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

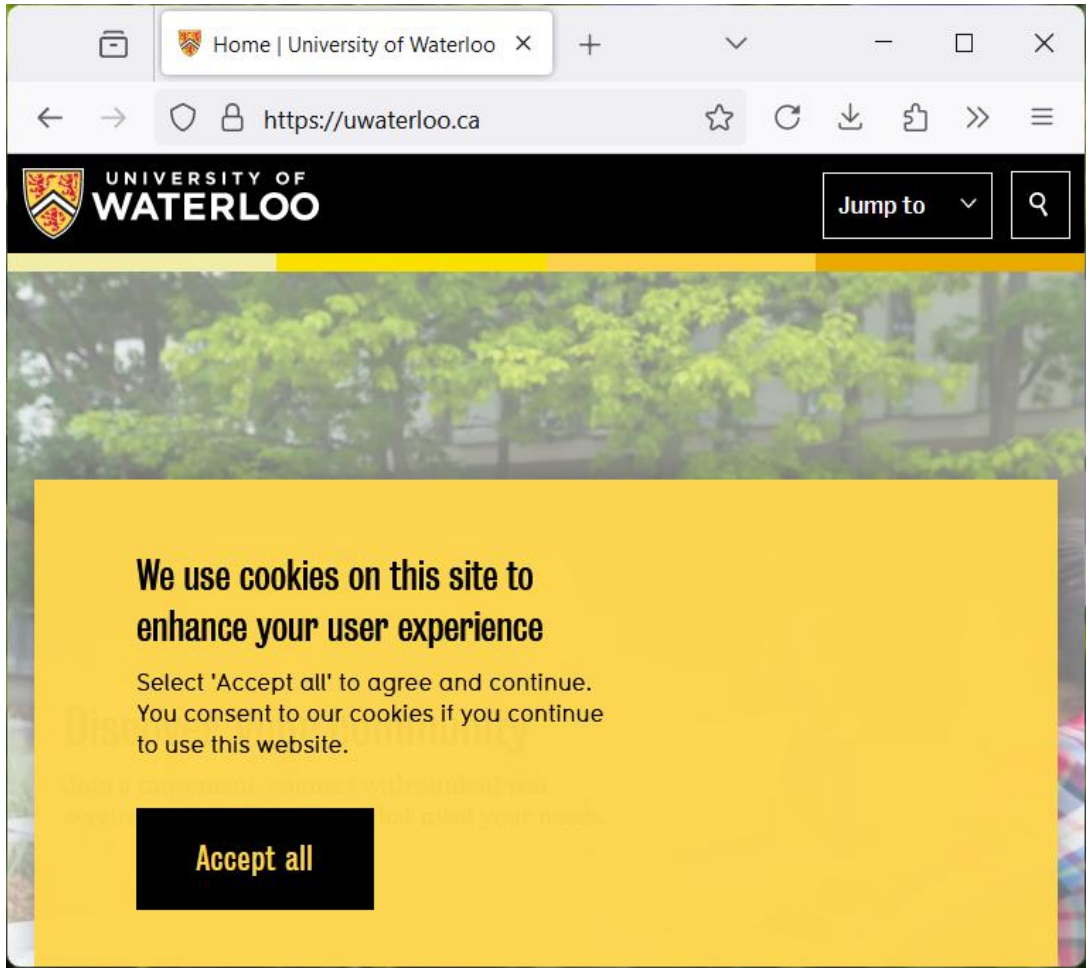
First, the news...

- 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

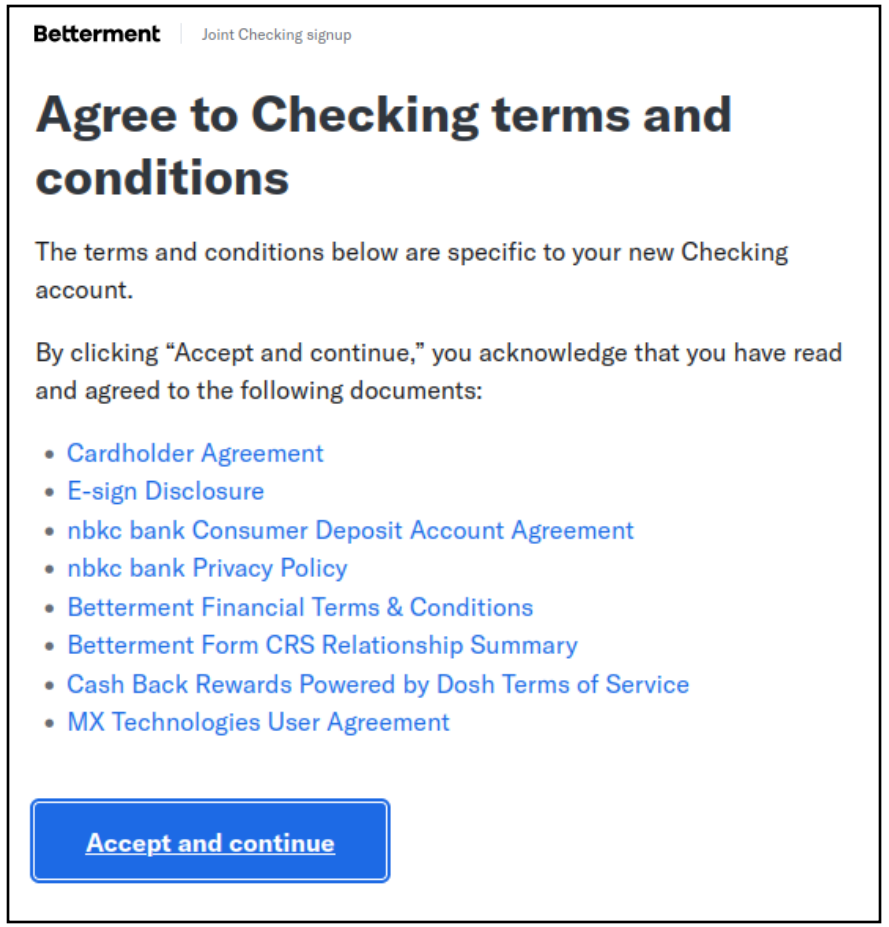
Notice and Choice: The idea

- 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



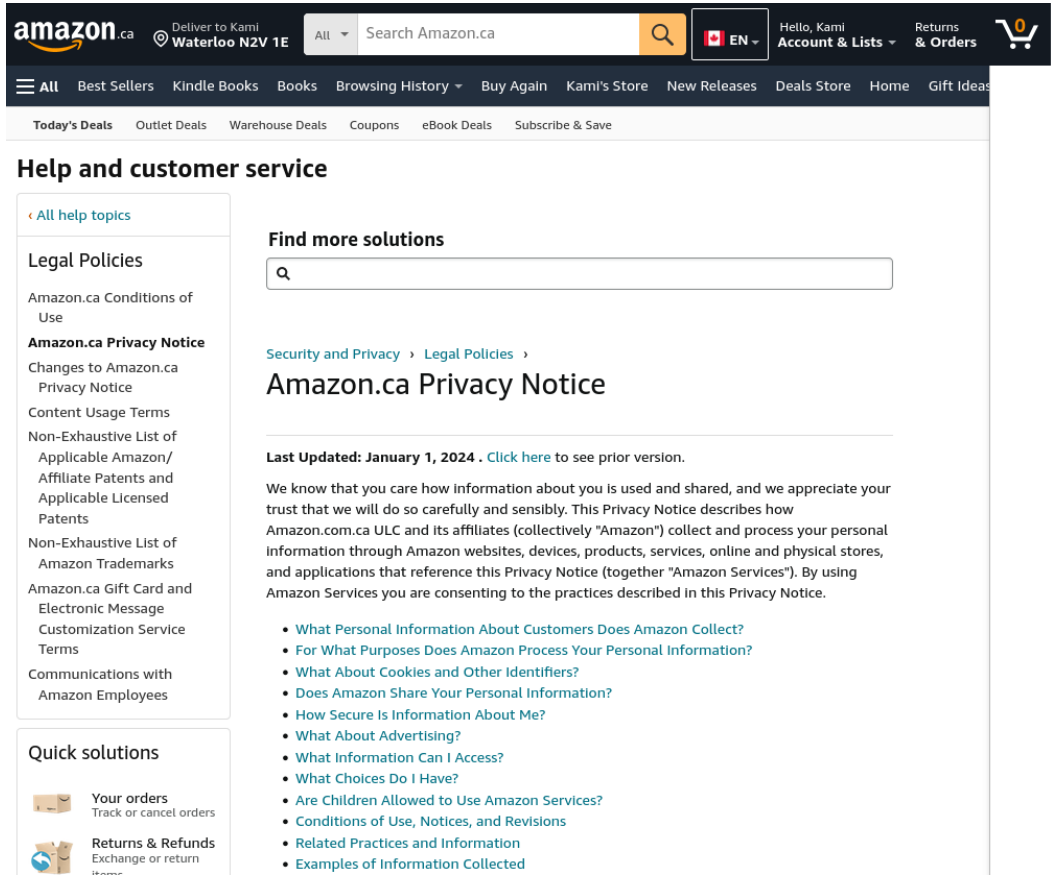
Notice is provided via privacy policies

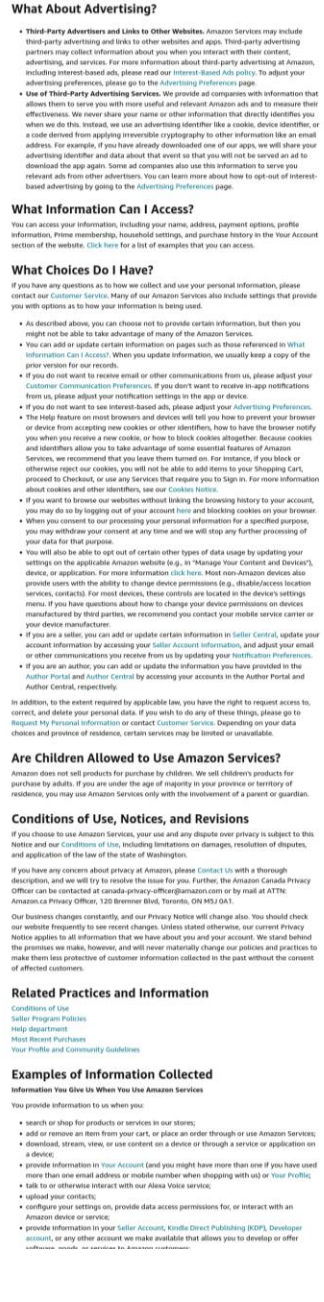
- FTC, OPC and similar regulatory bodies enforce privacy policy accuracy so consumers can trust organizations
- Organizations make such policies readily available to consumers

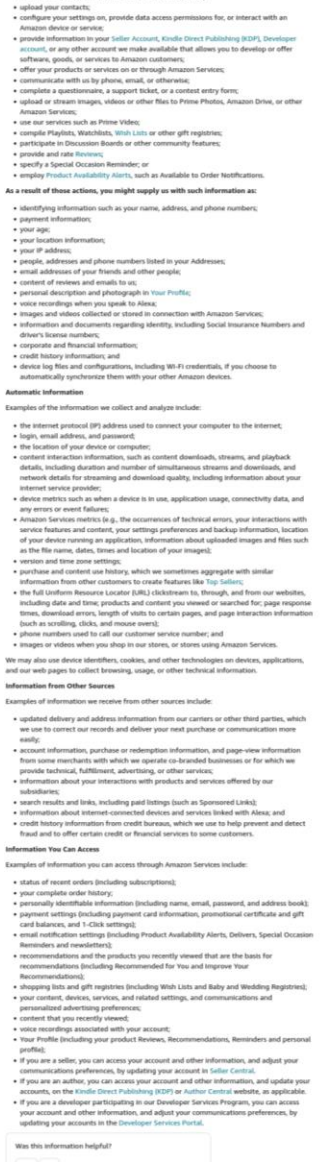


Amazon Privacy Policy

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

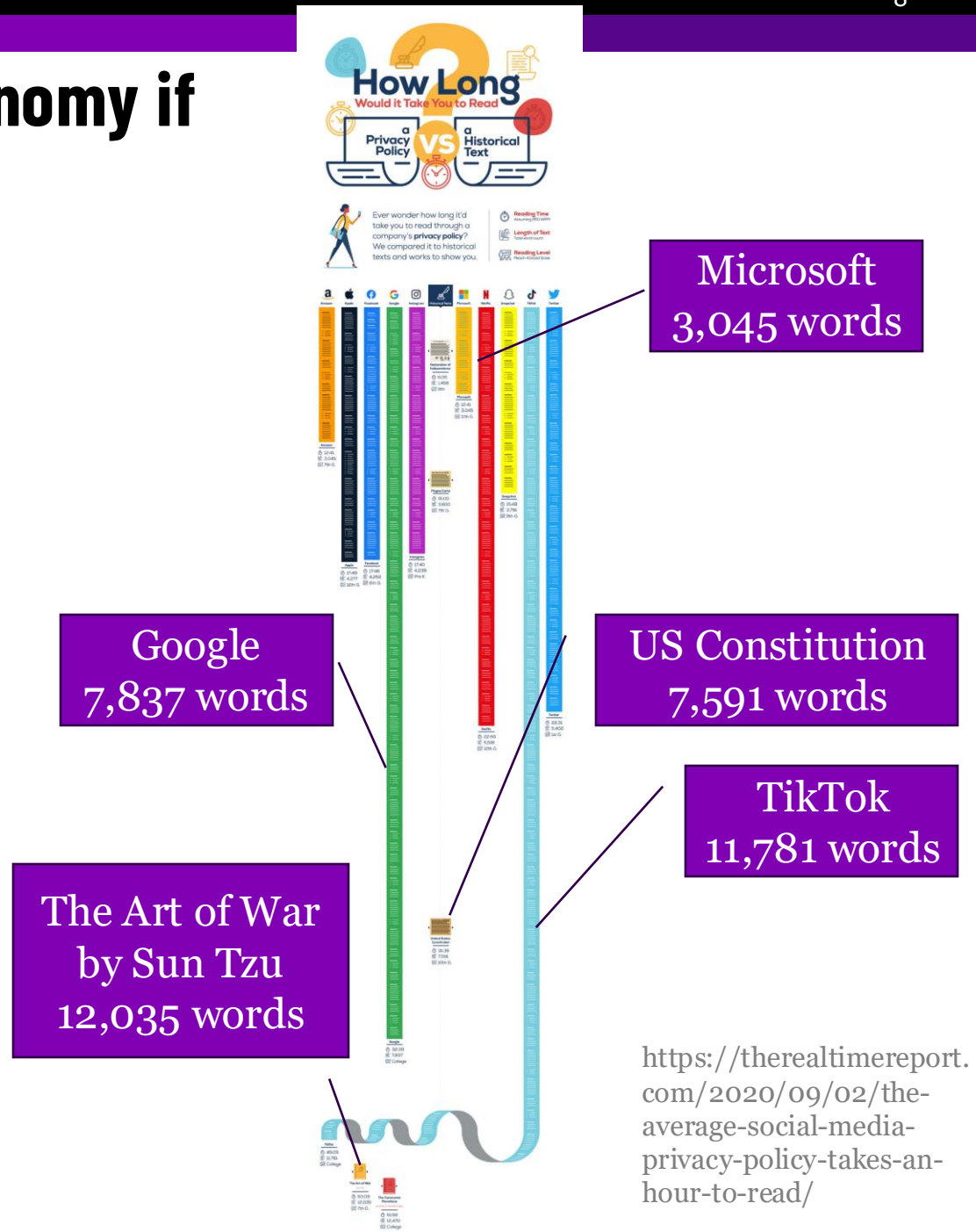






How much money would it cost the US economy if everyone read through privacy policies?

- Notice and choice is dependent on awareness of content of privacy policies
- People do not read all the privacy polices, 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)



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

Aleecia McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, 2008.

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 polices, 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

Aleecia McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, 2008.

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

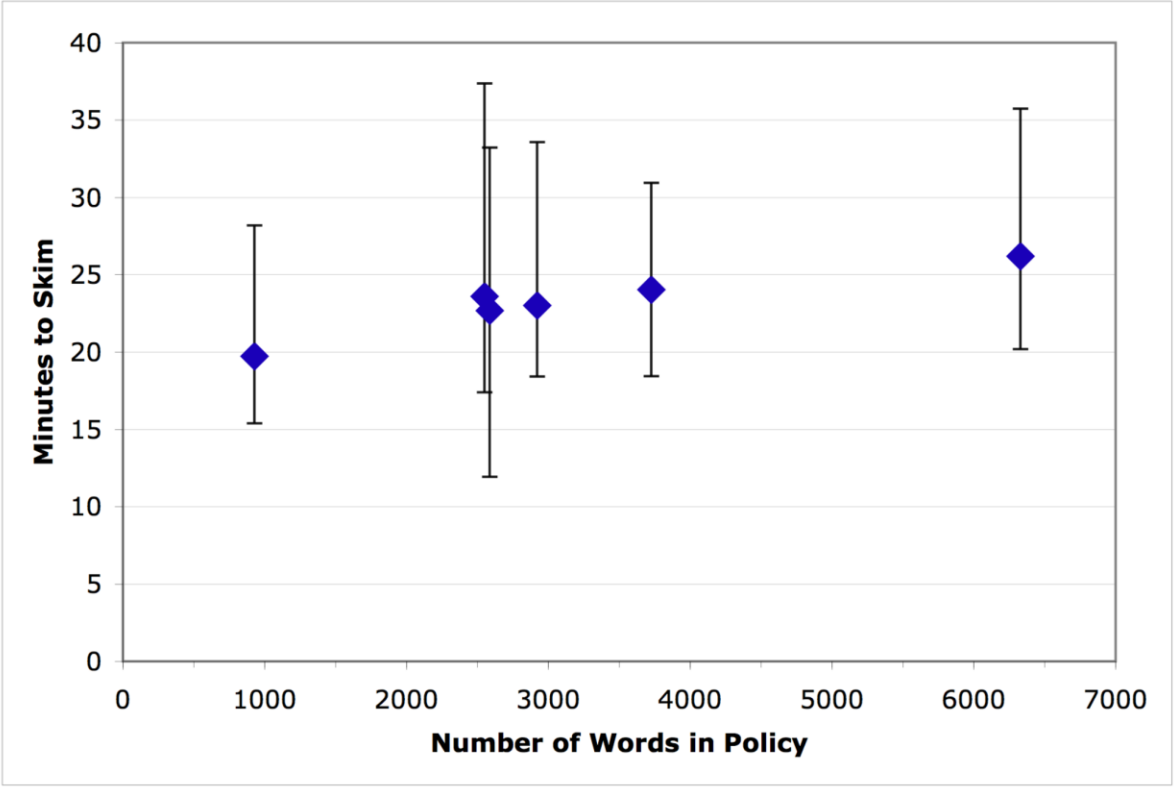
Lets look at how skimming time was determined.

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 very by policy length

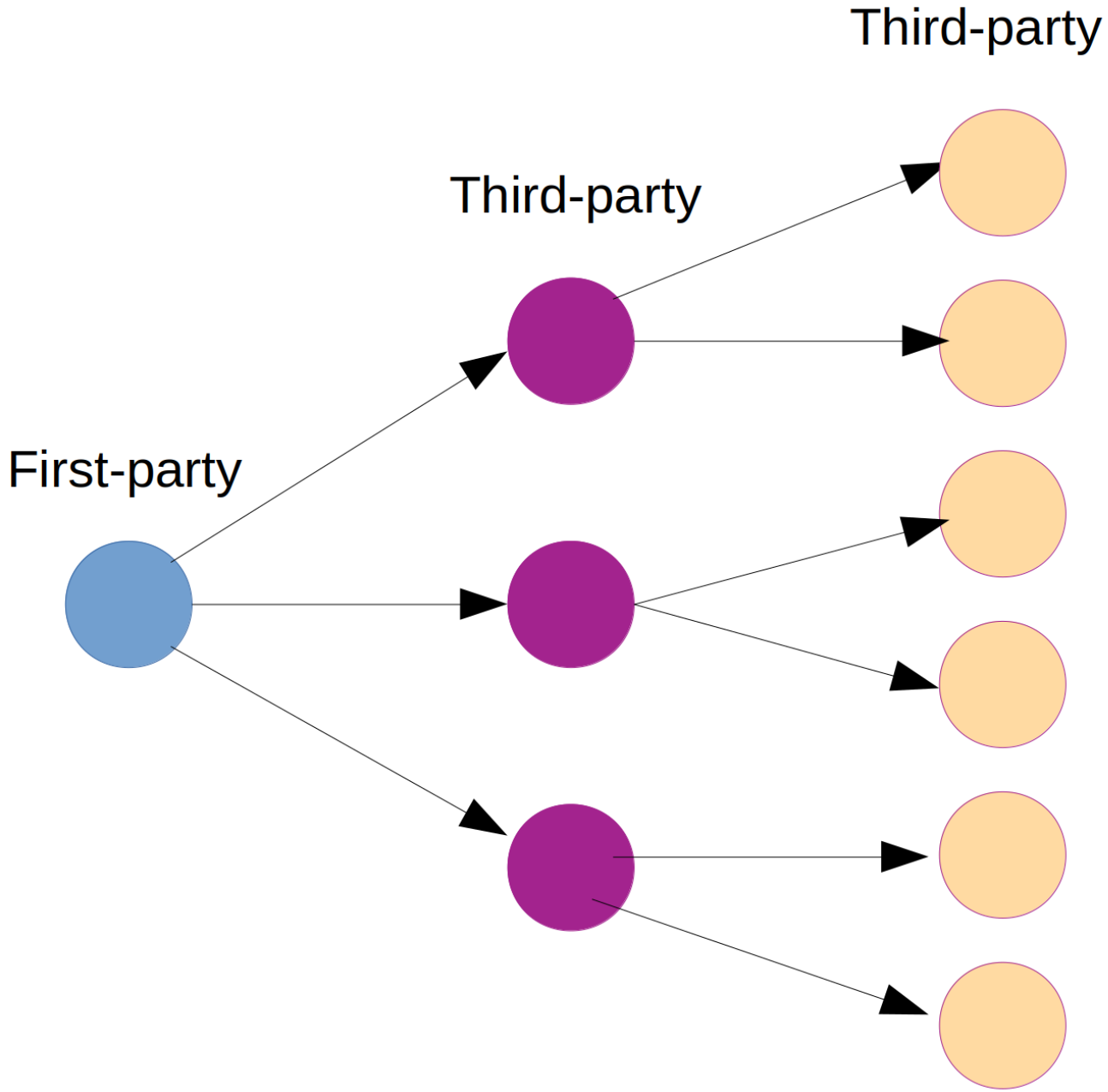
Aleecia McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, 2008.

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)

Aleecia McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, 2008.

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



How long to read all privacy policies, including 3rd party policies?

- Looked at top 100 US websites and the 3403 connections from those sites
- Only 75% of connecting sites had a privacy policy
  - 63.4% required a query to WHOIS to find the policy
- After deduplication: 79 first party policies, and 113 third-party
- 83 billion hours (USA) to read all
  - McDonald and Cranor found 67.1 billion hours for first party sites

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 loose all the value of privacy policies
- Idea: structured notices
- Banks in the US are required to provide privacy notices in a specific format

charles SCHWAB

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

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 • 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 • 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 • *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. • *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. • *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.sml.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.

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?	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

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

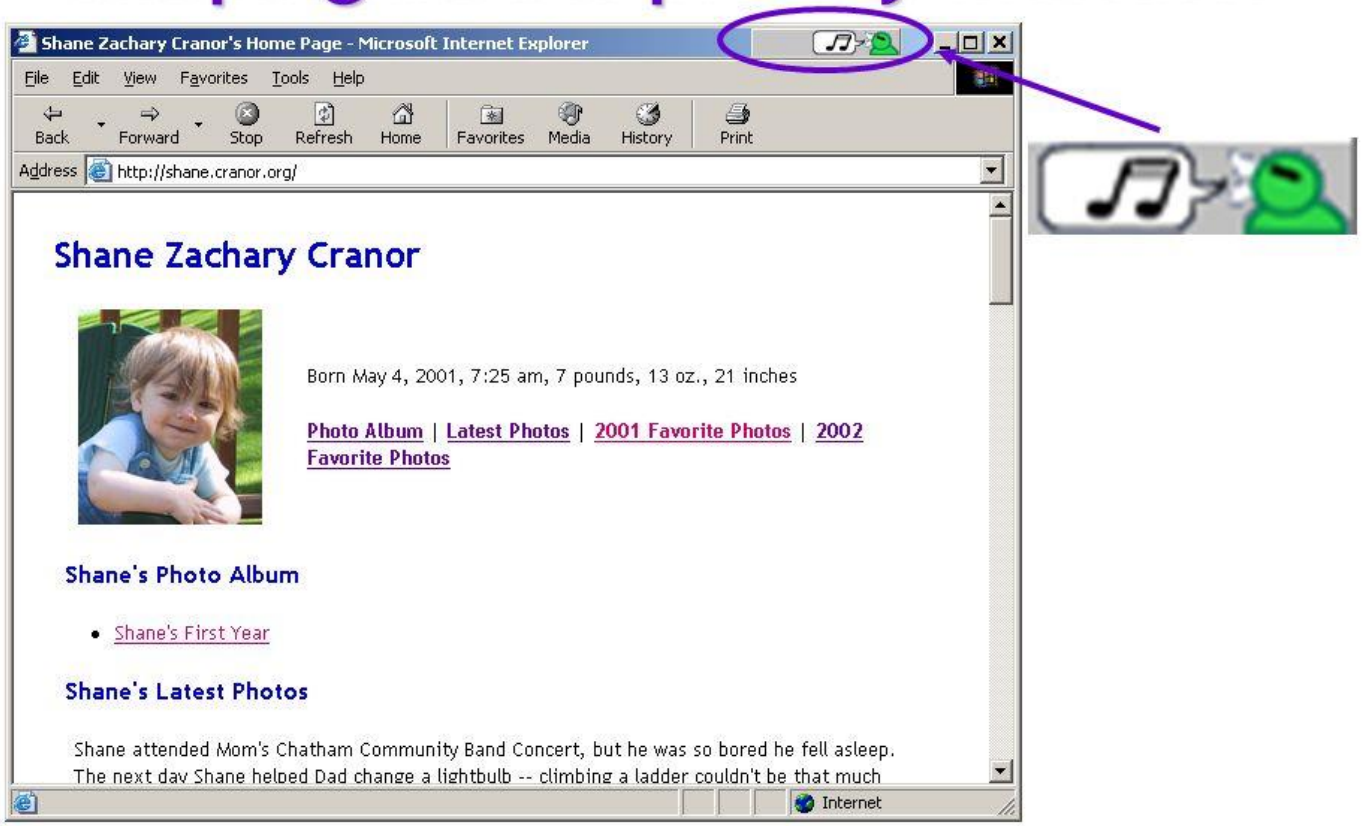
```
<?xml version="1.0"?>
<P3P xmlns="http://www.w3.org/2002/01/P3Pv1">
  <POLICY>
    <ENTITY>
      <DATA-GROUP>
        <DATA ref="#business.name">ExampleCorp</DATA>
        <DATA ref="#business.contact-info.online.email">privacy@example.com</DATA>
      </DATA-GROUP>
    </ENTITY>

    <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

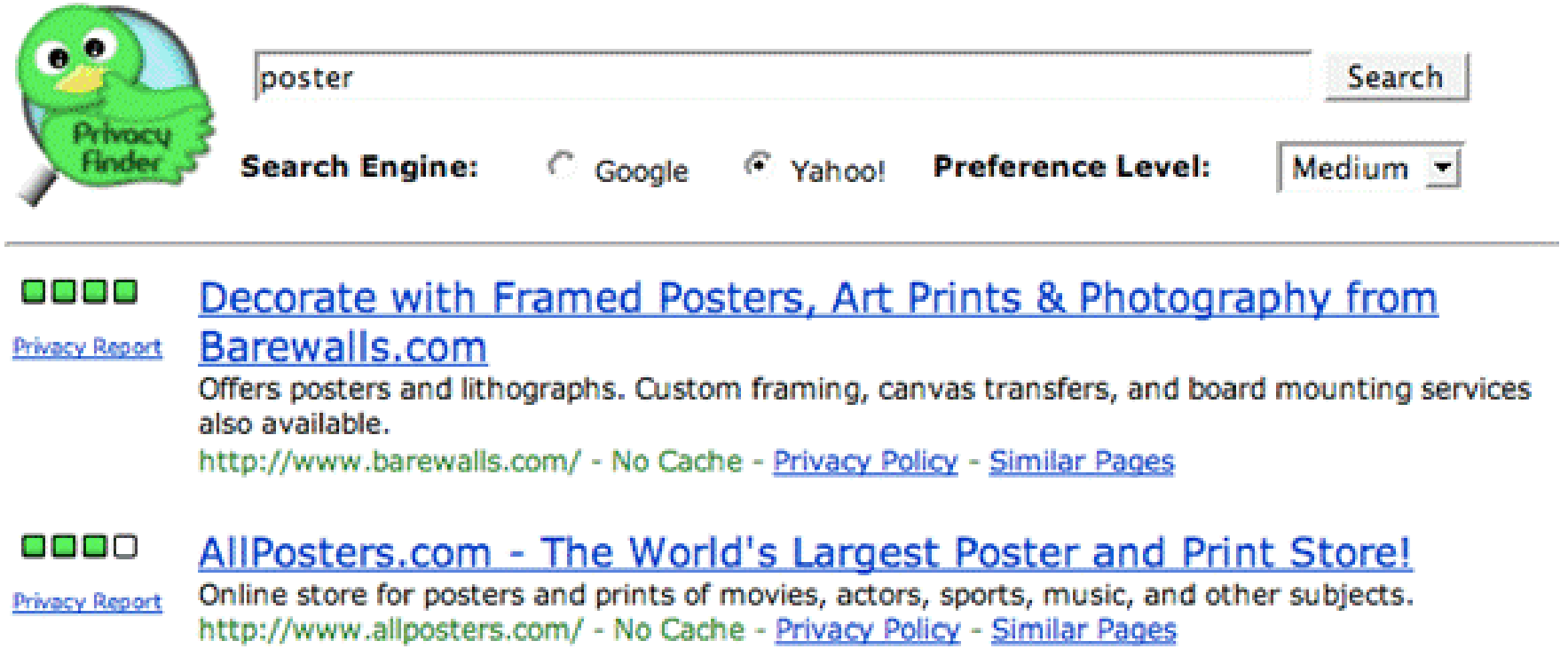
Chirping bird is privacy indicator



Lorrie Faith Cranor • http://lorrie.cranor.org/ 7

Privacy Finder and Privacy Bird

- Search engine that includes P3P information in the results



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

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 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

•••• [redacted]

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

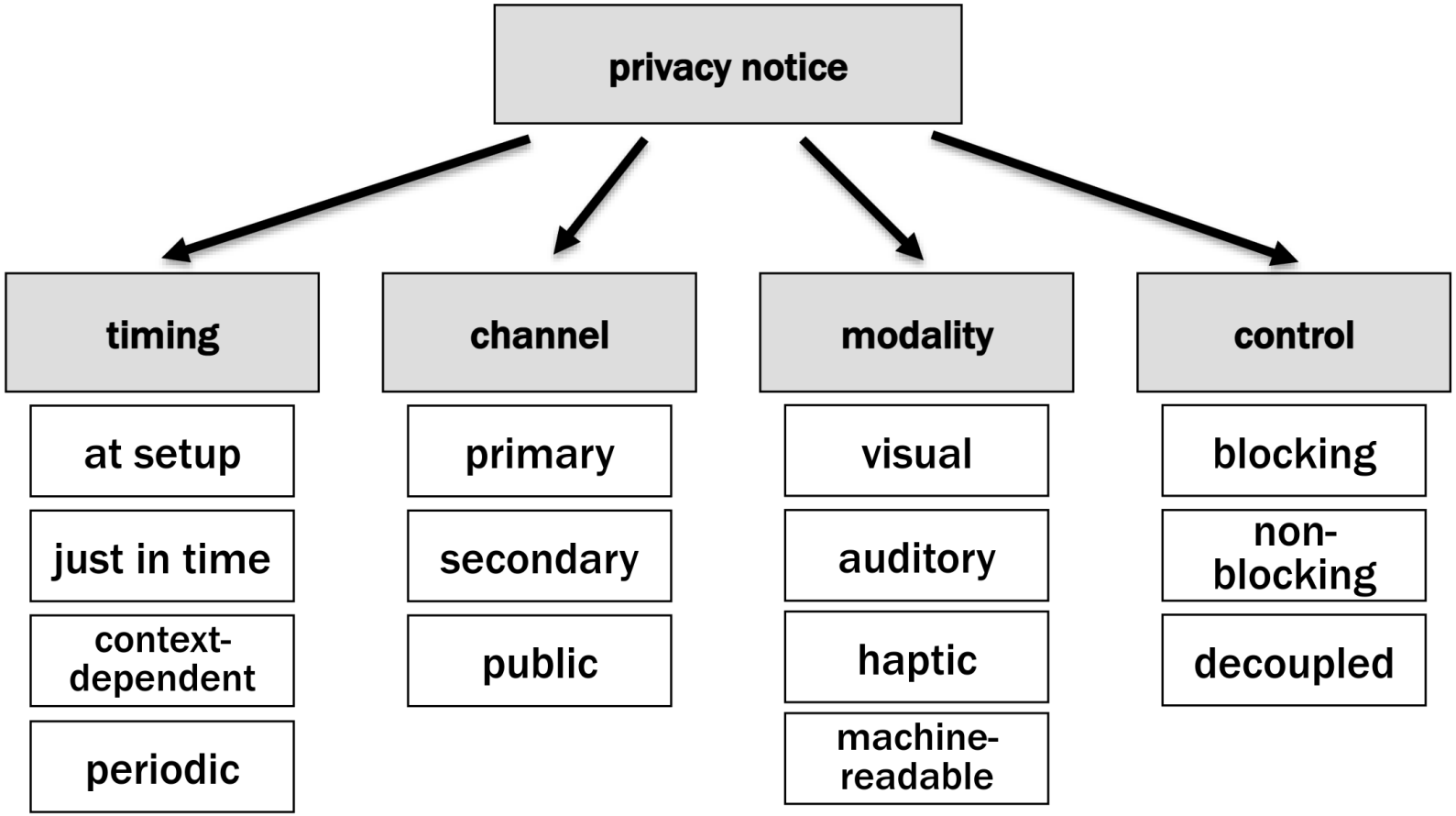
Privacy by Design

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 is 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

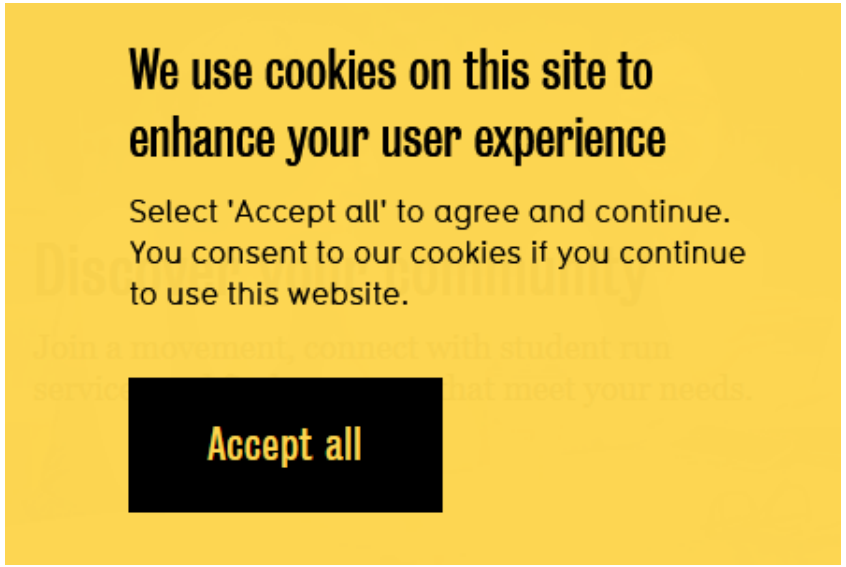


Privacy notice design space

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."



Amazon Alexa Smart Speaker