

ECE750: Usable Security and Privacy

Designing notice, choice, and privacy policies

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



UNIVERSITY OF
WATERLOO

FACULTY OF
ENGINEERING



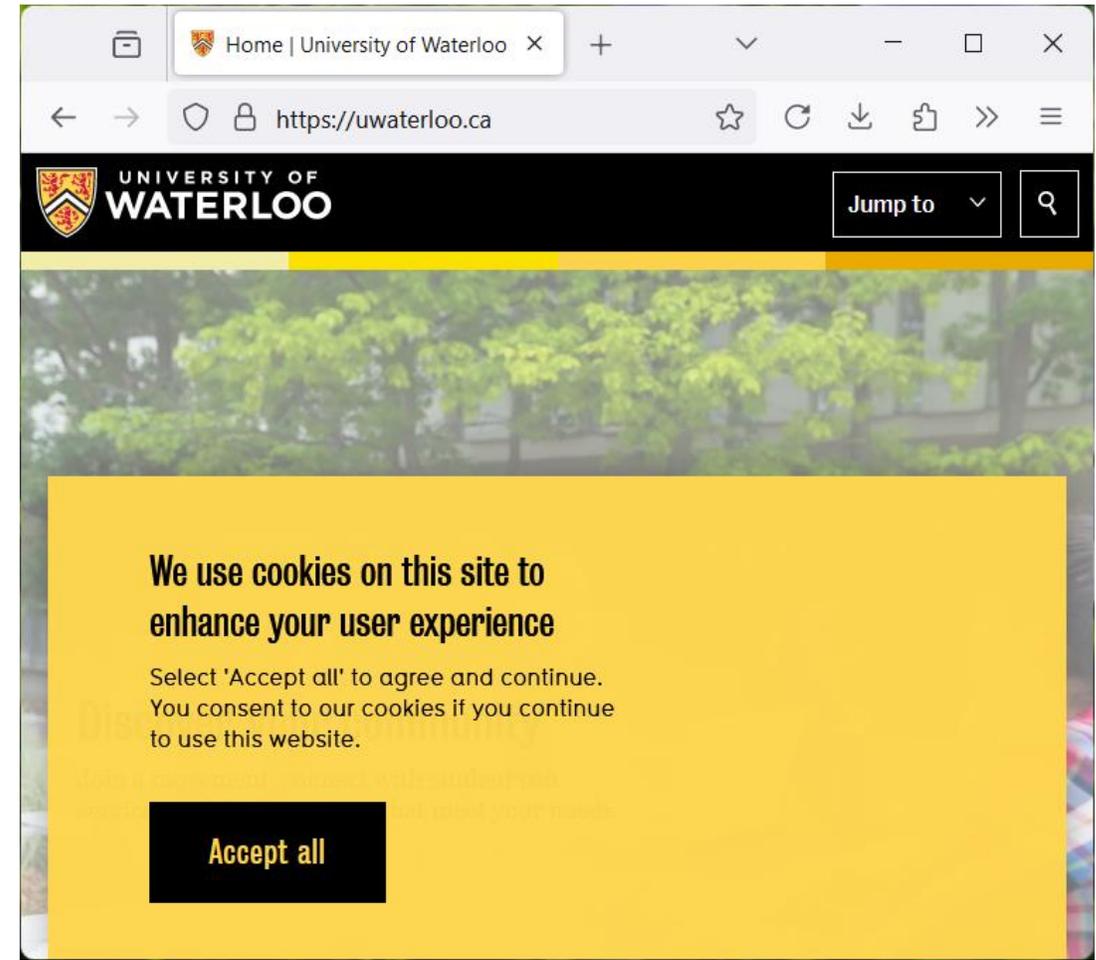
First, the news...

- 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

NOTICE AND CHOICE

Notice and Choice: The idea

- Users have the right to know how their data will be used
- 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.

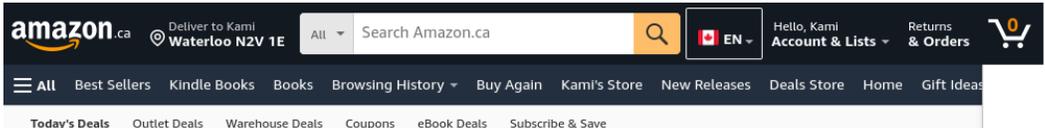
By clicking "Accept and continue," you acknowledge that you have read and agreed to the following documents:

- [Cardholder Agreement](#)
- [E-sign Disclosure](#)
- [nbc bank Consumer Deposit Account Agreement](#)
- [nbc 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](#)

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

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 visit browser or device accounts Amazon Services and other services we serve 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 performance.** 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 service, we can your voice input, images, videos, and other personal information to respond to your requests, provide the requested service to you, and improve our services. For more information about Alexa voice services, [click here](#).
- **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 target 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 Ad Policy](#).
- **Fraud Prevention and Credit Risk.** We use personal information to prevent and detect fraud and abuse in order to protect the true 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 third parties for use on or through Amazon Services, 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 Alexa 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 a sale 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 case 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, 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 protection and credit risk reduction.

Other than as set out above, you will receive notice when 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 or 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 device 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.
- It is important for you to protect against unauthorized access to your password and to your computers, 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 Ad Policy](#). To adjust your advertising preferences, please go to the [Advertising Preferences](#) page.
- **Use of Third-Party Advertising Services.** We provide certain types of 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 suggest ads that you will not see served as ad to download the app again. Some ad companies also use this information to share your 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 our Amazon Services.
- 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, and 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 Service that requires you to Sign In. For more information about cookies and other identifiers, see our [Cookies Notice](#).
- If you want to know where websites without linking the browsing history to your account, you may do so by logging out of your account from and blocking cookies on your browser. Amazon Services restricts the use of the accuracy of technical errors, your interactions with service features and content, your settings, preferences and backup information, location of your device naming an application information about updated images and files such as the name, 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, downloaded images, length of visits to certain pages, and page interaction information (such as scrolling, clicks, and mouseovers).
- Phone numbers used 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, and other behavioral information.

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 concerns 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 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 inferring and read modifications to our 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 cart, 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](#); 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 content, or use to interact with other users, or interact with an Amazon device or service;
- configure your settings on, provide data access permissions for, or interact with an Amazon device or service;
- upload your contacts;
- specify a [Specialized Information](#) identifier;
- employ [Product Availability Alerts](#), such as [Available to Order Notifications](#).

- use to interact with other users, or interact with an Amazon device or service;
- 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 content, or use to interact with other users, or interact with an Amazon device or service;
- offer your product information to other Amazon Services;
- communicate with us by phone, email, or otherwise;
- complete a questionnaire, a request ticket, or a contact area 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](#);
- compile [Playlists](#), [Watchlists](#), [Wish Lists](#) or other gift registries;
- participate in [Discussion Boards](#) or other community features;
- provide and use Reviews;
- specify a [Specialized Information](#) identifier;
- 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 numbers;
- payment information;
- your IP address;
- your location information;
- your name;
- people, addresses and phone numbers listed in your Address;
- 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 stored 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;
- device and Wi-Fi and configurations, including Wi-Fi credentials, if you choose to automatically synchronize them with your Amazon devices.

- #### Automatic Information
- Examples of 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;
 - device and financial information, such as content downloads, streams, and playback details, including duration and number of simultaneous streams and downloads, and network data for streaming and download quality, including information about your internet service provider;
 - device metrics such as when a device is in use, application usage, connectivity data, and any errors or event failures;
 - Amazon Services metrics like: the accuracies of technical errors, your interactions with service features and content, your settings, preferences and backup information, location of your device naming an application information about updated images and files such as the name, 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, downloaded images, length of visits to certain pages, and page interaction information (such as scrolling, clicks, and mouseovers).
 - phone numbers used 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, and 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, and 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

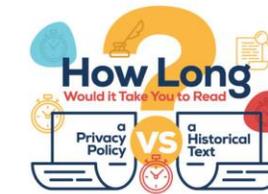
Examples of information you can access through Amazon Services include:

- 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 certificates and gift card balances, and 1-Click settings);
- account modification settings (including Product Availability Alerts, Deliveries, Specialized Information Reminders and readmits);
- recommendations and the products you recently viewed that are the basis for recommendations; and
- shopping lists and gift registries (including Wish Lists and Baby and Wedding Registries);
- your content, device, services, and related settings, and communications and personalized advertising preferences;
- content that you recently viewed (including content that you viewed and improved their Recommendations);
- 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 communications 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)



Ever wonder how long it'd take you to read through a company's privacy policy? We compared it to historical texts and works to show you.



Microsoft
3,045 words

Google
7,837 words

US Constitution
7,591 words

TikTok
11,781 words

The Art of War
by Sun Tzu
12,035 words

<https://therealtimeport.com/2020/09/02/the-average-social-media-privacy-policy-takes-an-hour-to-read/>

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?
- To estimate costs, the information to the right is needed:
 - How many websites do people visit at work? At home?
 - How many unique policies encountered?
 - How much time is required to read all those policies? To skim them?
 - Average salary in USA.
 - Estimate of home time value in dollars

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

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 visited per year

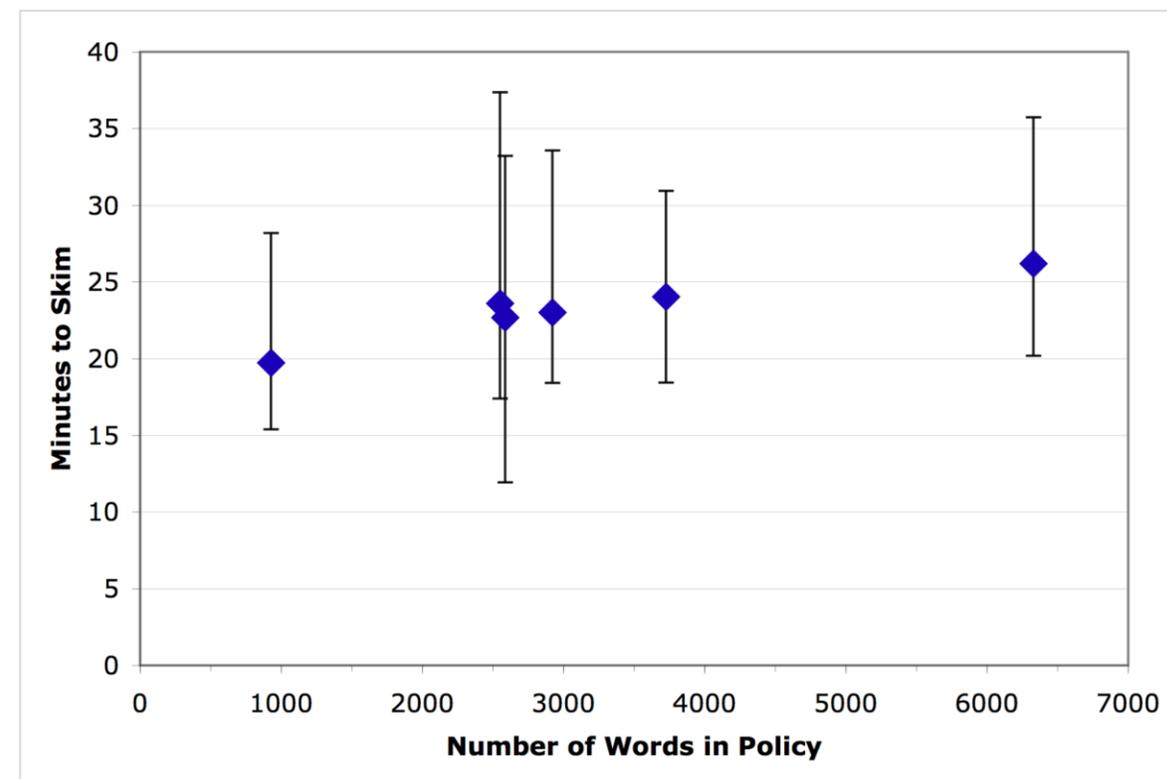
Lets look at how
skimming time
was determined.

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.

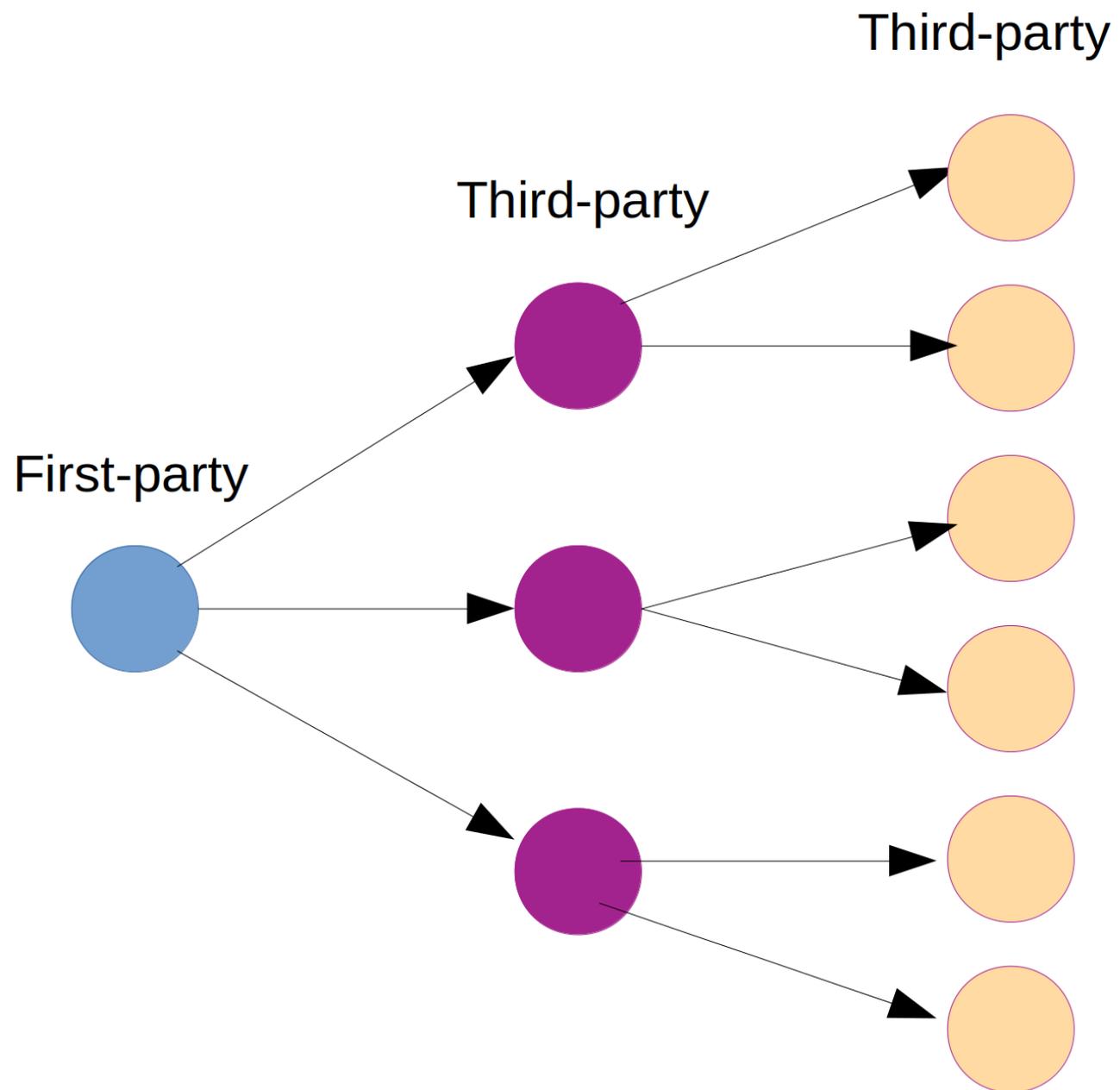


- Result: skimming times are constant and do not vary by policy length

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)

But wait... we learned earlier that web pages are made up of lots of content. Doesn't each site have its own privacy policy?



Think-pair-share

- When was the last time you looked at a privacy policy or other similar document?
- What were you looking for?
- OR if you have never read a privacy policy:
 - What was the last time you had a question about how a company treats your data?
 - How did you find the answer to that question? Or why did you give up?

STRUCTURED LAYERED NOTICES

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 we are	
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 .	
©2024 The Charles Schwab Corporation. All rights reserved. E-0124-586554613802718954 REG6035FM14-19 (01/24)	

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: <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

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?	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

P3P, DNT, AND OTHERS

P3P Platform for Privacy Preferences (2002)

- US Government told companies that privacy was an issue. They needed to find a solution or the Government would regulate.
- W3C worked with companies to propose a machine-readable privacy policy.
- Idea was that users would express their privacy preferences once to their browser. Then the browser would automatically compare preferences to each site's privacy policy.
- Automatic negotiation would happen between the browser and the site to pick the best privacy option for this user.
- No one has to read long policies any more.

Simple Example P3P Policy

```
<?xml version="1.0"?>
<P3P xmlns="http://www.w3.org/2002/01/P3Pv1">
  <POLICY>
    <ENTITY>
      <DATA-GROUP>
        <DATA ref="#business.name">ExampleCorp</DATA>
        <DATA ref="#business.contact-info.online.email">privacy@example.com</DATA>
      </DATA-GROUP>
    </ENTITY>

    <ACCESS>
      <contact-and-other/>
    </ACCESS>

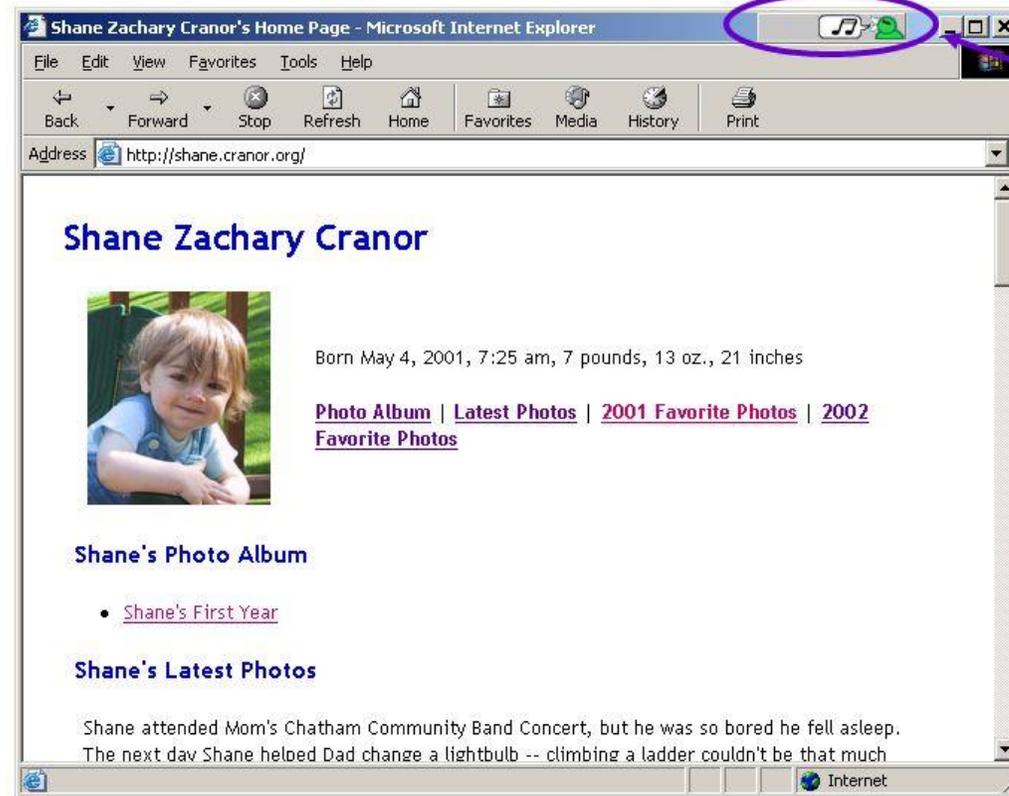
    <DISPUTES-GROUP>
      <DISPUTES resolution-type="independent">
        <SERVICE>PrivacySeal</SERVICE>
        <STATEMENT>We follow industry best practices for dispute resolution.</STATEMENT>
      </DISPUTES>
    </DISPUTES-GROUP>
```

```
<STATEMENT>
  <PURPOSE><current/><admin/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><indefinitely/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#user.name"/>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.clickstream"/>
    <DATA ref="#dynamic.http"/>
  </DATA-GROUP>
</STATEMENT>
</POLICY>
</P3P>
```

P3P Privacy Bird Plugin

Use of P3P User Agent by Early Adopters

Chirping bird is privacy indicator



Privacy Finder and Privacy Bird

- Search engine that includes P3P information in the results



poster

Search Engine: Google Yahoo! Preference Level:



[Privacy Report](#)

[Decorate with Framed Posters, Art Prints & Photography from Barewalls.com](#)

Offers posters and lithographs. Custom framing, canvas transfers, and board mounting services also available.

<http://www.barewalls.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)



[Privacy Report](#)

[AllPosters.com - The World's Largest Poster and Print Store!](#)

Online store for posters and prints of movies, actors, sports, music, and other subjects.

<http://www.allposters.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)

P3P was politically challenging to create

- There were many stakeholders (advertising companies, technology companies, consumer rights groups, international legal issues, etc.)
- Structured content requires some loss of details, and companies view those details as vital

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

Sharing with partners, preferred partners, affiliates, associated companies

- Companies have complex relationships with each other, often managed via formal contract.
- What does “share” mean? What about “transfer”? Or “rent”? “Access”?
- There is a large difference between selling data to a third party and sharing it with a “preferred provider” under an ongoing relationship legal contract.

Sharing with partners, preferred partners, affiliates, associated companies



- “We do not sell the names or other Personal Information of our customers. We do not disclose the names or other Personal Information of our customers to companies outside of [BMO Financial Group](#), for their own use, without consent unless required or permitted by law. “
- We may disclose your Personal Information to:
 - “To a merchant, a payment system, a payment card network, or a telecommunications provider.”
 - “To companies or affiliates where we offer loyalty or reward programs, for the purposes of the program, include analyzing and developing new benefits.”
 - “To BMO's affiliates or other companies to provide services on our behalf such as data processing, account administration, analytics and marketing.”

Do Not Track

- Mozilla-initiated attempt to send a much simpler computer signal: track, don't track, or no setting.
- Hard to incorrectly interpret (theoretically)
- Companies refused to honor the signal so it died

REGULATIONS

Notice and Consent is a key part of many laws and regulations

GDPR

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

FTC

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

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.



USA Phone

7:41 📶 🔋

Cancel **Payment** Login

✓ Add to Apple Wallet

Collect from station ⓘ

To pay

Booking fee £0.80

Total £45.40

Set up Apple Pay

Pay by card

Pay with **PayPal**

[Login](#) or [Create a trainline account](#)

We'll send you personalised marketing, valuable discounts and great offers.

Tick here if you don't want this

By booking your ticket you accept our **Website Terms & Conditions** and **National Rail conditions of travel**

Privacy policy applies

EU Phone

📶 giffgaff 🔋 7:41 pm 23%

Cancel **Payment**

To pay

Booking fee £0.75

16-25 Railcard discounts applied

Total £30.20

Card security code

.....

Pay by card

[Change payment method](#)

Be first to hear

Yes, I want great discounts, sales, offers and more from Trainline.

By booking your ticket you accept our **Website Terms & Conditions** and **National Rail conditions of travel**

Privacy policy applies

PRIVACY BY DESIGN

Privacy by Design

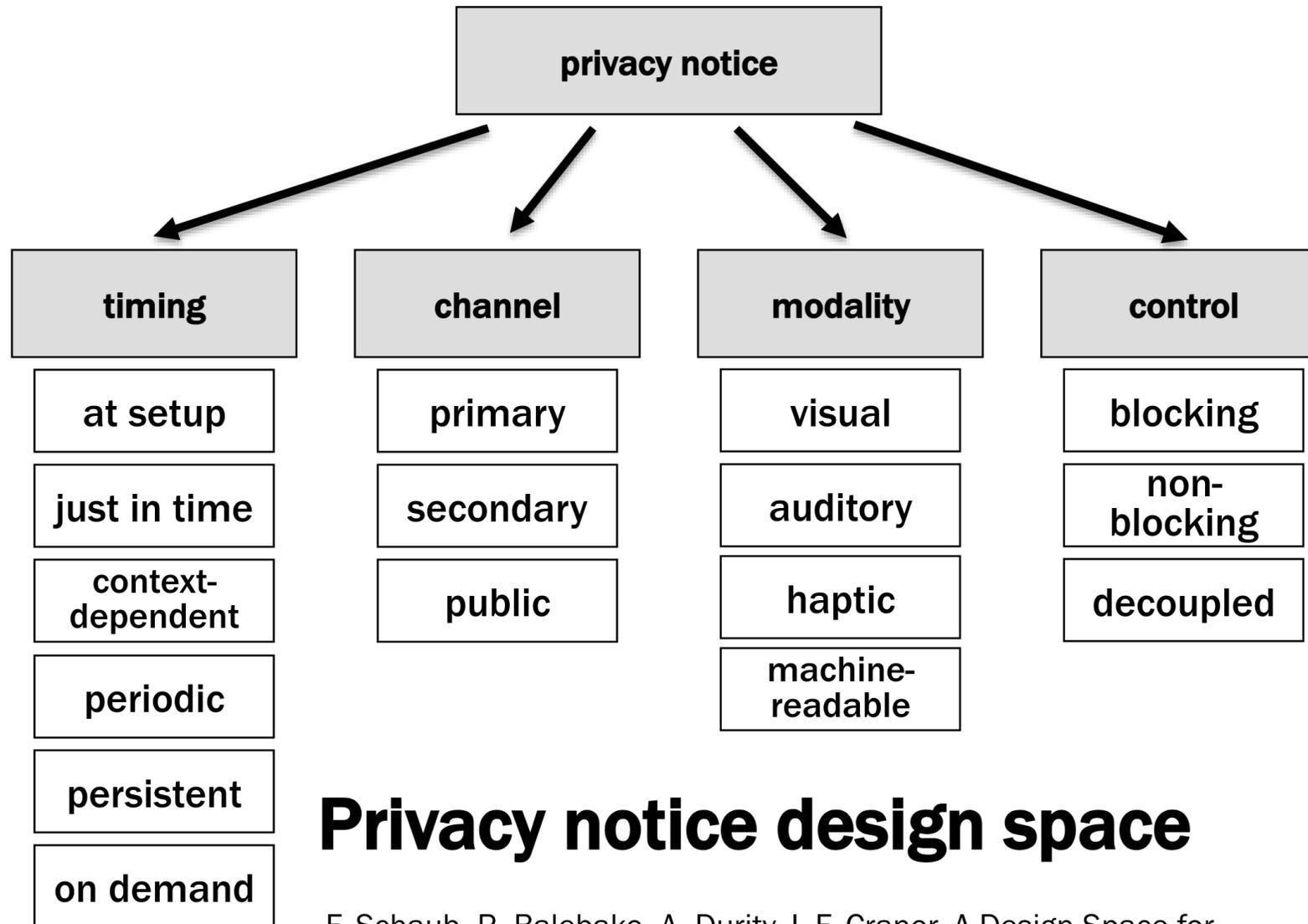
1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy

Proactive not Reactive; Preventative not Remedial



- I once went to a major security company's faculty outreach event
- The very first thing they did was show a "funny" video of a motorcycle rider stopping to help someone and getting both his motorcycle and phone stolen
- The starting message was simple: users are stupid
- That message was clearly how they thought about users internally and it impacted many of their choices

DESIGN OF CONSENT



Privacy notice design space

F. Schaub, R. Balebako, A. Durity, L.F. Cranor, A Design Space for Effective Privacy Notices, SOUPS'15

For each of the four notice and choice below, where do they sit in the design space?



"This call may be recorded for training purposes."



We use cookies on this site to enhance your user experience

Select 'Accept all' to agree and continue. You consent to our cookies if you continue to use this website.

Accept all



Amazon Alexa Smart Speaker

