOTICE AND CHOICE

Basis for USA privacy

Notice and Choice: The idea

- Users have the right to know how their data will be used, so that information should be available
- Once users are aware, they can make good choices
- Interacting with a site or service is a choice
- Market pressures will force companies to provide good choices that customers demand



Notice is provided via privacy policies

- FTC, OPC and similar regulatory bodies enforce privacy policy accuracy so consumers can trust organizations
- Organizations make such policies readily available to consumers

Betterment | Joint Checking signup

Agree to Checking terms and conditions

The terms and conditions below are specific to your new Checking account.

By clicking "Accept and continue," you acknowledge that you have read and agreed to the following documents:

- [Cardholder Agreement](#)
- [E-sign Disclosure](#)
- [nbkc bank Consumer Deposit Account Agreement](#)
- [nbkc bank Privacy Policy](#)
- [Betterment Financial Terms & Conditions](#)
- [Betterment Form CRS Relationship Summary](#)
- [Cash Back Rewards Powered by Dosh Terms of Service](#)
- [MX Technologies User Agreement](#)

[Accept and continue](#)

Privacy Information

Online Privacy Notice

Effective Date: 12/01/2023

nbkc bank is committed to safeguarding the privacy and security of your information. This Online Privacy Notice describes how we may collect, use, transfer, and disclose information about you when you use our products, services, mobile application, or visit our website. By using our products, services, mobile application, or visit our website, you agree to be bound by the terms and conditions of this Online Privacy Notice. Please note that this Online Privacy Notice does not apply to websites owned and operated by third parties regardless of whether we provide a hyperlink to them through our websites. Websites not owned or operated by us will be subject to their own privacy policies. We have no control over third-party websites or their privacy policies.

Types of Information We Collect

We may collect the following types of information when you use our products, services, or mobile application, or visit our website:

- "Personal Information" is information that we may collect that identifies you as an individual, customer, or consumer. Examples of Personal Information include your name, date of birth, social security number or tax identification number, driver's license number, mailing address, email address, government-issued photo identification, personal photograph of yourself, telephone number(s), telephone number data, and your account number(s).
- "Non-Personal Information" is information that we may collect that does not identify you as an individual, customer, or consumer. Examples of non-personal information are the version of your Internet browser, your computer or mobile device's operating system, information from tracking technologies, websites you visit, your computer's IP address, and location information or other data.

How We Collect Your Information

We collect Personal Information about you when you request information about, or apply for, our products or services, register for online or mobile account access, contact us for customer service, communicate with us through social media, or otherwise interact with us. We may also collect Personal Information about you from other sources, such as public databases, credit reporting agencies, social media platforms, affiliated companies, and other third parties.

We also collect Non-Personal Information about your online and mobile activity automatically using the following tracking technologies:

1. HTTP cookies ("Cookies") are pieces of information that are stored directly on the device you are using. Cookies provide us with anonymous online and mobile activity information such as the time of your site visits and the pages you viewed. Cookies are commonly used with internet browsers, and do not harm your computer or device.
2. Mobile advertising ID's (MAIDs) are similar to Cookies but are used in connection with a mobile device. MAIDs are user specific, resettable identifiers provided by your mobile device's operating system. When we use MAIDs, you remain anonymous. You can reset your MAIDs by following these steps: (a) for Google Android, open Google Settings on your Android device, tap the Ads Menu under Services, tap "reset advertising ID", and confirm the reset when the confirmation prompt is displayed; for Apple devices, open the Settings app, tap Privacy, scroll down to the bottom of the page and tap Advertising, tap "reset Advertising Identifier", confirm this choice by tapping "reset Advertising Identifier" again.
3. Web beacons and pixel tags ("Beacons and Tags") are technologies that allow tracking of your online activity and websites you visited. Beacons and Tags may gather anonymous information such as your computer's operating system, your computer's IP address, and time and duration of your website visits.

You may disable these tracking technologies or opt-out of targeted advertising generally in the settings menu of your Internet browser or mobile device. For Apple devices, open the Settings app, tap Privacy, scroll down to the bottom of the page and tap Advertising, then turn the Limit Ad Tracking button to "ON". For Android devices, tap Menu, tap Google Settings, tap Ads, and then check the box identified as "Opt-out of interest-based ads."

How We Use Collected Information

We use information we collect about you to:

- process your requests for our products or services and provide those products or services to you;
- provide relevant information to you about our products and services, including, but not limited to, important changes to our policies and terms and conditions;
- make improvements to and personalize our products and services;
- communicate with you about your account(s) and transactions, including inviting you to participate in surveys, contests, and other promotions;
- track the effectiveness of our advertisements;
- detect, respond to, and protect against illegal activity, activity which may violate our business policies, or activity which may compromise our business operations or security;
- maintain and service your account; respond to your requests;
- detect, respond to, and protect against fraud, security breaches, identity theft, and other risks of harm;
- comply with applicable legal and regulatory obligations;
- honor your personal settings (e.g., font size, location), enhance your online and mobile experience;
- improve our products and services; and provide targeted marketing to you.

Sharing Your Information

If you are our customer or former customer, we will share your information as disclosed in our Privacy Notice. This Privacy Notice explains how we collect, use, and share information about you with third parties and, if applicable, your right to limit that sharing. Our Privacy Notice may be accessed at www.nbkc.com/security/privacy.

If you are not our customer, you are our consumer, and we will not share your information unless required to do so by law, such as to comply with federal, state, or local laws or to comply with a properly issued subpoena or summons by Federal, state, or local authorities.

We will not sell or lease the information we collect about you to third parties for any purpose, including for those third parties to engage in the direct marketing of their own products or services to you.

Keeping Your Information Secure

We are committed to keeping your information secure. To protect your information from unauthorized access and use, we use security measures designed to comply with federal and state law and meet recognized industry standards. This includes the use of encryption technology, contractual limitations on the use of your information with our service providers and subcontractors, and identity verification procedures.

Children's Online Privacy

Our products and services are not directed to children. We do not knowingly solicit or collect Personal Information from children under the age 13, without parental consent. If you are a parent or guardian of a child under the age of 13 and become aware that he or she disclosed Personal Information to us, please contact us at the address below. For more information about the Children's Online Privacy Protection Act, visit the Federal Trade Commission's website at <https://www.ftc.gov/>.

Mobile App Privacy

Our Mobile Banking Application may request access to information stored on your device such as location, contact lists, external storage, camera/photo information, contacts, or other features you are enrolled in to simplify your user experience, improve our services, and provide additional security to protect your account. The mobile application may also access other information as outlined in this policy.

It is important to understand that:

- Before granting access to this information, you will be prompted to give the application that permission.
- If you do not wish to grant that permission, you may decline.
- If you later change your mind, you may update those permissions in your device settings.

IMPORTANT PRIVACY INFORMATION FOR CALIFORNIA RESIDENTS

California's "Shine the Light" Law, California Civil Code Section 1798.83, permits you to request and obtain from us once a year, free of charge, a list of all third parties to which we have disclosed personally identifiable information as defined under California law for such third parties' direct marketing purposes in the preceding calendar year. If you are a California resident and would like to make such a request, see the Contact Information section below.

The California Online Privacy Protection Act requires nbkc bank to disclose how it responds to Do Not Track signals set in your browser. We do not support Do Not Track browser settings. If you enable Do Not Track settings in the browser you are using, we will not respond to them. We await the result of the privacy industry and legal community to determine when a response is appropriate and what form such a response should take. The California Consumer Privacy Act ("CCPA") grants you specific rights in regard to Personal Information we have collected about you. Under the CCPA, you have the right to request from us up to two times every 12 months, free of charge, a list of all the categories and/or specific pieces of Personal Information we have collected about you and that we delete such Personal Information. In the 12 months prior to the Effective Date of this Online Privacy Notice, we have collected the following categories of Personal Information about our customers:

Category	Examples	Collected
Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(a)).	A 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. Some personal information included in this category may overlap with other categories.	YES
Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	YES
Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystrokes, gait, or other physical patterns, and sleep, health, or exercise data.	NO
Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	NO
Geolocation data.	Physical location or movements.	NO
Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO
Professional or employment-related information.	Current or past job history or performance evaluations.	YES
Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. section 1222g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO
Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

Right to Request

The CCPA also grants you the right to request that your Personal Information not be sold to third-parties. nbkc bank does not sell Personal Information about our customers to third parties and has not sold any Personal Information about our customers in the 12 months prior to the Effective Date of this Online Privacy Notice.

To exercise your rights under the CCPA, please contact us at using the information listed in the Contact Information section below. If you choose to exercise these rights, we will not deny you goods or services, charge you different prices, impose different interest rates or fees, or provide you with a different level of quality of goods or services.

Record Deletion

Subject to certain exceptions, you have the option to delete Personal Information about you that we have collected from you.

Data Portability

You have the right to receive the personal information you have previously provided to us and that we have collected.

Changes to this Online Privacy Notice

We may make changes to this Online Privacy Notice at any time and without notice. Any changes to this notice will become effective when posted unless indicated otherwise. Please revisit this notice to ensure you understand how we collect and use your information.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. If you choose to exercise your rights under the CCPA, we will not deny you goods or services, charge you different prices, impose different interest rates or fees, or provide you with a different level of quality of goods or services.

Contact Information

If you have any questions or comments about this notice, the ways in which we collect and use your personal information, your choices and rights regarding our use of personal information, or wish to exercise your rights under the CCPA, please contact us at:

Phone: (888) 905-2165
Website: nbkc.com
Email: Compliance.CCPA@nbkc.com
Address: nbkc bank
Attn: Privacy and CCPA Compliance
8320 Ward Parkway
Kansas City, MO 64114

[Click Here](#) for a printer-friendly version of this Online Privacy Notice.

How We Protect Your Privacy

Protecting your personal information is important. To understand what information nbkc bank collects and how your information is used, please visit our [Consumer Privacy Policy](#). To opt out of personal information sharing for the following: joint marketing with other financial companies, affiliates' everyday business purposes, and non-affiliates' marketing, please [Click Here](#).

Resident of California

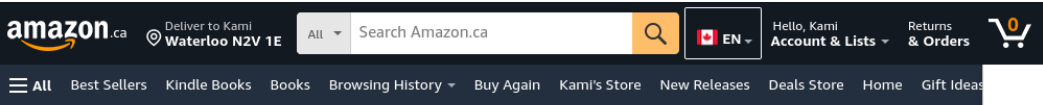
The California Consumer Privacy Act includes certain rights for California residents. [Click Here](#) to view our California Privacy Notice. To exercise your rights for the California Consumer Privacy Act (CCPA), please call (888) 905-2165 or fill out this [form](#). All requests should specify CCPA § include your full name, email address, and phone number used when submitting personal information to nbkc bank.

Betterment's privacy policy



Amazon Privacy Policy

- 3478 words long
- College education required to read
- Estimated reading time of 15-20 minutes



Help and customer service

[All help topics](#)

Legal Policies

- Amazon.ca Conditions of Use
- Amazon.ca Privacy Notice
- Changes to Amazon.ca Privacy Notice
- Content Usage Terms
- Non-Exhaustive List of Applicable Amazon/Affiliate Patents and Applicable Licensed Patents
- Non-Exhaustive List of Amazon Trademarks
- Amazon.ca Gift Card and Electronic Message
- Customization Service Terms
- Communications with Amazon Employees

Quick solutions

- Your orders
Track or cancel orders
- Returns & Refunds
Exchange or return items

Find more solutions

[Security and Privacy](#) › [Legal Policies](#) ›

Amazon.ca Privacy Notice

Last Updated: January 1, 2024 - [Click here](#) to see prior version.

We know that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This Privacy Notice describes how Amazon.com.ca ULC and its affiliates (collectively "Amazon") collect and process your personal information through Amazon websites, devices, products, services, online and physical stores, and applications that reference this Privacy Notice (together "Amazon Services"). By using Amazon Services you are consenting to the practices described in this Privacy Notice.

- What Personal Information About Customers Does Amazon Collect?
- For What Purposes Does Amazon Process Your Personal Information?
- What About Cookies and Other Identifiers?
- Does Amazon Share Your Personal Information?
- How Secure Is Information About Me?
- What About Advertising?
- What Information Can I Access?
- What Choices Do I Have?
- Are Children Allowed to Use Amazon Services?
- Conditions of Use, Notices, and Revisions
- Related Practices and Information
- Examples of Information Collected

What Personal Information About Customers Does Amazon Collect?

We collect your personal information in order to provide and continually improve our products and services.

Here are the types of personal information we collect:

- **Information You Give Us.** We receive and store any information you provide in relation to Amazon Services. [Click here](#) to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our Amazon Services.
- **Automatic Information.** We automatically collect and store certain types of information about your use of Amazon Services, including information about your interaction with content and services available through Amazon Services. Like many websites, we use "cookies" and other unique identifiers, and we obtain certain types of information when you web browser or device access Amazon Services and other Amazon services or on behalf of Amazon on other websites. [Click here](#) to see examples of what we collect.
- **Information From Other Sources.** We might receive information about you from other sources, such as updated delivery and address information from our carriers, which we use to correct our records and deliver your next purchase more easily. [Click here](#) to see additional examples of the information we receive.

For What Purposes Does Amazon Process Your Personal Information?

We use your personal information to operate, provide, develop, and improve the products and services that we offer our customers. These purposes include:

- **Purchase and delivery of products and services.** We use your personal information to take and handle orders, deliver products and services, process payments, and communicate with you about orders, products and services, and promotional offers.
- **Provide, troubleshoot, and improve Amazon Services.** We use your personal information to provide functionality, analyze performance, fix errors, and improve the usability and effectiveness of the Amazon Services.
- **Recommendations and personalization.** We use your personal information to recommend features, products, and services that might be of interest to you, identify your preferences, and personalize your experience with Amazon Services.
- **Provide voice, image and camera services.** When you use our voice, image and camera services, we can use your voice input, images, videos, and other personal information to respond to your requests, provide the requested service to you, and improve our services.
- **Comply with legal obligations.** In certain cases, we collect and use your personal information to comply with laws. For instance, we collect from sellers information regarding place of establishment and bank account information for identity verification and other purposes.
- **Communicate with you.** We use your personal information to communicate with you in relation to Amazon Services via different channels (e.g., by phone, email, chat).
- **Advertising.** We use your personal information to display interest-based ads for features, products, and services that might be of interest to you. We do not use information that personally identifies you to display interest-based ads. To learn more, please read our [Interest-Based Ads policy](#).
- **Fraud Prevention and Credit Risks.** We use personal information to prevent and detect fraud and abuse in order to protect the data security of our customers, Amazon, and others. We may also use scoring methods to assess and manage credit risks.
- **Purposes for which we seek your consent.** We may also ask for your consent to process your personal information for a specific purpose that we communicate to you.

What About Cookies and Other Identifiers?

To enable our systems to recognize your browser or device and to provide and improve Amazon Services, we use cookies and other identifiers. For more information about cookies and how we use them, please read our [Cookies Notice](#).

Does Amazon Share Your Personal Information?

Information about our customers is an important part of our business, and we are not in the business of selling our customers' personal information to others. We share customer personal information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

- **Transactions Involving Third Parties.** We make available to you services, products, applications, or skills provided by third parties for use on or through Amazon Services. For example, you can order products from third parties through our stores, download applications from third-party application providers from our App Store, and enable third-party skills through our Amazon services. We also offer services or sell product lines jointly with third-party businesses, such as co-branded credit cards. You can tell when a third party is involved in your transactions, and we share customer personal information related to those transactions with that third party.
- **Third-Party Service Providers.** We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders for products or services, delivering packages, sending postal mail and email, removing negative information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing payments, transmitting content, scoring, assessing and managing credit risk, and providing customer service. These third-party service providers have access to personal information needed to perform their functions, but may not use it for other purposes.
- **Business Transfers.** As we continue to develop our business, we might sell or buy other businesses or services. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com.ca LLC or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.
- **Protection of Amazon and Others.** We disclose account and other personal information when we believe disclosing is appropriate to comply with the law, enforce or apply our Conditions of Use and other agreements, or protect the rights, property, or safety of Amazon, our users, or others. This includes exchanging information with other companies and organizations for fraud prevention and credit risk reduction.

Other than as set out above, you will receive notice when your personal information about you might be shared with third parties, and you will have an opportunity to choose not to share the information.

Cross-Border Transfers. Whenever we transfer personal information outside of your province or territory, or outside of Canada, we ensure that the information is transferred in accordance with this Privacy Notice and as permitted by applicable laws on data protection.

How Secure Is Information About Me?

We design our systems with your security and privacy in mind.

- We work to protect the security of your personal information during transmission by using encryption protocols and software.
- We follow the Payment Card Industry Data Security Standard (PCI DSS) when handling credit card data.
- We maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of personal customer information. Our security procedures mean that we may occasionally request proof of identity before we disclose personal information to you.
- Our devices offer security features to protect them against unauthorized access and loss of data. You can control these features and configure them based on your needs. [Click here](#) for more information on how to manage the security settings of your device.
- We encourage you to protect against unauthorized access to your personal information by using secure logins, devices, and applications. We recommend using a unique password for your Amazon account that is not used for other online accounts, be sure to sign off when finished using a shared computer. [Click here](#) for more information on how to sign off.

What About Advertising?

- **Third-Party Advertisers and Links to Other Websites.** Amazon Services may include third-party advertising and links to other websites and apps. Third-party advertising partners may collect information about you when you interact with their content, advertising, and services. For more information about third-party advertising at Amazon, including interest-based ads, please read our [Interest-Based Ads policy](#). To adjust your advertising preferences, please go to the [Advertising Preferences](#) page.
- **Use of Third-Party Advertising Services.** We provide our companies with information that allows them to serve you with more useful and relevant Amazon ads and to measure their effectiveness. We never share your name or other information that directly identifies you when we do this. Instead, we use an advertising identifier like a cookie, device identifier, or a code derived from applying irreversible cryptography to other information like an email address. For example, if you have already downloaded one of our apps, we will share your advertising identifier and data with that app so that you will not be served an ad to download the app again. Some ad companies also use this information to serve you relevant ads from other advertisers. You can learn more about how to opt-out of interest-based advertising by going to the [Advertising Preferences](#) page.

What Information Can I Access?

You can access your information, including your name, address, payment options, profile information, Prime membership, household settings, and purchase history in the Your Account section of the website. [Click here](#) for a list of examples that you can access.

What Choices Do I Have?

If you have any questions as to how we collect and use your personal information, please contact our [Customer Service](#). Many of our Amazon Services also include settings that provide you with options as to how your information is being used.

- As described above, you can choose not to provide certain information, but then you might not be able to take advantage of many of the Amazon Services available to you.
- You can add or update certain information on pages such as those referenced in [What Information Can I Access?](#) When you update information, we usually keep a copy of the prior version for our records.
- If you do not want to receive email or other communications from us, please adjust your [Customer Communication Preferences](#). If you don't want to receive in-app notifications from us, please adjust your notification settings in the app or device.
- If you do not want to see interest-based ads, please adjust your [Advertising Preferences](#).
- The help feature on most browsers and devices will tell you how to prevent your browser or device from accepting new cookies or other identifiers, how to have the browser notify you when you receive a new cookie, or how to block cookies altogether. Because cookies and identifiers allow you to take advantage of some essential features of Amazon Services, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Services that require you to Sign in. For more information about cookies and other identifiers, see our [Cookies Notice](#).
- If you want to remove our websites without linking the browsing history to your account, you may try to go to logging out of your account but blocking cookies on your browser.
- When you consent to our processing your personal information for a specified purpose, you may withdraw your consent at any time and we will stop any further processing of your data for that purpose.
- You will also be able to opt-out of certain other types of data usage by updating your settings on the applicable Amazon website (e.g., in "Manage Your Content and Device"), device, or application. For more information [click here](#). Most non-A Amazon devices also provide users with the ability to change device permissions (e.g., disable/access location services, contacts) for most devices, these controls are located in the device's settings menu. If you have questions about how to change your device permissions or device manufactured by third parties, we recommend you contact your mobile service carrier or your device manufacturer.
- If you are a seller, you can add or update certain information in [Seller Central](#), update your account information by accessing your [Seller Account](#) information, and adjust your email or other communications you receive from us by updating your [Notification Preferences](#).
- If you are an author, you can add or update the information you have provided in the [Author Portal](#) and [Author Central](#) by accessing your accounts in the [Author Portal](#) and [Author Central](#), respectively.

In addition, to the extent required by applicable law, you have the right to request access to, correct, and delete your personal data. If you wish to do any of these things, please go to [Request My Personal Information](#) or contact [Customer Service](#). Depending on your data choices and province of residence, certain services may be limited or unavailable.

Are Children Allowed to Use Amazon Services?

Amazon does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under the age of majority in your province or territory of residence, you may use Amazon Services only with the involvement of a parent or guardian.

Conditions of Use, Notices, and Revisions

If you choose to use Amazon Services, your use and any dispute over privacy is subject to this notice and our [Conditions of Use](#), including limitations on damages, resolution of disputes, and application of the law of the state of Washington.

If you have any concern about privacy at Amazon, please [Contact Us](#) with a thorough description, and we will try to resolve the issue for you. Further, the Amazon Canada Privacy Office can be contacted at canada.privacy@amazon.com or by mail at ATTN: Amazon.ca Privacy Office, 120 Bremner Blvd, Toronto, ON M5G 0A1.

Our business changes constantly, and our Privacy Notice will change also. You should check our website frequently to see recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never materially change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers.

Related Practices and Information

[Conditions of Use](#)
[Seller Program Policies](#)
[Help department](#)
[Most Recent Purchases](#)
[Your Profile and Community Guidelines](#)

Examples of Information Collected

You provide information to us when you:

- search or shop for products or services in our stores;
- add or remove an item from your wish list, or place an order through or use Amazon Services;
- download, stream, view, or use content on a device or through a service or application on a device;
- provide information in [Your Account](#) (and you might have more than one if you have used more than one email address or mobile number when shopping with us or your [Profile](#));
- talk to or otherwise interact with our Alexa Voice service;
- upload your contacts;
- configure your settings on, provide data access permissions for, or interact with an Amazon device or service;
- provide information in your [Seller Account](#), [Kindle Direct Publishing \(KDP\)](#), [Developer account](#), or any other account we make available that allows you to develop or offer software, mobile or desktop or Amazon customers.

- look to or connect with other users from your mobile device service;
- upload your contacts;
- configure your settings on, provide data access permissions for, or interact with an Amazon device or service;
- provide information in your [Seller Account](#), [Kindle Direct Publishing \(KDP\)](#), [Developer account](#), or any other account we make available that allows you to develop or offer software, mobile or desktop or Amazon customers;
- offer your products or services on or through Amazon Services;
- communicate with us by phone, email, or otherwise;
- complete a questionnaire, a support ticket, or a contact survey form;
- upload or stream images, videos or other files to Prime Photos, Amazon Drive, or other Amazon Services;
- use our services such as Prime Video;
- complete Playlists, Watchlists, Wish Lists or other gift registries;
- participate in Discussion Boards or other community features;
- provide and rate Reviews;
- specify a Special Order Availability Reminder; or
- employ Product Availability Alerts, such as Available to Order notifications.

As a result of these actions, you might supply us with such information as:

- identifying information such as your name, address, and phone number(s);
- payment information;
- your age;
- your location information;
- your IP address;
- people, addresses and phone numbers listed in your Address(es);
- email addresses of your friends and other people;
- content of reviews and emails to us;
- personal description and photograph in your [Profile](#);
- voice recordings when you speak to Alexa;
- images and videos collected or shared in connection with Amazon Services;
- information and documents regarding identity, including Social Insurance Numbers and driver's license numbers;
- corporate and financial information;
- credit history information; and
- device type and configurations, including Wi-Fi credentials, if you choose to automatically synchronize them with our other Amazon devices.

Automatic Information

Examples of the information we collect and analyze include:

- the internet protocol (IP) address used to connect your computer to the internet;
- login, email address, and password;
- the location of your device or computer;
- content viewed and information (e.g., the occurrence of technical errors, your interactions with service features and content, your settings preferences and backup information, location of your device running an application, information about uploaded images and files such as the same, date, time and location of your images);
- version and time zone settings;
- purchase and content use history, which we sometimes aggregate with similar information from other customers to create features like [Top Sellers](#);
- the full [Amazon Resource Locator \(URL\)](#) clickstream to, through, and from our websites, including date and time, products and content you viewed or searched for, page response times, download times, length of visits to certain pages, and page interaction information (such as scrolling, clicks, and mouse moves);
- phone numbers you use to call our customer service number;
- images or videos when you shop in our stores, or stores using Amazon Services.

We may also use device identifiers, cookies, or other technologies on devices, applications, and our web pages to collect browsing, usage, or other behavioral information.

Information From Other Sources

Examples of information we receive from other sources include:

- updated delivery and address information from our carriers or other third parties, which we use to correct our records and deliver your next purchase or communication more easily;
- account information, purchase or redemption information, and page-view information from some merchants with which we operate co-branded businesses or for which we provide technical, fulfillment, advertising, or other services;
- information about your interactions with products and services offered by our subsidiaries;
- search results and links, including paid listings (such as Sponsored Links);
- information about internet-connected devices and services linked with Alexa; and
- credit history information from credit bureaus, which we use to help prevent and detect fraud and to offer certain credit or financial services to some customers.

Information You Can Access

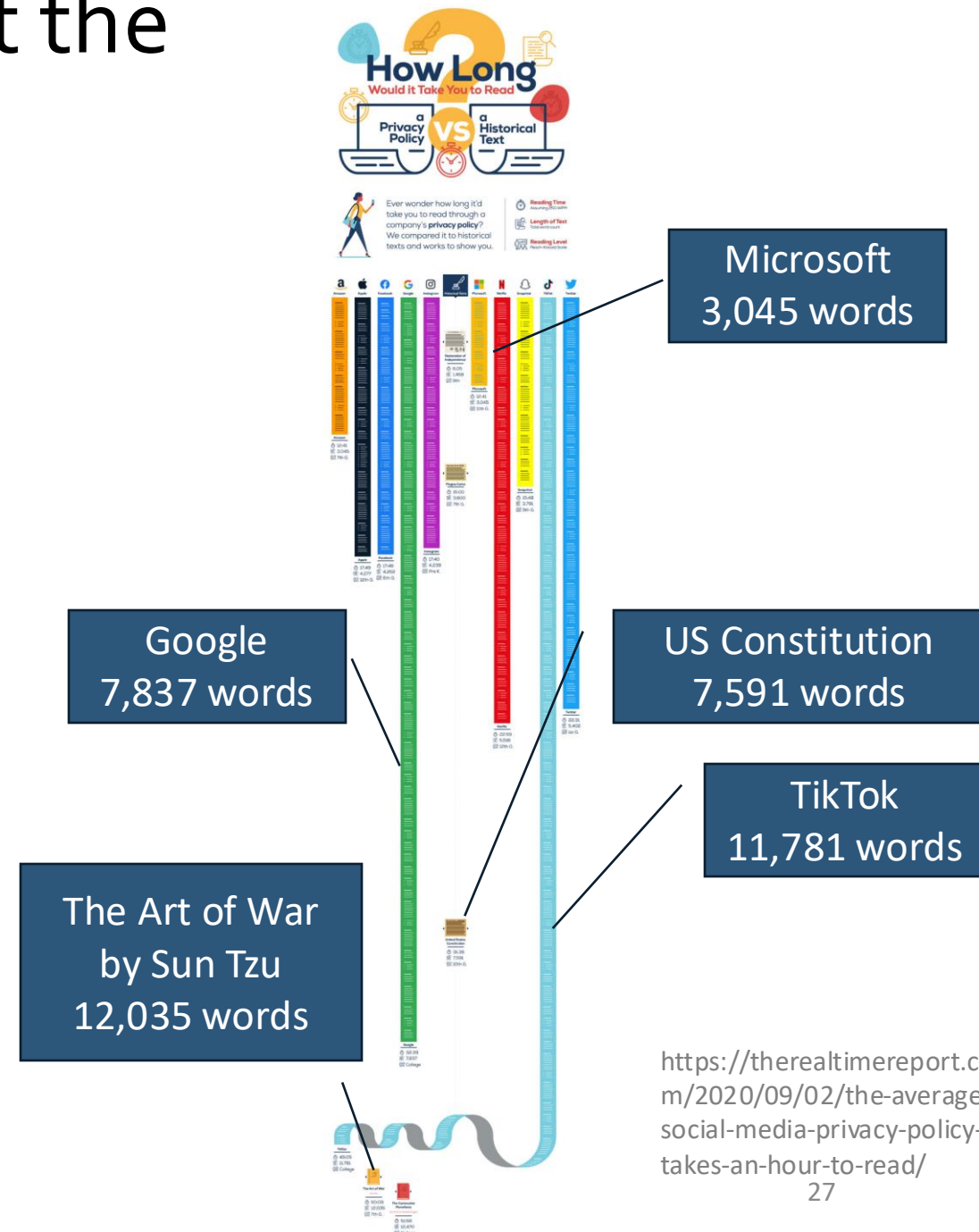
Examples of information you can access through Amazon Services include:

- status of recent orders (including subscriptions);
- your complete order history;
- personally identifiable information (including name, email, password, and address book);
- payment settings (including payment card information, promotional certificate and gift card balances, and 1-Click settings);
- notification settings (including Product Availability Alerts, Delivery, Special Order Availability Reminders and reminders);
- recommendations and the products you recently viewed that are the basis for recommendations (including Recommendations for You and Improve Your Recommendations);
- shopping lists and gift registries (including Wish Lists and Baby and Wedding Registries);
- your content, devices, services, and related settings, and communications and personalized advertising preferences;
- content that you recently viewed with us or Amazon;
- voice recordings associated with your account;
- your [Profile](#) (including your product Reviews, Recommendations, Reminders and personal profile);
- if you are a seller, you can access your account and other information, and adjust your communications preferences, by updating your account in [Seller Central](#).
- If you are an author, you can access your account and other information, and update your accounts, on the [Kindle Direct Publishing \(KDP\)](#) or [Author Central](#) website, as applicable.
- If you are a developer participating in our Developer Services Program, you can access your account and other information, and adjust your communication preferences, by updating your accounts in the [Developer Services Portal](#).

Was this information helpful?

How much money would it cost the US economy if everyone read through privacy policies?

- Notice and choice is dependent on awareness of content of privacy policies
- People do not read all the privacy policies, but if they did, how much would it cost the US economy?
- This information is important for policy makers and regulatory bodies (i.e. OPC)



**HOW MUCH MONEY WOULD IT COST
IF EVERYONE READ PRIVACY
POLICIES?**

Calculating the cost of reading privacy policies

$$T_R = p * R * n$$

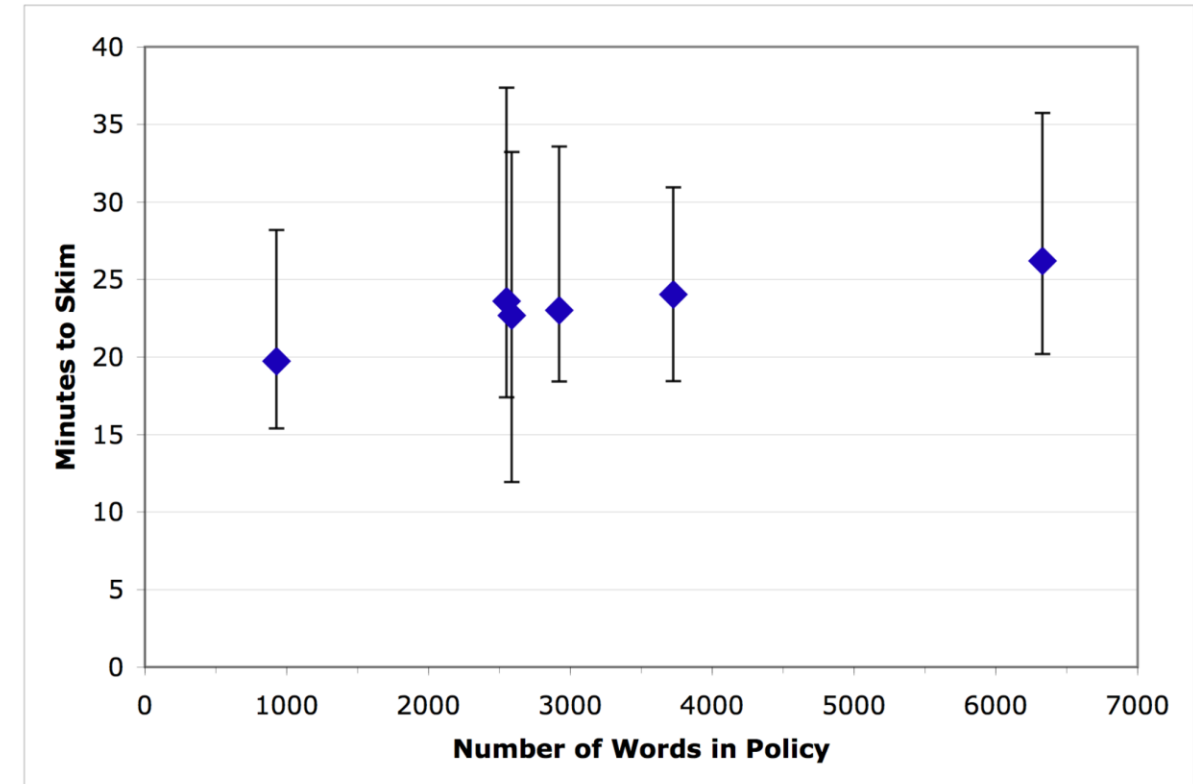
- T_R - Annual time to read online privacy policies
- p – Population of USA internet users
- R – Average national reading rate (words per minute)
- n – Average number of unique sites visited per year

Factors to consider:

- Cost of time at work (wages) vs time at home (opportunity cost)
- Number of websites seen at work vs at home
- Number of websites seen rather than visits
- People do not always read, they skim
- Privacy policies vary in length and content complexity

Amount of time needed to skim a policy

- Online survey where users had to find answers to privacy question in a provided policy
- Policies: very short policy (928 words), one very long policy (6,329 words) and four policies close to the typical 2,500 word length.
- The three policies clustered near 2,500 words ranged in median times from 23 to 24 minutes and did not show statistically significant differences in mean values.



- Result: skimming times are constant and do not vary by policy length

Cost of privacy policy reading: \$1.1 trillion a year

Estimate	Individual cost to read	Individual cost to skim	National cost to read	National cost to skim
Lower bound	\$2,533 / year (work: \$1,970; home: \$563)	\$1,140 / year (work: \$886; home: \$253)	\$559.7 billion / year (work: \$435 B; home: \$124 B)	\$251.9 billion / year (work: \$196 B; home: \$56 B)
Point	\$3,534 / year (work: \$2,791; home: \$743)	\$2,226 / year (work: \$1,758; home: \$468)	\$781 billion / year (work: \$617 B; home: \$164 B)	\$492 billion / year (work: \$389 B; home: \$103 B)
Upper bound	\$5,038 / year (work: \$4,203; home: \$835)	\$4,870 / year (work: \$4,063; home: \$807)	\$1.1 trillion / year (work: \$929 B; home: \$184 B)	\$1.1 trillion / year (work: \$898 B; home: \$178 B)

LAYERED PRIVACY POLICIES

Structured Layered Notices

- Privacy policies are too complex to read
- But if consumers can't or won't read them, we lose all the value of privacy policies
- Idea: structured notices
- Banks in the US are required to provide privacy notices in a specific format



FACTS

WHAT DOES THE CHARLES SCHWAB CORPORATION DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none">• Social Security number and income• account balances and transaction history• investment experience and assets
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons The Charles Schwab Corporation chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does The Charles Schwab Corporation share?	Can you limit this sharing?
For our everyday business purposes —such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	YES	NO
For our marketing purposes —to offer our products and services to you	YES	NO
For joint marketing with other financial companies	NO	We don't share
For our affiliates' everyday business purposes —information about your transactions and experiences	YES	NO
For our affiliates' everyday business purposes —information about your creditworthiness	YES	YES
For our affiliates to market to you	YES	YES
For nonaffiliates to market to you	NO	We don't share

To limit our sharing	Call 877-812-1817 within the U.S. or +1-415-667-8400 from outside the U.S.—our menu will prompt you through your choices. Please note: If you are a new customer, we can begin sharing your information 30 days from the date we sent this notice. When you are no longer our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call 877-812-1817 or 800-435-4000 or go to schwab.com/privacy .

Who is providing this notice?	The Charles Schwab Corporation (also "Schwab") and its affiliates. See list of affiliates below.
-------------------------------	--------------------------------------------------------------------------------------------------

What we do	
How does Schwab protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. To learn more about security at Schwab, please visit www.schwab.com/schwabsafe .
How does Schwab collect my personal information?	We collect your personal information, for example, when you <ul style="list-style-type: none">• open an account or give us your income information• seek advice about your investments or tell us about your investment or retirement portfolio• make deposits or withdrawals from your account We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only <ul style="list-style-type: none">• sharing for affiliates' everyday business purposes — information about your creditworthiness• affiliates from using your information to market to you• sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. See below for more on your rights under state law.
What happens when I limit sharing for an account I hold jointly with someone else?	Your choices will apply to everyone on your account.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies <ul style="list-style-type: none">• Our affiliates include companies with a Charles Schwab (with the exception of Schwab Charitable™) or TD Ameritrade name; and nonfinancial companies such as Schwab Performance Technologies and Charles Schwab Media Productions Company.
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. <ul style="list-style-type: none">• The Charles Schwab Corporation does not share with nonaffiliates so they can market to you.
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. <ul style="list-style-type: none">• The Charles Schwab Corporation doesn't jointly market.

Other important information
Charles Schwab Bank, SSB, and Charles Schwab Premier Bank, SSB, are chartered under the laws of the State of Texas and by state law are subject to regulatory oversight by the Department of Savings and Mortgage Lending. Any consumer wishing to file a complaint against Charles Schwab Bank, SSB, or Charles Schwab Premier Bank, SSB, should contact the Department of Savings and Mortgage Lending through one of the means indicated below: In Person or by Mail: 2601 North Lamar Boulevard, Suite 201, Austin, Texas 78705-4294; Phone: 1-877-276-5550; Fax: 1-512-936-2003; or through the Department's website at https://www.smt.texas.gov/ .
California residents: Please go to schwab.com/ccpa to learn more about our Privacy Notice for California Residents.
Nevada residents: Nevada law requires us to disclose that you may request to be placed on Schwab's internal "do not call" list at any time by calling 800-435-4000, and that we are providing this notice to you pursuant to state law. You may obtain further information by contacting the Nevada Attorney General, 555 E. Washington Ave., Suite 3900, Las Vegas, NV 89101; phone 702-486-3132; email BCPINFO@ag.state.nv.us .
Vermont residents: We will automatically limit sharing of your information.
To learn more about our Online Privacy & Tracking practices, please go to schwab.com/online-privacy .
<small>©2024 The Charles Schwab Corporation. All rights reserved. E-0124-0885054018802718956 REG0009F4-19 (01/24)</small>

Structured Layered Notices

- Structured notices make finding information easier because it is in the same place on all policies
- Specific questions also require clear yes/no answers

FACTS

WHAT DOES THE CHARLES SCHWAB CORPORATION DO WITH YOUR PERSONAL INFORMATION?

Why?

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

What?

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and income
- account balances and transaction history
- investment experience and assets

How?

All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons The Charles Schwab Corporation chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does The Charles Schwab Corporation share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	YES	NO
For our marketing purposes— to offer our products and services to you	YES	NO
For joint marketing with other financial companies	NO	We don't share
For our affiliates' everyday business purposes— information about your transactions and experiences	YES	NO
For our affiliates' everyday business purposes— information about your creditworthiness	YES	YES
For our affiliates to market to you	YES	YES
For nonaffiliates to market to you	NO	We don't share

Structured Layered Notices

Nice idea but:

- Requires policy makers to make laws and regulations
- Requires in-depth knowledge of issues around a specific industry
- Nuances are hidden/lost
- People still do not normally read these
- Will not work for all sites

FACTS

WHAT DOES THE CHARLES SCHWAB CORPORATION DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	<p>The types of personal information we collect and share depend on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none">• Social Security number and income• account balances and transaction history• investment experience and assets
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons The Charles Schwab Corporation chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does The Charles Schwab Corporation share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	YES	NO
For our marketing purposes— to offer our products and services to you	YES	NO
For joint marketing with other financial companies	NO	We don't share
For our affiliates' everyday business purposes— information about your transactions and experiences	YES	NO
For our affiliates' everyday business purposes— information about your creditworthiness	YES	YES
For our affiliates to market to you	YES	YES
For nonaffiliates to market to you	NO	We don't share

GDPR AND RELATED REGULATIONS

Data Protection Directive (EU, 1995)

- **Notice**—data subjects should be given notice when their data is being collected;
- **Purpose**—data should only be used for the purpose stated and not for any other purposes;
- **Consent**—data should not be disclosed without the data subject's consent;
- **Security**—collected data should be kept secure from any potential abuses;
- **Disclosure**—data subjects should be informed as to who is collecting their data;
- **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data
- **Accountability**—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

Safe Harbor: International Safe Harbor Privacy Principles

- EU prohibited the transfer of data to countries with weaker privacy laws.
 - The US had weaker protection laws.....
- Safe Harbor was a list of privacy principles non-EU companies could promise to uphold
- Declared invalid in 2015 because the United States could order companies to give data

AMICUS BRIEFS

Data Protection Commissioner v Facebook and Max Schrems (Standard Contractual Clauses)

[DOWNLOAD PDF 269.0KB](#)

[CONTENTS](#) +

SUMMARY

One of the most important international privacy cases in recent history arose from a complaint against Facebook brought to the Irish Data Protection Commissioner by an Austrian privacy advocate named Max Schrems. In the complaint, Mr. Schrems challenged the transfer of his data (and the data of EU citizens' generally) to the United States by Facebook, which is incorporated in Ireland. The case ("Schrems I") led the Court of Justice of the European Union on October 6, 2015, to invalidate the Safe Harbor arrangement, which governed data transfers between the EU and the US.

**Sound familiar? US
wants to ban TikTok
because China
government can
access data....**

What a TikTok ban in the US could mean for you

BY THE ASSOCIATED PRESS

Updated 10:51 AM EDT, April 24, 2024

No, TikTok will not suddenly disappear from your phone. Nor will you go to jail if you continue using it after it is banned.

After years of attempts to [ban the Chinese-owned app](#), including by [former President Donald Trump](#), a measure to outlaw the popular video-sharing app has won congressional approval and is on its way to President Biden for his signature. The measure gives Beijing-based parent company ByteDance nine months to sell the company, with a possible additional three months if a sale is in progress. If it doesn't, TikTok will be banned.

So what does this mean for you, a TikTok user, or perhaps the parent of a TikTok user? Here are some key questions and answers.

WHEN DOES THE BAN GO INTO EFFECT?

The original proposal gave ByteDance just six months to divest from its U.S. subsidiary, negotiations lengthened it to nine. Then, if the sale is already in progress, the company will get another three months to complete it.

So it would be at least a year before a ban goes into effect — but with likely court challenges, this could stretch even longer, perhaps years. TikTok has seen some success with court challenges in the past, but it has never sought to prevent federal legislation from going into effect.

GDPR Principles

- **Lawfulness, fairness and transparency** – there needs to be a lawful basis for processing and the data subject as the right to know how their data will be used.
- **Purpose limitation** - data must be collected with the purpose and only used for it or compatible purposes.
- **Data minimization** – personal data should be adequate, relevant, and limited to what is necessary.
- **Accuracy** – personal data should be kept updated and incorrect data must be deleted.
- **Storage limitation** – only keep personal data as long as you need it
- **Integrity and confidentiality** (security) – appropriate security measures should be taken. Follow “integrity and confidentiality”.
- **Accountability** – take responsibility and keep records showing compliance.

GDPR differs from US notice-and-choice model

Notice-and-choice

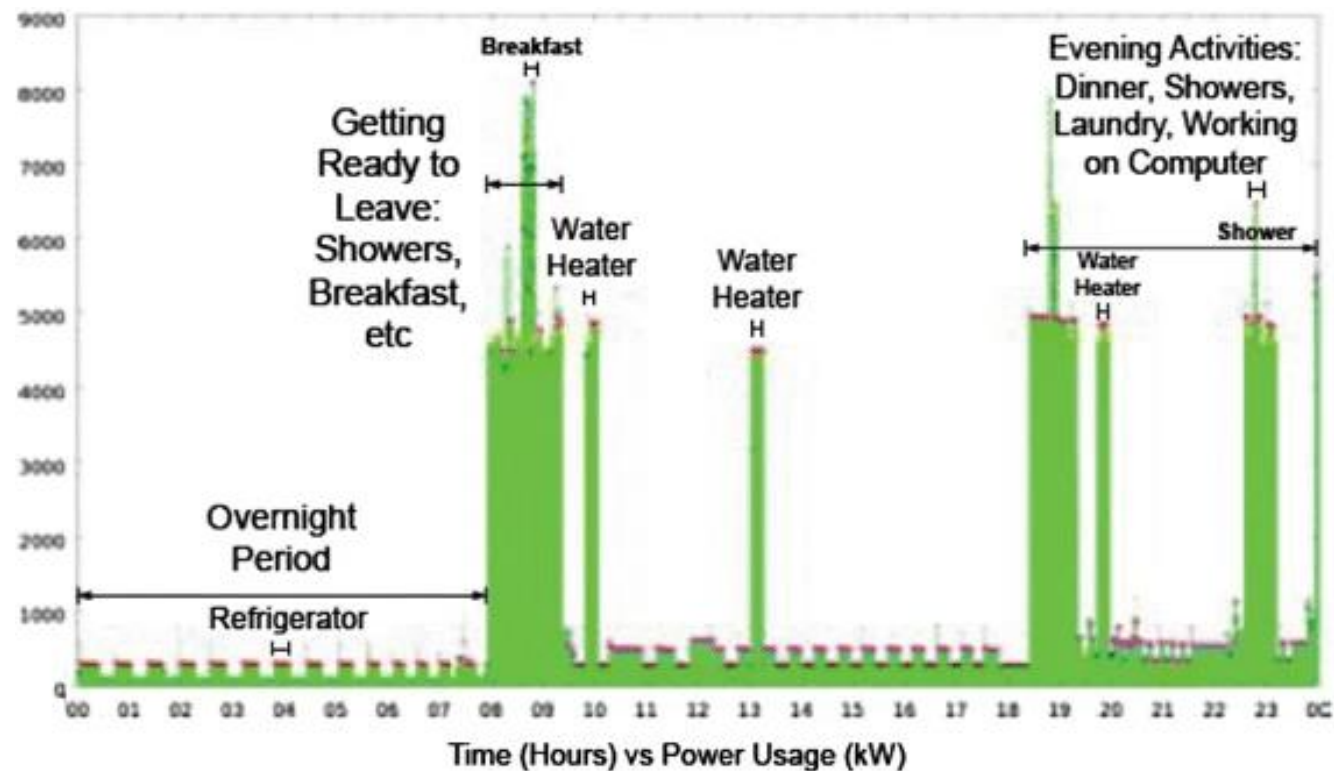
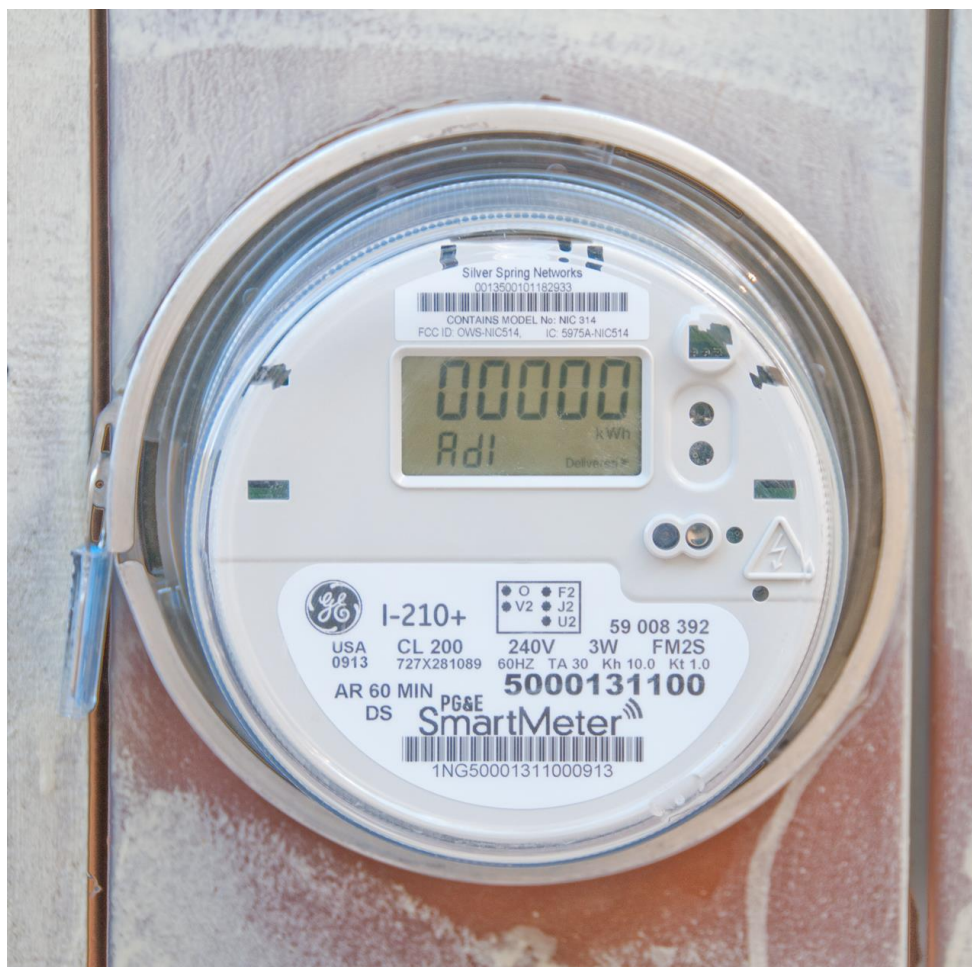
- Consumer is responsible for deciding who to give their data to
- Minimal government requirements about company behavior with data as long as behavior is disclosed to consumers
- Privacy loss is hard to link to evidence of harms, and legal system focuses on harms

GDPR

- Government has picked “guardrails” where privacy practices must conform to a stated set of rather broad rules
- Company that originally collects data legally responsible for ensuring it is used for the purposes originally stated AND that consent was given
- Privacy loss is considered an issue when data becomes used for purposes other than the original stated ones

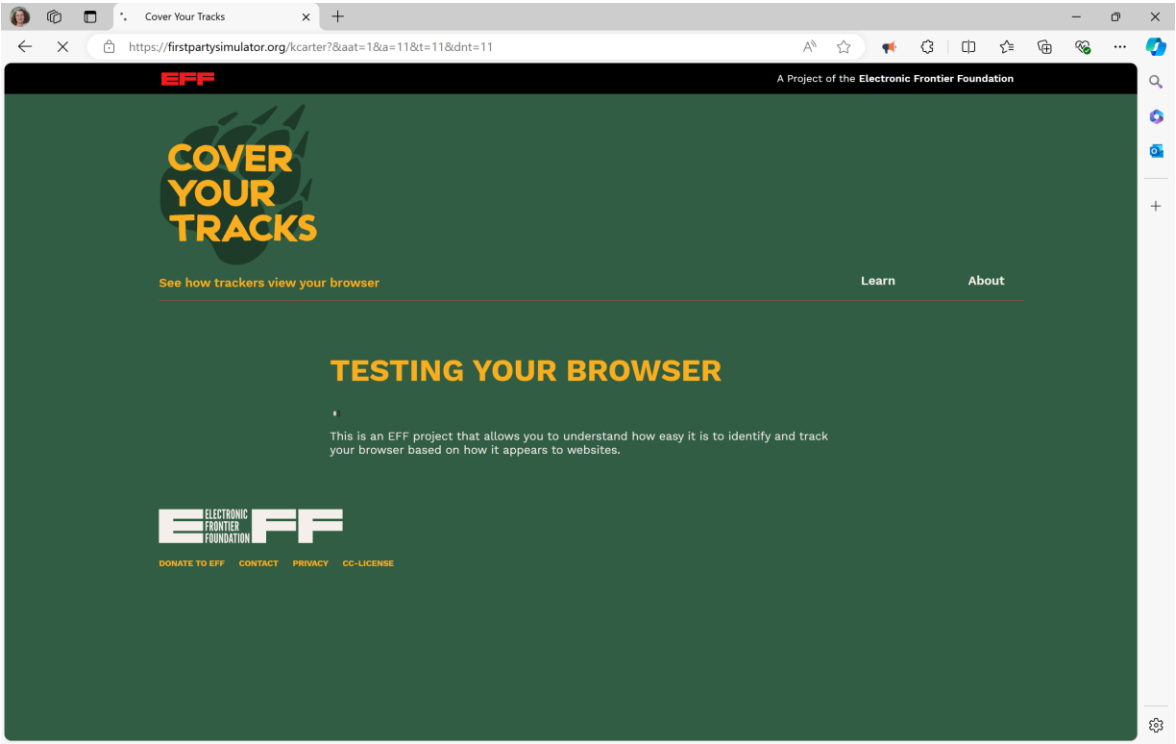
FINGERPRINTING

Smart Electricity Meter



Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D (2010) Private memoirs of a Smart Meter. In: workshop on embedded sensing systems for energy-efficiency in building

Browser Fingerprinting: <https://coveryourtracks.eff.org/> Visited via Edge on a Windows Surface



Our tests indicate that you are not protected against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	<u>No</u>
Blocking invisible trackers?	<u>No</u>
Protecting you from <u>fingerprinting</u> ?	Your browser has a unique fingerprint

Still wondering how fingerprinting works?

LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique** among the 169,763 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.37 bits of identifying information.**

<https://coveryourtracks.eff.org/> (Visited via Edge)

USER AGENT

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0

WHAT IS THIS?

A web header that relays information to the web server about your browser and its version.

HOW IS THIS USED IN YOUR FINGERPRINT?

This information can be very specific. *If customized* can single-handedly identify a specific user’s browser.

Bits of identifying information: **5.22**
One in *x* browsers have this value: **37.28**

HTTP_ACCEPT HEADERS

text/html, */*; q=0.01 gzip, deflate, br, zstd en-US,en;q=0.9

WHAT IS THIS?

A web header that is used to let the server know what types of content the browser is able to handle.

For example, a server can choose to deliver a plain text file if it sees that a user’s browser does not support rich documents.

HOW IS THIS USED IN YOUR FINGERPRINT?

This information can be fairly unique, and varies from browser to browser. However, this string doesn’t tend to change much over time, and can remain constant through many versions of the same browser.

Bits of identifying information: **3.26**
One in *x* browsers have this value: **9.55**

HASH OF CANVAS FINGERPRINT

9eb50926ea429abee0c1c45bee140a62

WHAT IS THIS?

A tracking site can perform a specific test on the HTML5 <canvas> element in your browser. This metric is the unique identification the tracker assigns to your browser after it performs this test.

Canvas fingerprinting is invisible to the user. A tracker can create a “canvas” in your browser, and generate a complicated collage of shapes, colors, and text using JavaScript. Then, with the resulting collage, the tracker extracts data about exactly how each pixel on the canvas is rendered. Many variables will affect the final result. These include your operating system, graphics card, firmware version, graphics driver version, and installed fonts.

HOW IS THIS USED IN YOUR FINGERPRINT?

This is a complex and very reliable fingerprinting metric for trackers.

Slightly different images will be rendered due to small differences in:

- video card hardware,
- video drivers,
- operating system, and
- installed fonts.

These settings are different from one computer to the next. But they tend to be consistent enough on a single machine to clearly identify a user.

Bits of identifying information: **10.07**
One in *x* browsers have this value: **1077.88**

Default Firefox on Surface

Our tests indicate that you have **some protection** against Web tracking, but it has **some gaps**.

IS YOUR BROWSER:

Blocking tracking ads?	<u>Partial protection</u>
Blocking invisible trackers?	<u>Partial protection</u>
Protecting you from fingerprinting?	<u>Your browser has a unique fingerprint</u>

My Normal Firefox on Surface with Javascript blocker and adblocker enabled

Our tests indicate that you have **strong protection** against Web tracking.

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from fingerprinting?	Your browser has a nearly-unique fingerprint

Default Firefox on Surface

Our tests indicate that you have **some protection** against Web tracking, but it has **some gaps**.

IS YOUR BROWSER:

Blocking tracking ads?	<u>Partial protection</u>
Blocking invisible trackers?	<u>Partial protection</u>
Protecting you from <u>fingerprinting</u> ?	<u>Your browser has a unique fingerprint</u>

Your browser fingerprint **appears to be unique** among the 168,171 tested in the past 45 days.

My Normal Firefox on Surface

with Javascript blocker and adblocker enabled

Our tests indicate that you have **strong protection** against Web tracking.

IS YOUR BROWSER:

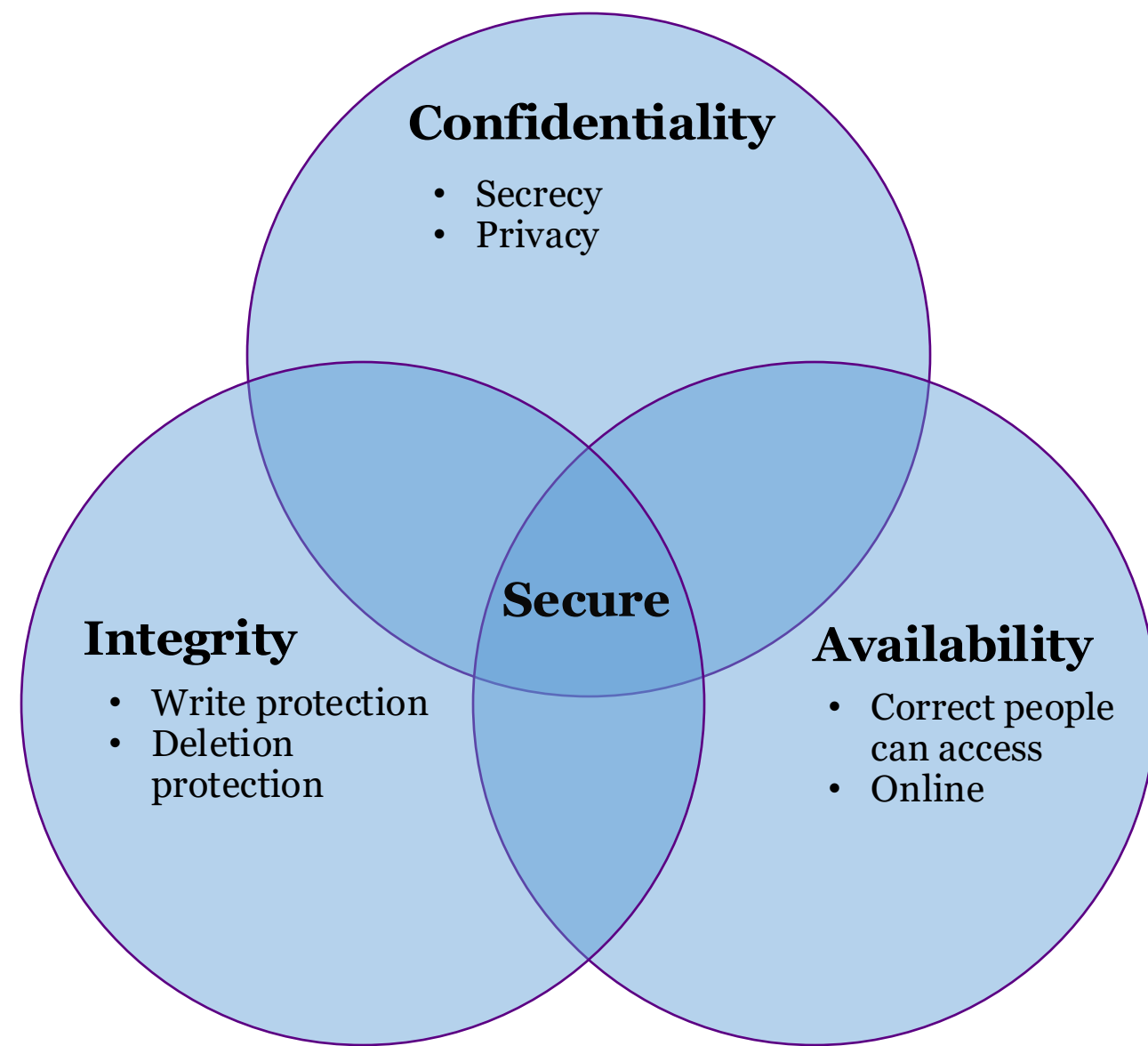
Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from <u>fingerprinting</u> ?	Your browser has a nearly-unique fingerprint

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 84086.5 browsers have the same fingerprint as yours**.

ENCRYPTION \neq PRIVACY

Defining Security - CIA

- **Confidentiality**
 - Ensures that computer-related assets are accessed only by authorized parties.
- **Integrity**
 - Assets can be modified only by authorized parties or only in authorized ways.
- **Availability**
 - Assets are accessible to authorized parties at appropriate times.



Bad assumption....

- Cryptography gives us Confidentiality
- Privacy is all about Confidentiality
- Encryption == Privacy

- If a person uses an app that supports end-to-end encryption they get confidentiality and therefore privacy.
 - Actually, they may not get either privacy or security

WhatsApp is E2E encrypted. Does that give you privacy?

- Natalie May Edwards was convicted of “unlawful disclosure”
- Aka talking to a journalist confidentially
- She used WhatsApp
- Her WhatsApp conversation metadata was used in court

Former Senior FinCEN Employee Sentenced To Six Months In Prison For Unlawfully Disclosing Suspicious Activity Reports

Thursday, June 3, 2021

Share

>

For Immediate Release

U.S. Attorney's Office, Southern
District of New York

Natalie Mayflower Sours Edwards Repeatedly Transmitted SARs and

Alexander. EDWARDS had access to each of the pertinent SARs and saved them — along with thousands of other files containing sensitive government information — to a flash drive provided to her by FinCEN. **She transmitted the SARs to Reporter-1 by means that included taking photographs or images of them and texting the photographs or images to Reporter-1 over an encrypted application.** In addition to disseminating SARs to Reporter-1, EDWARDS sent or described to Reporter-1 internal FinCEN emails or correspondence appearing to relate to SARs months in federal prison for unlawfully disclosing Suspicious Activity Reports (“SARs”) and other sensitive information. **EDWARDS previously pled guilty** to participating in a conspiracy to disclose SARs before United States District Judge Gregory H. Woods, who imposed today’s sentence.

WhatsApp is E2E encrypted. Does that give you privacy?

- *Message content* in WhatsApp is E2E encrypted
- Metadata like who is sending/receiving is not E2E encrypted and the times sending and receiving happen
- WhatsApp shares contact data with Facebook
- Law enforcement can and does request detailed metadata about WhatsApp chats



WhatsApp is E2E encrypted. Does that give you privacy?

- EU fined Facebook for saying it would not share WhatsApp data with Facebook and then doing so

PRESS RELEASE | 18 May 2017 | Brussels | 4 min read

Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover

[Top](#)

[Related topics](#)

[Print friendly pdf](#)

[Contacts for media](#)

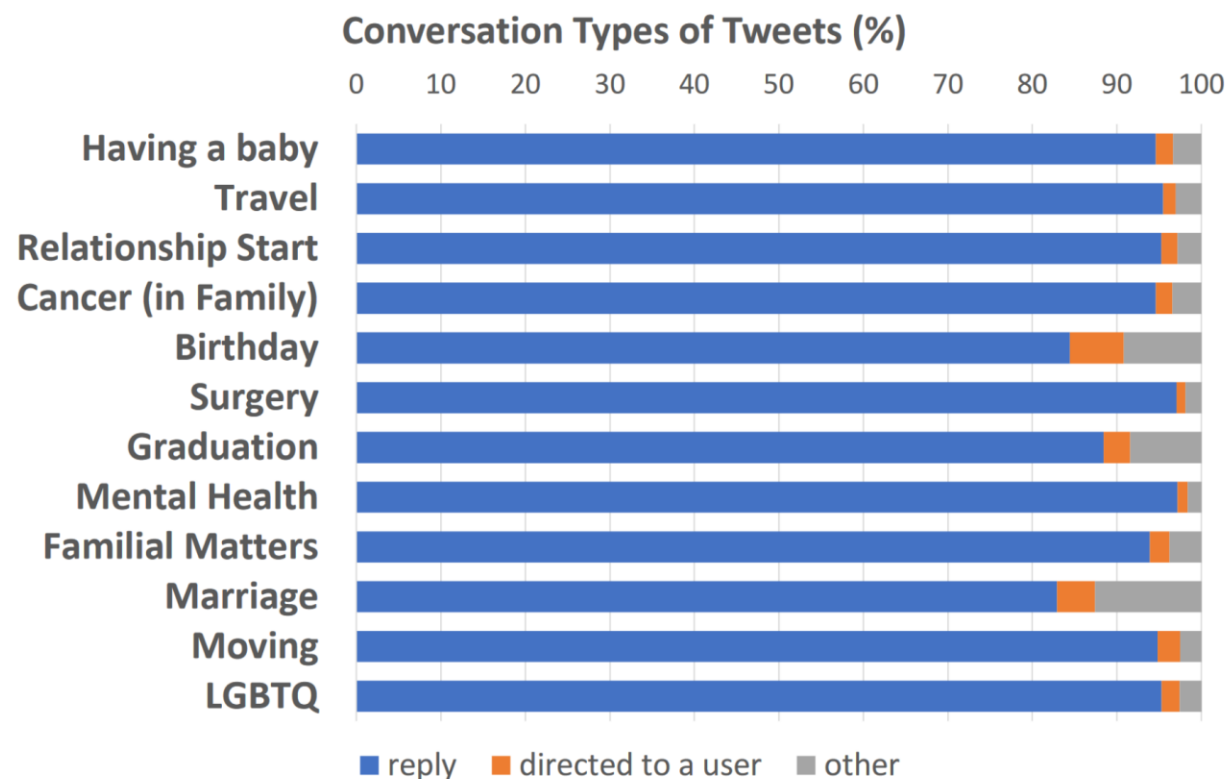
The European Commission has fined Facebook €110 million for providing incorrect or misleading information during the Commission's 2014 investigation under the EU Merger Regulation of Facebook's acquisition of WhatsApp.

Commissioner Margrethe **Vestager**, in charge of competition policy, said: "*Today's decision sends a clear signal to companies that they must comply with all aspects of EU merger rules, including the obligation to provide correct information. And it imposes a proportionate and deterrent fine on Facebook. The Commission must be able to take decisions about mergers' effects on competition in full knowledge of accurate facts.*"

WhatsApp is E2E encrypted. Does that give you privacy?

- You can learn quite a bit about someone from what their friends post
- Knowing who their friends are really helps
- Contact lists create a network graph with weights based on how often communication happens

Privacy leakage on Twitter. Automatic identification of life events of Protected accounts.



Unexpected uses of technology make making good choices hard

- You are more inclined to trust people who look like people you trust (including yourself)
- Idea: use AI to create ads that look like someone you would trust by combining a model with your or your friend's face
- This approach is nearly impossible to detect and is effective

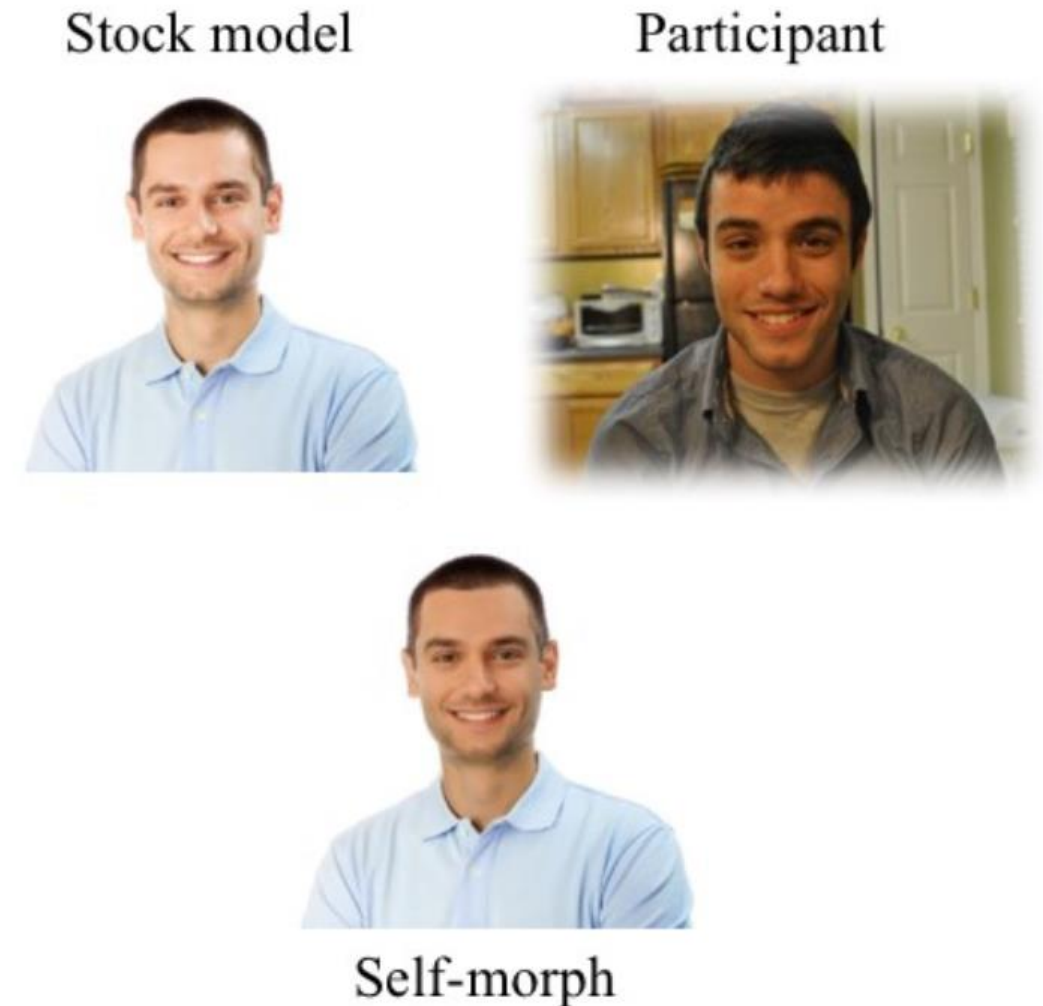



Figure 1. Example stimuli used in Study 1.

Metadata can have huge impacts on people

- Many cases of people being declared dead by an algorithm
 - This woman was declared dead (incorrectly) when a former employee “told the court she had died to win damages from her beneficiaries, following two other failed lawsuits.”
 - She had to get COVID shots by pretending to be homeless, because dead people don’t get healthcare




 **Reuters** World ▾ Business ▾ Markets ▾ More ▾ My News 🔍 Register

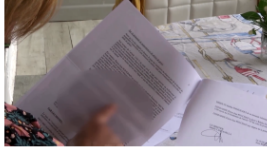
Europe

Frenchwoman officially considered dead fights to be "alive" again

By Cecile Mantovani

September 1, 2021 8:38 AM EDT · Updated 3 years ago



SAINT-JOSEPH, France, Aug 31 (Reuters) - Declared dead by a French court in 2017, Jeanne Pouchain has spent the past four years trying to escape a bewildering legal twilight zone and prove to officialdom that she is in fact very much alive. She says the experience has been devastating.

"My name was Jeanne. It still is Jeanne, after I've been declared dead in 2017," says the 59-year old, smoking cigarette after cigarette. She breaks into tears at times when recounting her ordeal - and what she plans for when she will officially be "alive" again.

It all started, Pouchain recalls, when the family received a letter four years ago from a court saying mistakenly that she was dead and that her husband and son had to pay for money she was alleged to have owed.

The letter was part of a complicated legal procedure launched by a former employee of Pouchain's cleaning business and, unlike what they had assumed at first, it was not easy, or quick, to clear up the error.

Well that is concerning....

Only real option is to hide in plain sight

STEGANOGRAPHY

Steganography

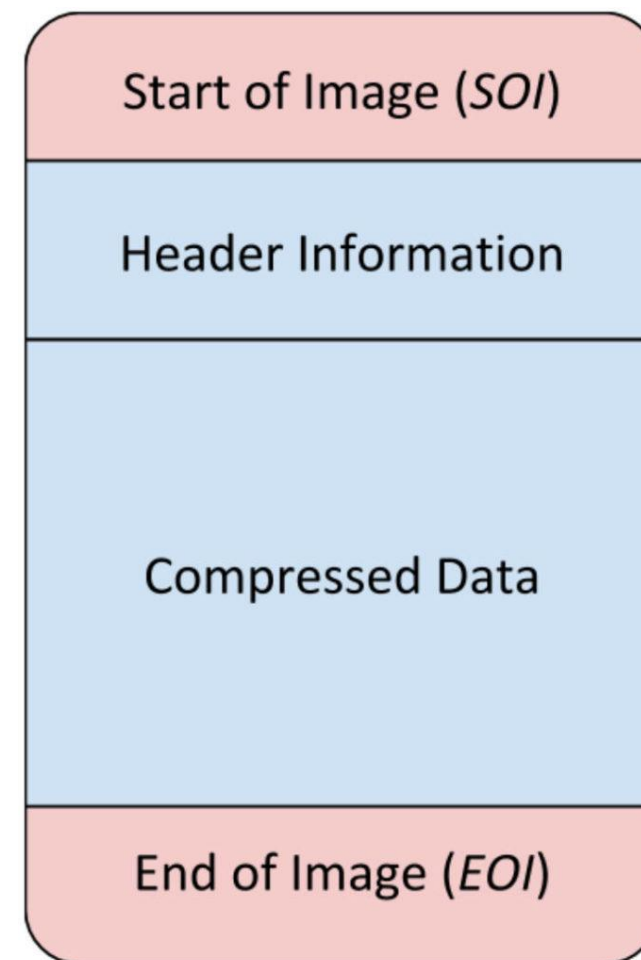
- Hiding information in plain sight
- Used to hide that a message is even being sent
- Or used to hide the real message in a less problematic message



Photo of a kitten?
Secret message?
Both?

Hiding information in images

- Jpeg format includes a start of image and end of image set string
- Photo viewers will stop reading after reading the EOI even if there is more data



Jpeg images

- First line (BASE64) for two kitten photos

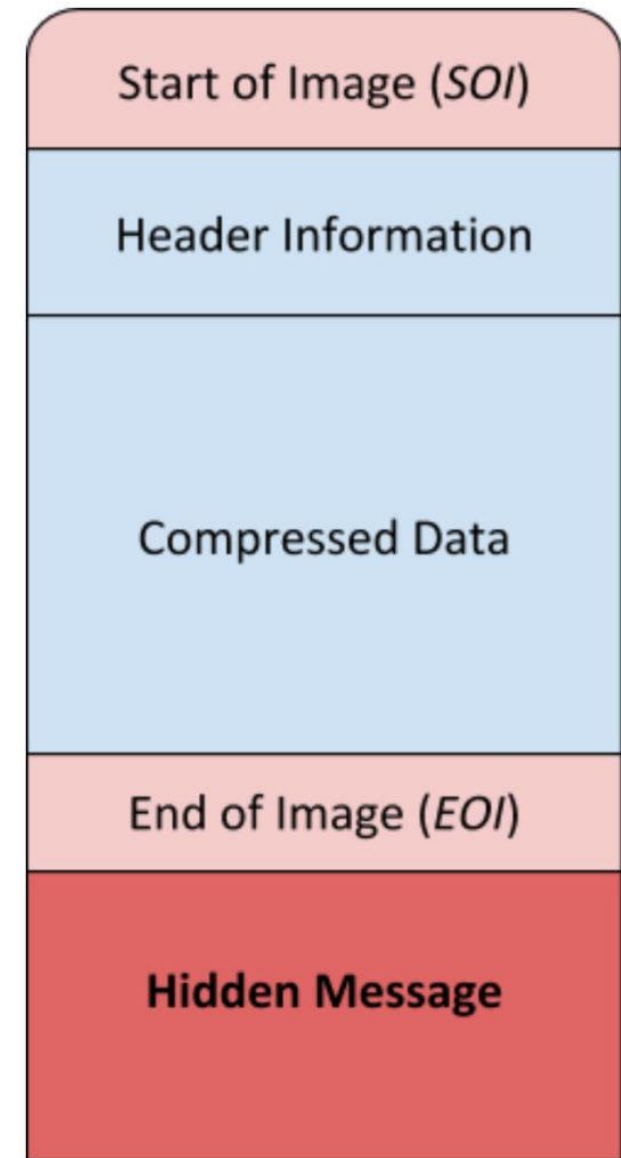


```
/9j/4AAQSkZJRgABAQAAQABAAAD/4TIGRXhpZgAATU0AKgAAAACwEPAAIAAAAGAAAIngEQAAIA  
/9j/4AAQSkZJRgABAQAAQABAAAD/4TIGRXhpZgAATU0AKgAAAACwEPAAIAAAAGAAAIngEQAAIA
```



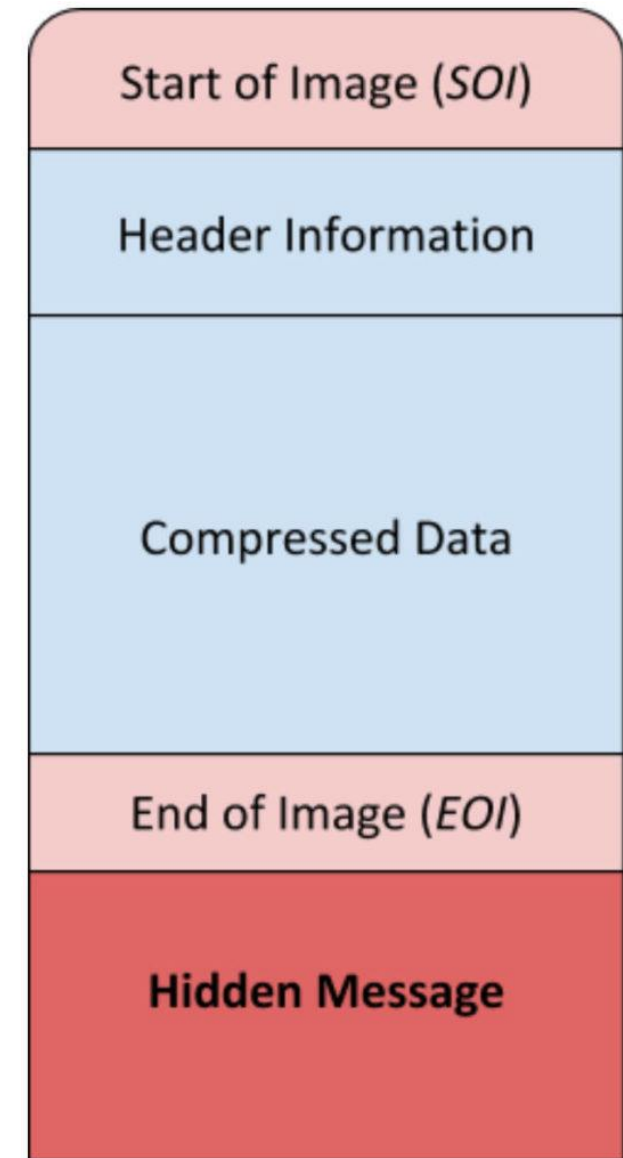
Hiding information in images

- Jpeg format includes a start of image and end of image set string
- Photo viewers will stop reading after reading the EOI even if there is more data
- So just put some data at the end of the file after the EOI



Hiding information in images

- Problem: the “Hidden Message” still has identifiable substrings
- Great Firewall of China (for example) that looks at all packets going past would spot unacceptable content
- Scanning software that scans the whole file will also spot the message



Hide in least significant bits

- Images are just RGB values

R = 11111111

G = 00000000

B = 00000000

- Lowest values have minimal impact on color
- Text is just bits
- Swap message bits for least significant image bits

S = 01010011

O = 01001111

S = 01010011

Encode SOS in lowest two bits

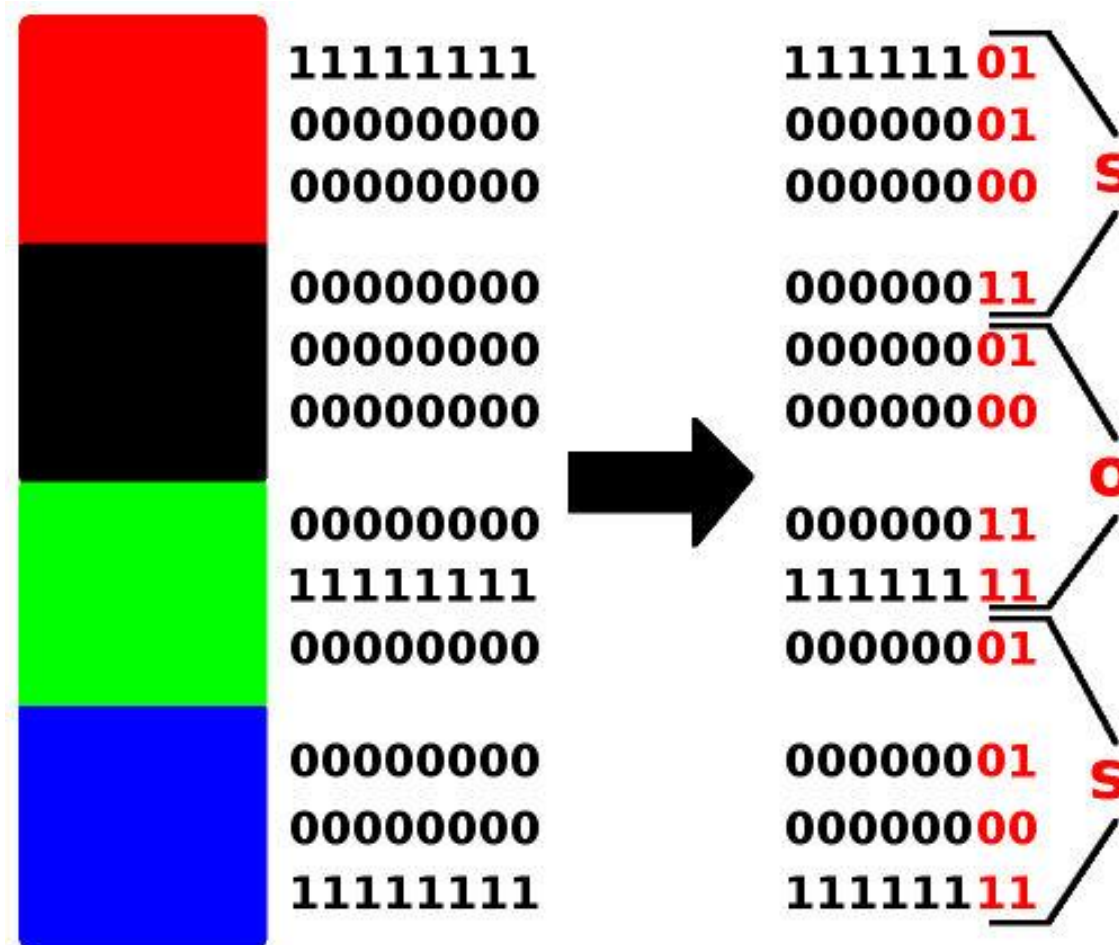


Image Steganography

Original



R = 11111111**1**
G = 00000000
B = 00000000

1 bit used to hide



Image Steganography

Original



3 bits used to hide



Image Steganography

Original



5 bits used to hide



Image Steganography

Original



6 bits used to hide



Image Steganography

Original



7 bits used to hide

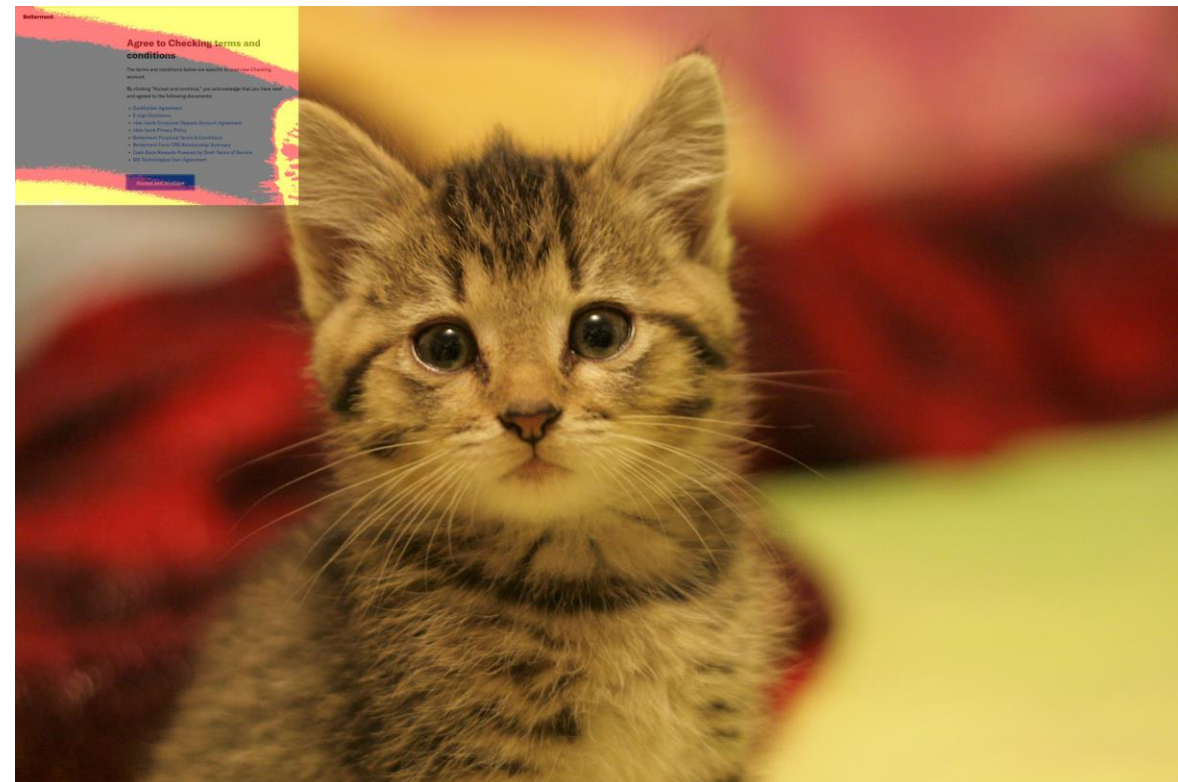


Image Steganography

Hidden Image

R = 11111111
G = 00000000
B = 00000000

7 bits used to hide

Betterment | Joint Checking signup

Agree to Checking terms and conditions

The terms and conditions below are specific to your new Checking account.

By clicking "Accept and continue," you acknowledge that you have read and agreed to the following documents:

- [Cardholder Agreement](#)
- [E-sign Disclosure](#)
- [nbkc bank Consumer Deposit Account Agreement](#)
- [nbkc bank Privacy Policy](#)
- [Betterment Financial Terms & Conditions](#)
- [Betterment Form CRS Relationship Summary](#)
- [Cash Back Rewards Powered by Dosh Terms of Service](#)
- [MX Technologies User Agreement](#)

Accept and continue

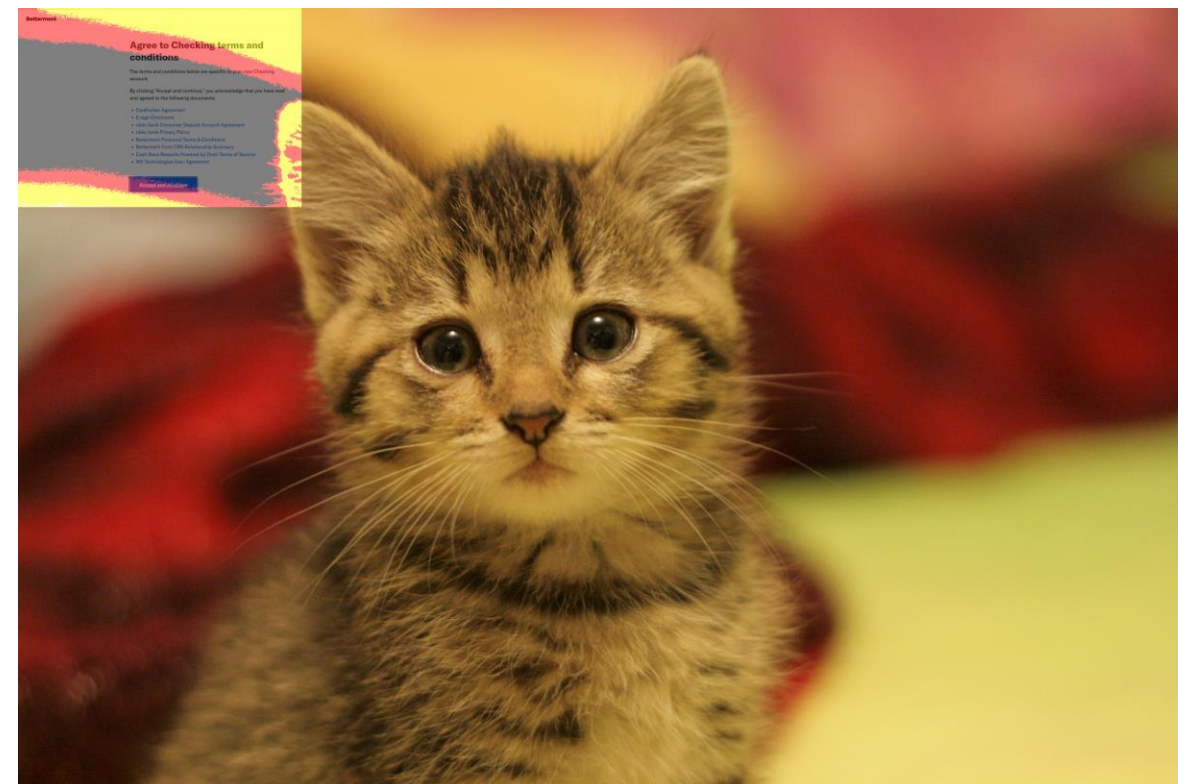


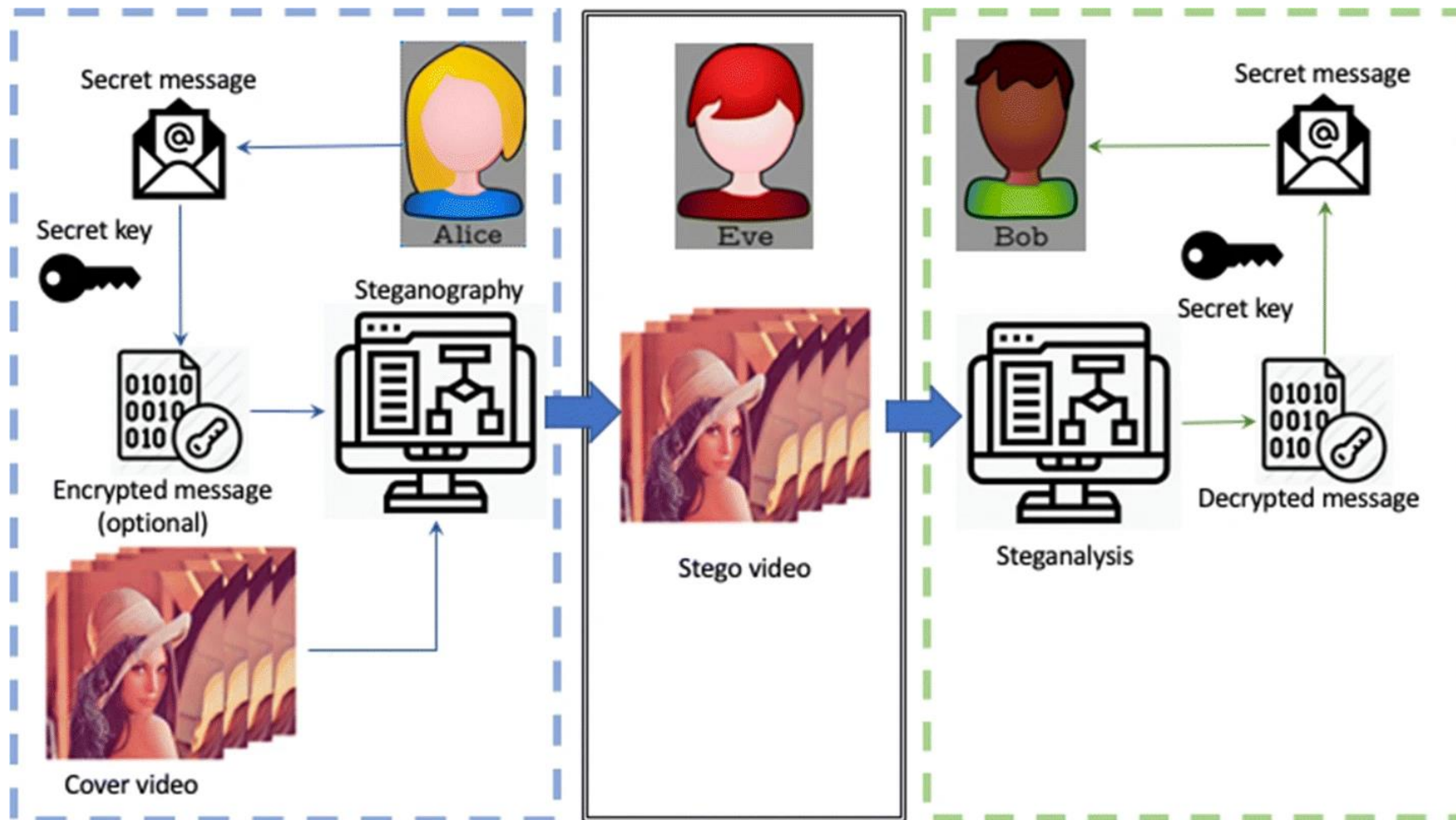
Image Steganography

- Challenging to automatically identify
- Pattern is mixed in with the image bits so simple pattern matching the file will not find it
- Larger image than message needed

3 bits used to hide



Video call steganography

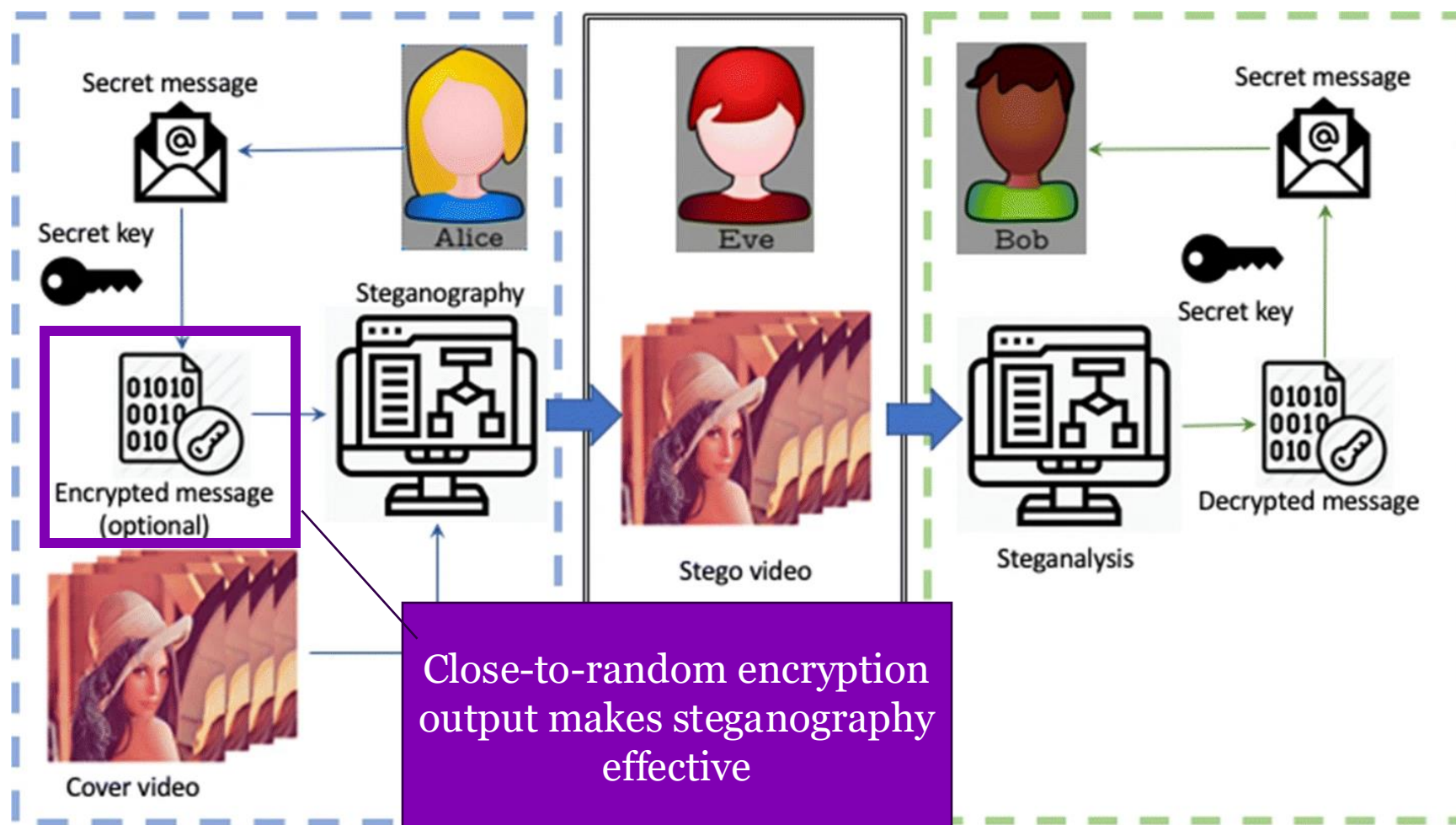


Alice and Bob communicate with each other using steganography methods. Eve does not suspect their secret communication since the secret information is not visible to HVS

Remember: Security model of what a "good" cipher is

- **Perfect Security** – Given any ciphertext, all possible plaintexts of that length are equally likely
- **Concrete Security** – Adversary needs to do X work to break the cipher
- **Indistinguishability** - The adversary is not able to distinguish between two messages M_1 and M_2 of the same length
- **Random Oracle** - Ciphertext looks random in that there is no efficient way to distinguish it from a random function.

Video call steganography



Alice and Bob communicate with each other using steganography methods. Eve does not suspect their secret communication since the secret information is not visible to HVS

Steganography Summary

- Effective way to hide “real” communication
- Relies on attacker not knowing it is there
- Communication still happens



Think-pair-share

- If Natalie May Edwards had used steganography instead of E2E encryption (WhatsApp) would it have protected her better?
- US FBI requested that WhatsApp record and provide metadata on her account
- She was observed to be speaking to a reporter frequently
- That reporter then published an article including information Edwards had

Former Senior FinCEN Employee Sentenced To Six Months In Prison For Unlawfully Disclosing Suspicious Activity Reports

Alexander. EDWARDS had access to each of the pertinent SARs and saved them — along with thousands of other files containing sensitive government information — to a flash drive provided to her by FinCEN. [She transmitted the SARs to Reporter-1 by means that included taking photographs or images of them and texting the photographs or images to Reporter-1 over an encrypted application.](#) In addition to disseminating SARs to Reporter-1, EDWARDS sent or described to Reporter-1 internal FinCEN emails or correspondence appearing to relate to SARs

Natalie Mayflower Sours Edwards Repeatedly Transmitted SARs and Other Sensitive Government Information to A Reporter

Audrey Strauss, the United States Attorney for the Southern District of New York, announced that NATALIE MAYFLOWER SOURS EDWARDS, a/k/a “Natalie Sours,” a/k/a “Natalie May Edwards,” a/k/a “May Edwards,” a former Senior Advisor at the Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”), was sentenced to six months in federal prison for unlawfully disclosing Suspicious Activity Reports (“SARs”) and other sensitive information. [EDWARDS previously pled guilty](#) to participating in a conspiracy to disclose SARs before United States District Judge Gregory H. Woods, who imposed today’s sentence.

IDENTITY AND DATA OWNERSHIP

Defining privacy

- The Cambridge Dictionary

- Someone's right to keep their personal matters and relationships secret
 - Right to control the disclosure and use of personal data
 - Right to not disclose information
- Be alone and control access to themselves
 - Right to be let alone
 - Right to control access to themselves
 - Right to have a space (physical, digital, mental) that is inaccessible to others



"On the Internet, Nobody knows you're a dog."

- **Anonymity** – No link to your identity
 - Great for hiding, bad for doing things like buying stuff
- **Multiple identities** – Most people have multiple identities naturally. You have an identity with every account.
 - Linking identities is considered a privacy breach
- **Pseudonymity** – A unique identifier exists but it is not linked to the true identity.
 - Writers often have Pen Names where they call themselves something else when publishing than when they get a bank account.



By Peter Steiner in The New Yorker 1993

Is your address your “identity”?

- Address is considered Personally Identifying Information but that is different than identity
- To the right is a list of people who lived in my “stair” in Edinburgh before me
- Addresses identify, but they do not necessarily identify you

John Scott, a young joiner, charged with “riding his bicycle at a furious and reckless pace down Minto Street”—police estimated 12mph; he said it was more like 11. Fined £1. (1897)

Thomas Calderwood, a destitute and unemployed law clerk from Shetland. Defrauded his landladies out of several pounds (in loans) as well as food and lodging by telling them he was employed by a good law firm. 10 days in jail. (1895)

Alexander Anderson, fireman, and Marion Johnston, his pregnant partner. Marion laughed at Alexander having difficulty lighting his pipe, so he knocked her down and

1 year in jail (1890)

Margaret Robertson, who lived there with her father after separating from her husband, Andrew Robertson. Their divorce case was the highlight of the 1887/88 season. (details below...)

Margaret, 27, had (according to the judge) “given herself up to the most intemperate use of intoxicating drinks” and was “in every particular reprehensible.” Her husband was (we are told) a respectable teetotal accountant.

Concept of data ownership: who owns data (Western)

- Western culture is very individualistic.
- Assumption is that the individual owns data that they create or about them
- Yet, when companies are fined for individual data loss, money is given to "the public"
- Oracle collected and sold personal data

Oracle reaches \$115 million consumer privacy settlement



JONATHAN STEMPEL

July 19, 2024 at 11:14 AM



By Jonathan Stempel

(Reuters) - Oracle agreed to pay \$115 million to settle a lawsuit accusing the database software and cloud computing company of invading people's privacy by collecting their personal information and selling it to third parties.

A preliminary settlement of the proposed class action was filed on Thursday night in San Francisco federal court, and requires a judge's approval. Oracle denied wrongdoing.

The plaintiffs, who otherwise have no connection to Oracle, said the company violated federal and state privacy laws and California's constitution by creating unauthorized "digital dossiers" for hundreds of millions of people.

They said the dossiers contained data including where people browsed online, and where they did their banking, bought gas, dined out, shopped and used their credit cards.

Oracle then allegedly sold the information directly to marketers or through products such as ID Graph, which according to the company helps marketers "orchestrate a relevant, personalized experience for each individual."

The settlement covers people whose personal information Oracle collected or sold since Aug. 19, 2018.

Concept of data ownership: who owns data (Indigenous)

- Indigenous culture is generally more collective (over simplification)
- Focus on not only privacy but also on community value of the data
- FAIR was created by researchers to ensure that data is not only available but also useful to other researchers
- CARE looks at issues like collective benefit and how data collected about indigenous people can benefit or harm indigenous communities



AI Data as a Public Good

Some resources are considered a public good where they are owned by “the public” and use is licensed

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

AERONAUTICAL MOBILE

AERONAUTICAL MOBILE SATELLITE

AERONAUTICAL RADIONAVIGATION

AIRTEL

BROADCASTING

BROADCASTING SATELLITE

EARTH EXPLORATION SATELLITE

FIXED

FIXED SATELLITE

INTER-SATELLITE

LAND MOBILE

LAND MOBILE SATELLITE

LAND-TO-LAND

LAND-TO-SPACE

LAND-TO-SPACE SATELLITE

METEOROLOGICAL SATELLITE

MOBILE

MOBILE SATELLITE

RADIO ASTRONOMY

RADIO DETERMINATION SATELLITE

RADIOLOCATION

RADIOLOCATION SATELLITE

RADIONAVIGATION

RADIONAVIGATION SATELLITE

RADIO RESEARCH

STANDARD FREQUENCY AND TIME SIGNAL

STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

SPACE OPERATION

SPACE RESEARCH

STANDARD FREQUENCY AND TIME SIGNAL

STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

NON-FEDERAL EXCLUSIVE

FEDERAL/COMMON/FEDERAL SHARED

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	Fixed	Capital Letter
Secondary	Mobile	1st Capital with letter case letters

The table is a public representation of the table of frequency allocations and is not to be used for the purpose of frequency allocation. It is intended to provide a general overview of the frequency allocation process and is not to be used for the purpose of frequency allocation. It is intended to provide a general overview of the frequency allocation process and is not to be used for the purpose of frequency allocation.

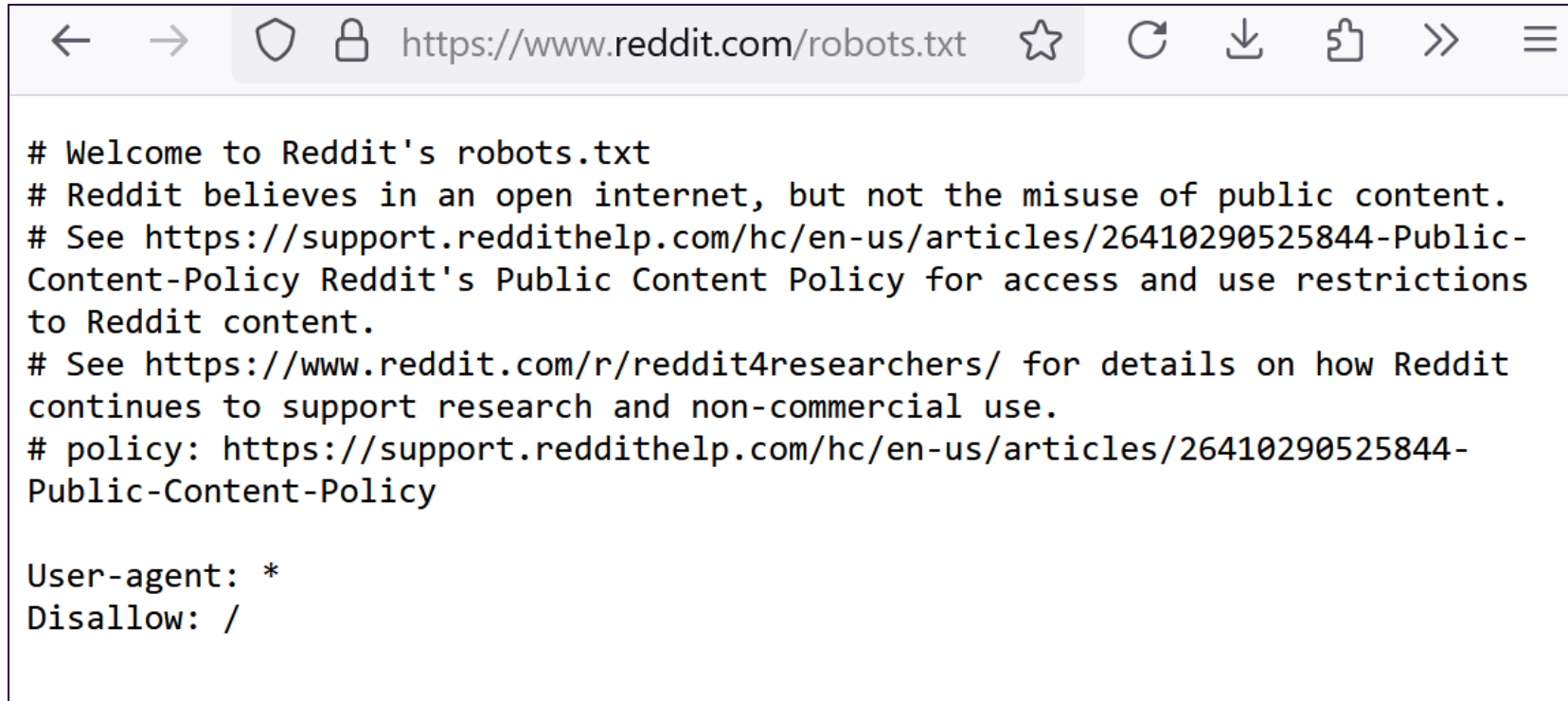
U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
JANUARY 2016

The chart displays frequency allocations for the United States, categorized by service type and frequency range. The services are color-coded according to the legend: Aeronautical Mobile (light blue), Aeronautical Mobile Satellite (light green), Aeronautical Radionavigation (red), Airtel (yellow), Broadcasting (dark green), Broadcasting Satellite (light blue), Earth Exploration Satellite (orange), Fixed (pink), Fixed Satellite (purple), Inter-Satellite (light yellow), Land Mobile (dark blue), Land Mobile Satellite (light green), Land-to-Land (dark red), Land-to-Space (dark blue), Land-to-Space Satellite (light green), Meteorological Satellite (light blue), Mobile (dark blue), Mobile Satellite (purple), Radio Astronomy (light blue), Radio Determination Satellite (light green), Radio Location (yellow), Radio Location Satellite (light blue), Radionavigation (dark green), Radionavigation Satellite (light blue), Radio Research (orange), Standard Frequency and Time Signal (pink), and Standard Frequency and Time Signal Satellite (purple). The frequency ranges are shown on the x-axis, with major divisions at 0 kHz, 300 kHz, 3 MHz, 30 MHz, 300 MHz, 3 GHz, and 300 GHz. The chart is divided into several sections, each representing a different frequency band and its associated services. The services are listed in a grid format, with the frequency range and the service type indicated by the color and the text within the grid cells. The chart is a complex and detailed representation of the radio spectrum, showing the allocation of frequencies for various services and the potential for future growth and development.

AI Data as a Public Good

Should the data collected and used to train AI models be considered a public good?

If it was, what obligations would AI companies have to give back to the public?



```
# Welcome to Reddit's robots.txt
# Reddit believes in an open internet, but not the misuse of public content.
# See https://support.reddithelp.com/hc/en-us/articles/26410290525844-Public-Content-Policy Reddit's Public Content Policy for access and use restrictions to Reddit content.
# See https://www.reddit.com/r/reddit4researchers/ for details on how Reddit continues to support research and non-commercial use.
# policy: https://support.reddithelp.com/hc/en-us/articles/26410290525844-Public-Content-Policy

User-agent: *
Disallow: /
```

In the USA each state has its own security breach notification laws

Summary 


Security Breach Notification Laws

Updated January 17, 2022

Related Topic: **TECHNOLOGY**

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws requiring private businesses, and in most states, governmental entities as well, to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data or information brokers, government entities, etc.); definitions of “personal information” (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

Search 

State	Applies to Private Sector	Applies to Government*
Alabama	Ala. Code § 8-38-1 et seq.	Ala. Code § 8-38-1 et seq.
Alaska	Alaska Stat. § 45.48.010 et seq.	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 18-551 to	Ariz. Rev. Stat. § 18-551 to

California maintains a public list of data breaches

- Most states require companies to notify state residence when there is a data breach
- Some (inc. California) also post those breach notifications online

Organization Name	Date(s) of Breach	Reported Date ▼
PHL Variable Insurance Company in Rehabilitation	11/02/2023	07/19/2024
Fidelity Investments Life Insurance Company & Empire Fidelity Investments Life Insurance Company	10/29/2023	07/19/2024
CCM Health	04/03/2023, 04/10/2023	07/18/2024
United Seating and Mobility L.L.C, dba Numotion	02/29/2024, 03/02/2024	07/17/2024
Financial Business and Consumer Solutions, Inc.	02/14/2024, 02/26/2024	07/17/2024
FCDG Management LLC	10/22/2023	07/16/2024
INJECTABLE THERAPY SERVICES, INC	12/08/2023	07/16/2024
MarineMax, Inc.	03/01/2024, 03/10/2024	07/16/2024
Designed Receivable Solutions, Inc.	01/18/2024	07/16/2024
Central Contra Costa Transit Authority	05/05/2024	07/15/2024
MNGI Digestive Health	08/20/2023	07/15/2024
Kaiser Foundation Hospitals, Northern California and The Permanente Medical Group, Inc.	n/a	07/15/2024
Freudenberg Medical, LLC	11/10/2023, 11/11/2023	07/15/2024
Rite Aid Corporation	06/06/2024	07/15/2024

QUESTIONS