

# ECE750: Usable Security and Privacy

## **Privacy policies, notice, and choice**

Dr. Kami Vaniea  
Electrical and Computer Engineering  
[kami.vaniea@uwaterloo.ca](mailto: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

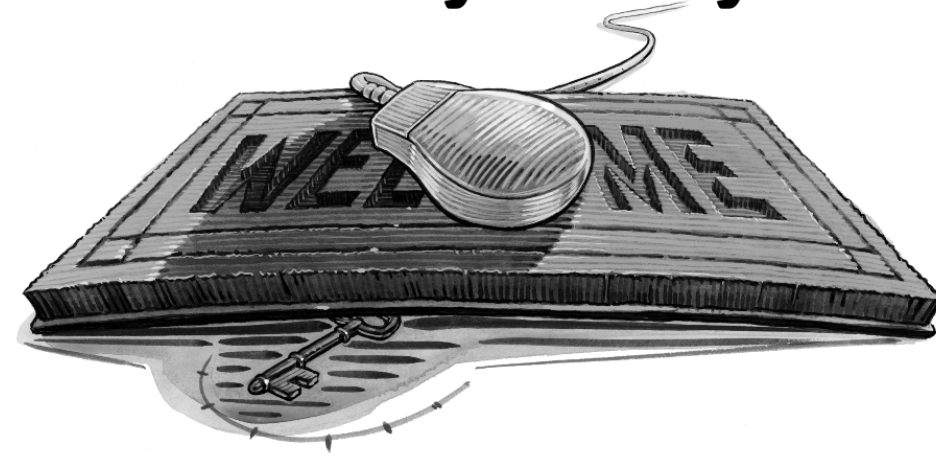
# TRUST AND E-COMMERCE

**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's a mistake. The unique economics of e-business make customer loyalty more important than ever."

ILLUSTRATION BY DOUGLAS JONES

# 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

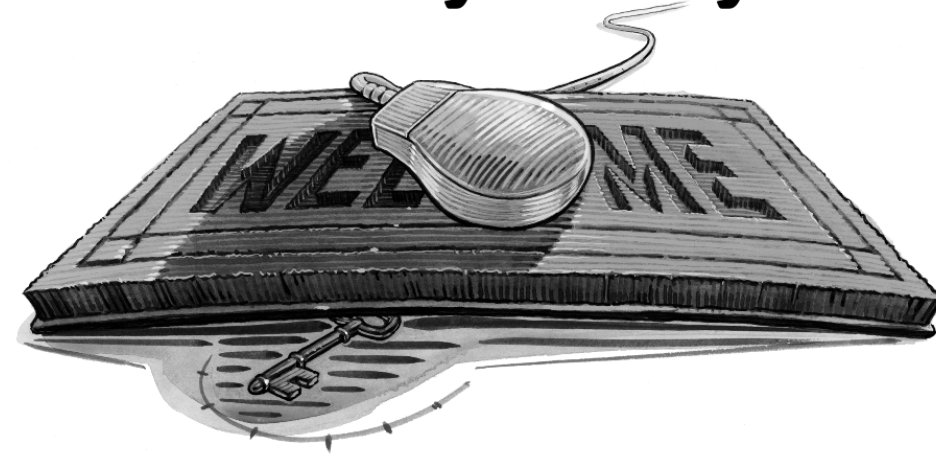
global marketplace? Loyalty must be on a fast track toward extinction, right?

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

"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."

ILLUSTRATION BY DOUGLAS JONES

# 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

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

Literature review

Interviewed  
8 e-commerce  
shoppers and  
5 non-shoppers

Built a theoretical  
model

Online experiment to  
test model using 53  
people

## Trustbuilders and Trustbusters

### *The Role of Trust Cues in Interfaces to e-Commerce Applications*

Jens Riegelsberger & M. Angela Sasse

*Hochschule der Künste Berlin & University College London*

**Abstract:** This paper investigates how interface design can help to overcome the proclaimed 'lack of trust' in e-commerce sites. Based on existing social science knowledge on trust, and our own exploratory study using Grounded Theory methods, we developed a model of consumer decision making in on-line shopping. Due to the separation in space and time when engaging in e-commerce, there is an *increased need for trust, rather than the oft-proclaimed lack of trust*. Based on this model we then review design guidelines through empirical tests. We focus on approaches that aim to increase trust by increasing the *social presence* of an interface. We identified cues in the user interface that help to build trust to some extent (*trustbuilders*), and some cues that have a great potential for destroying trust (*trustbusters*).

## 1. INTRODUCTION

Consider shopping in the real world: When a customer enters a shop for the first time, she sees the interior, goods and the sales staff. The customer may not conduct any risk evaluation at all, because shopping is a habit she does not perceive as risky. But the visual cues allow her to evaluate the shop's professionalism, competence and trustworthiness via a comparison with other shops. The situation is different for shopping on the Internet: Most people do not shop habitually on the Internet and do not understand the underlying technology, and the risks are numerous. It is thus not surprising that one of the leading advertisers on the Internet is TRUSTe [15], an organisation that assigns seals to e-commerce enterprises that it considers



# Risks people perceive in e-commerce

## 1. Risks that stem from the Internet include:

- a. Whether credit card data gets intercepted **Security**
- b. Whether the data is transmitted correctly **Security / Networking**
- c. Their own interaction with the system- i.e. whether they use it correctly **HCI**

## 2. Risks that are related to the physical absence of the online-retailer are:

- a. Whether the personal details they supply will be passed on to other parties **Privacy**
- b. Whether the online-vendor will actually deliver the products or services **Legal**

# To buy, or not to buy?

1. Retailer's performance as evaluated by the e-shopper
2. Perceived benefit (e.g. how much shopper can save)
3. Personal disposition (e.g. how much risk can they bear)

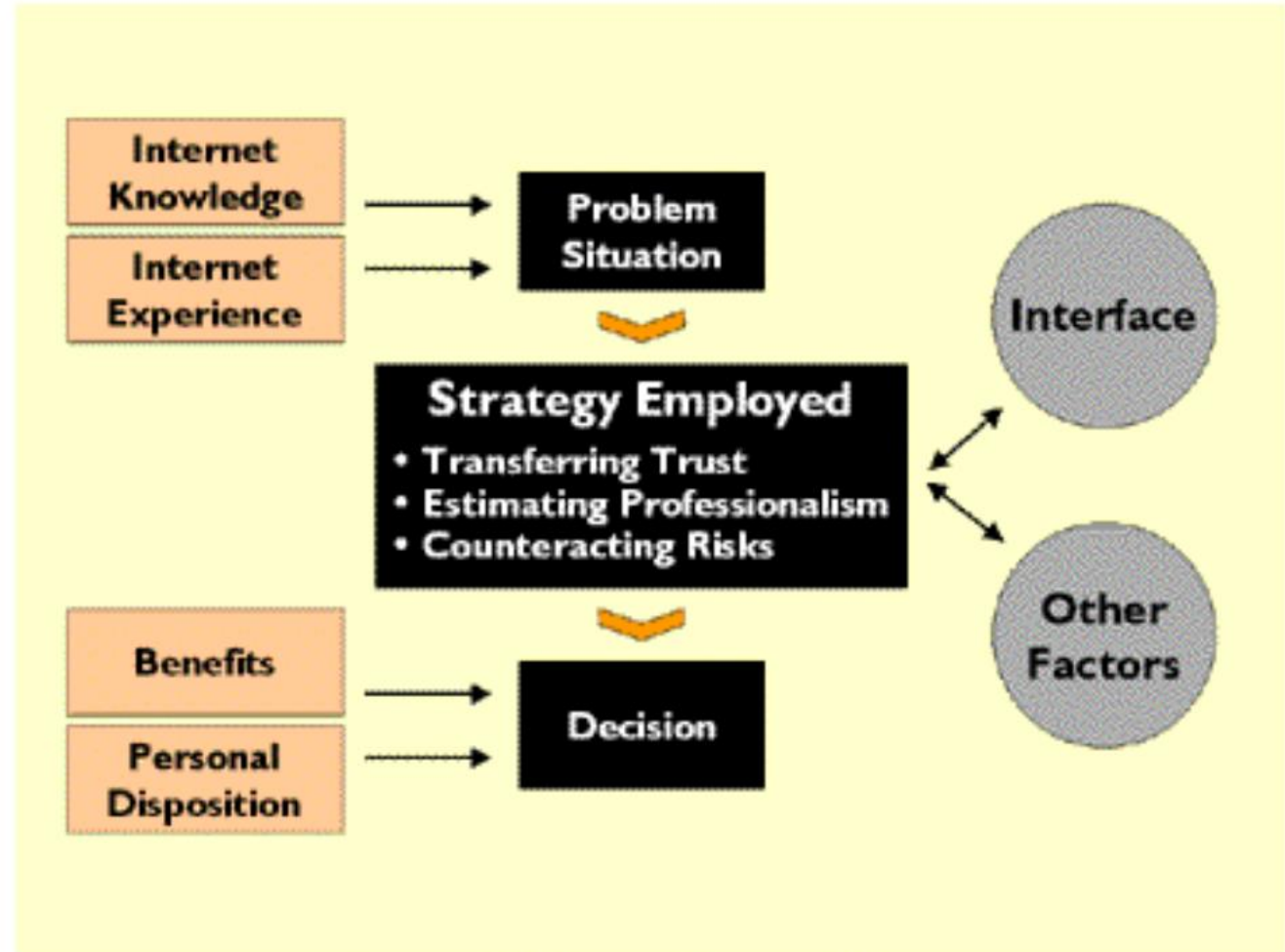


Figure 1. E-Shopper Decision Making

# Interviews found key issues to be:

- Internet knowledge
  - Are businesses even able to protect customers?
  - Low knowledge -> harder to judge accuracy of claims
- Internet experience
  - Will I make errors and order the wrong thing?
  - Few conventions – the “correct” approach on one page is different on another
- Separation in Space & Time
  - Give money, wait, get item

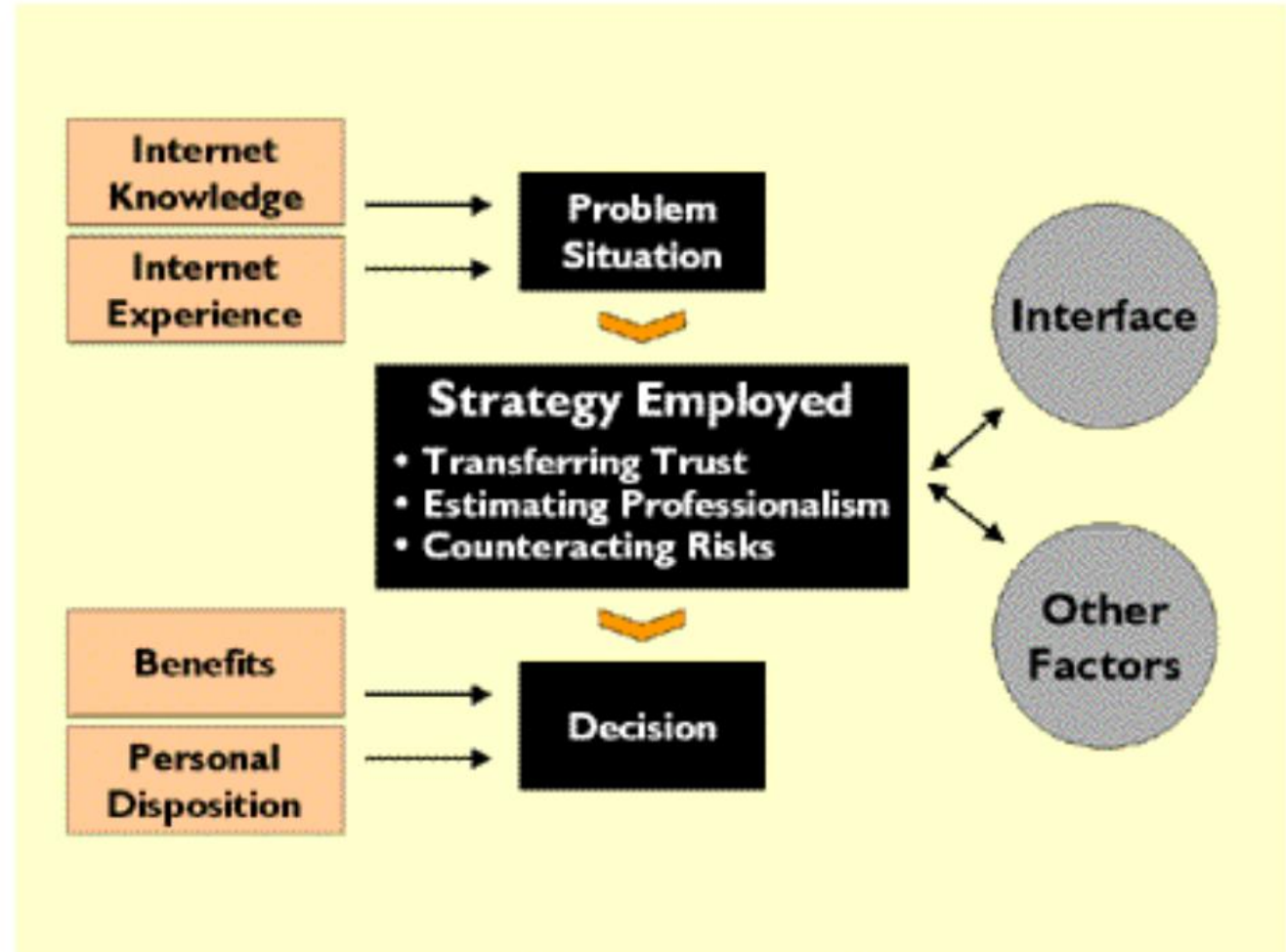


Figure 1. E-Shopper Decision Making

# A framework for trust in e-commerce

- Outcome of all the earlier work combined
- Proposed a framework of the different aspects that impact trust in online websites

## The mechanics of trust: A framework for research and design

Jens Riegelsberger\*, M. Angela Sasse, John D. McCarthy

*Department of Computer Science, University College London, Gower Street, London WC1E 6BT, UK*

Received 12 August 2004; received in revised form 18 December 2004; accepted 5 January 2005

Communicated by S. Wiedenbeck

### Abstract

With an increasing number of technologies supporting transactions over distance and replacing traditional forms of interaction, designing for trust in mediated interactions has become a key concern for researchers in human computer interaction (HCI). While much of this research focuses on increasing users' trust, we present a framework that shifts the perspective towards factors that support trustworthy behavior. In a second step, we analyze how the presence of these factors can be signalled. We argue that it is essential to take a systemic perspective for enabling well-placed trust and trustworthy behavior in the long term. For our analysis we draw on relevant research from sociology, economics, and psychology, as well as HCI. We identify *contextual properties* (motivation based on *temporal*, *social*, and *institutional embeddedness*) and the *actor's intrinsic properties* (*ability*, and motivation based on *internalized norms* and *benevolence*) that form the basis of trustworthy behavior. Our analysis provides a frame of reference for the design of studies on trust in technology-mediated interactions, as well as a guide for identifying trust requirements in design processes. We demonstrate the application of the framework in three scenarios: call centre interactions, B2C e-commerce, and voice-enabled on-line gaming.

© 2005 Elsevier Ltd. All rights reserved.

**Keywords:** Trust; Social capital; Dis-embedding; Interpersonal cues; Human computer interaction; Computer mediated communication; Computer supported collaborative work; Decision-making; Game theory; E-commerce

# Separation in time and space

- Physical retail is immediate – customer gives money and gets item right there
- Online retail happens
  - at a great distance, sometimes even international
  - with a time delay, the item will not arrive for a while after payment
- Time and space separation impacts trust

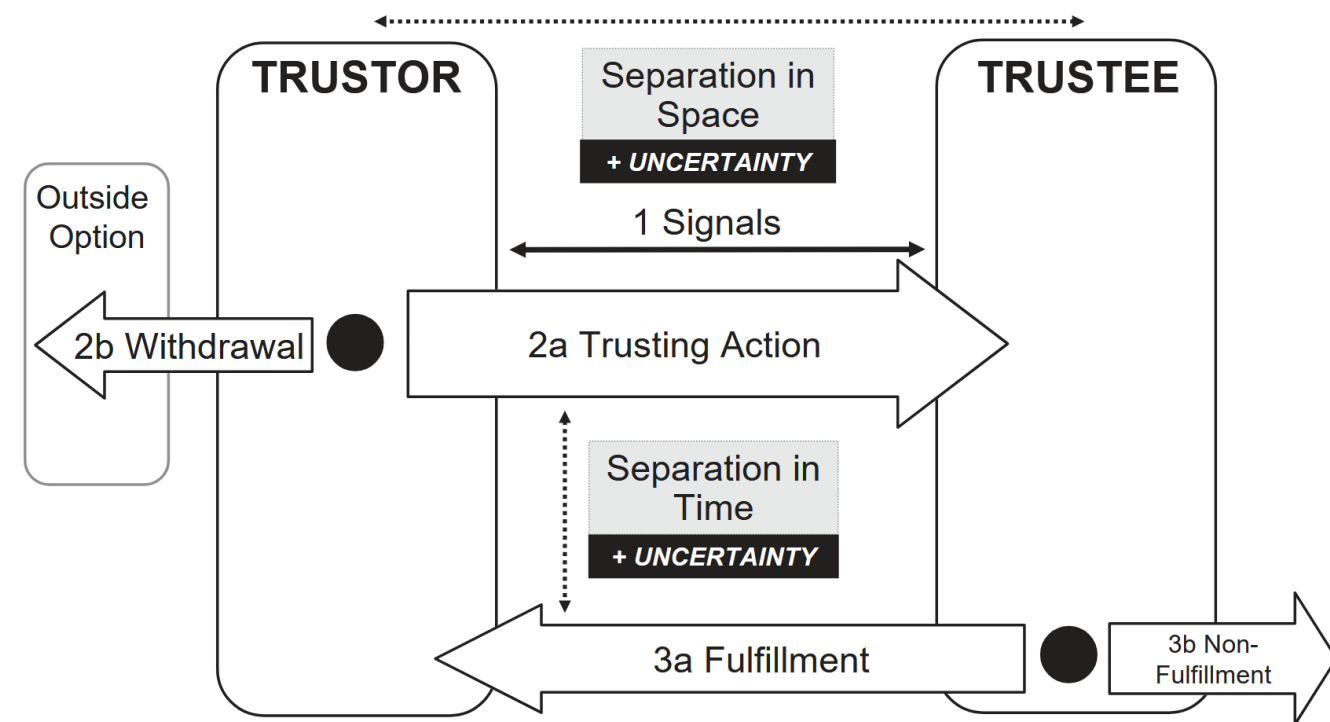


Fig. 2. Effects of separation in time and space.

# Trust factors

- Temporal – time, how long must the trustor trust the trustee? (e.g. shipping speed)
- Social – what other people think (e.g. reviews)
- Institutional – laws, regulations, what happens if the item never arrives?
- Ability – Is the company able to do what they said? (e.g. tariffs, egg shortage)
- Motivation
  - Internalized norms – principles the company adheres to because they value them (e.g. “do no evil” from Google)
  - Benevolence – what is the companies' goals and motivations (e.g. Apple wants to sell me another phone)

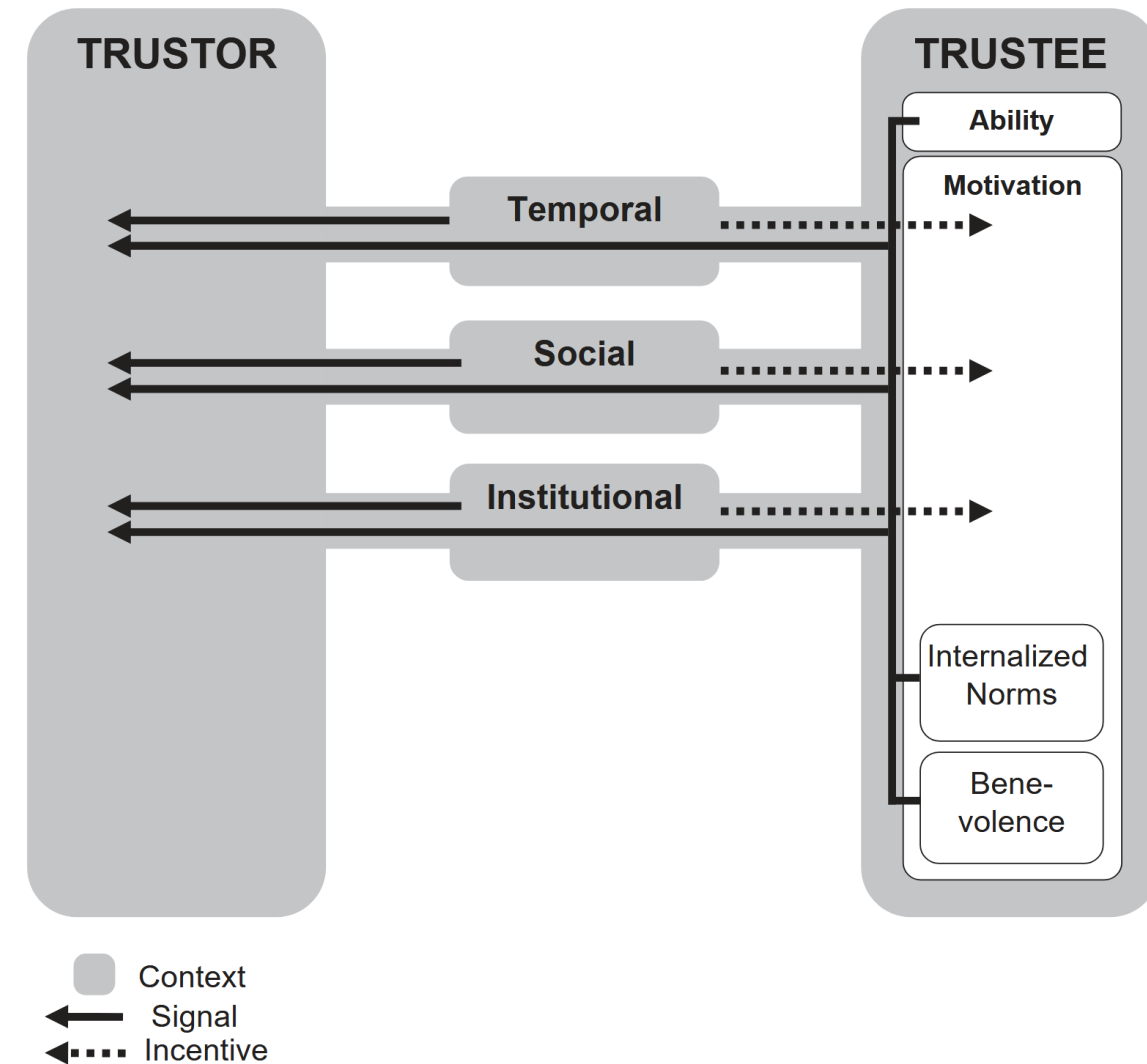


Fig. 7. The complete framework.

# 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
  - Issue of self-assertion: “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 Comision (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.**

# Trust factors

- FTC is trying to build trust by providing a legal framework to protect consumers
- Helps answer the question: “what happens if my package never arrives?”
- Ensures that information the company provides is legally enforceable

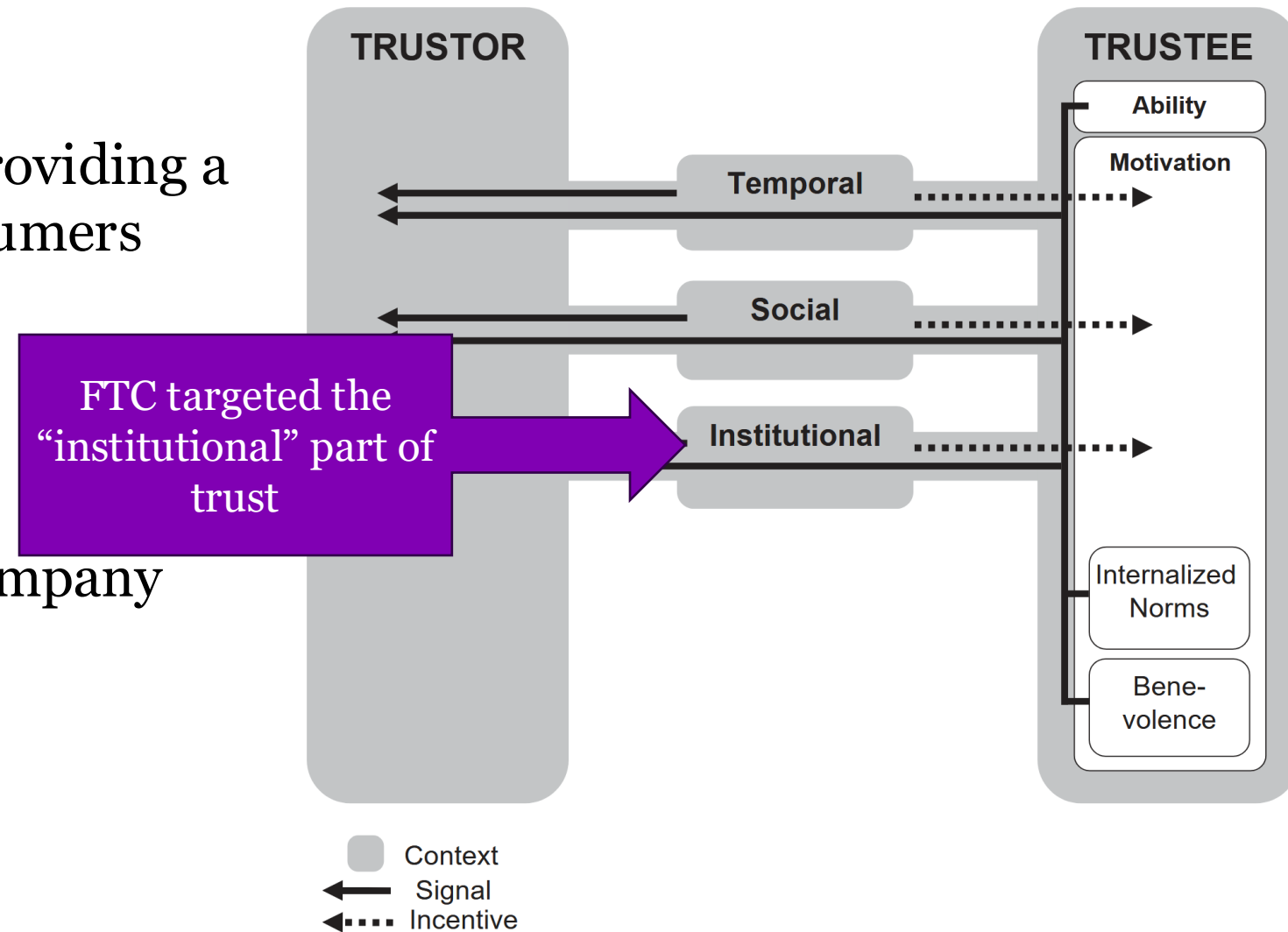


Fig. 7. The complete framework.

# T-Mobile “lifetime” plan

- T-Mobile offered a “lifetime” plan that claimed it would never change price
- Then they tried to change the price...
- Lawsuit
  - Their marketing material is heavily shown in lawsuit
  - There was an FAQ about how they might maybe change the price
  - Is it reasonable to expect the consumer to read FAQ to find this information, or was T-Mobile being deceptive?

## Lawsuit: T-Mobile must pay for breaking lifetime price guarantee

Class action filed over price hikes on plans with Un-contract price guarantee.

JON BRODWIN · JUL 24, 2024 2:36 PM · 105



→ John Legere, then-CEO of T-Mobile, at an event on March 26, 2013, in New York City. Credit: Getty Images | John Moore

Angry T-Mobile customers have filed a class action lawsuit over the carrier's decision to raise prices on plans that were advertised as having a lifetime price guarantee.

"Based upon T-Mobile's representations that the rates offered with respect to certain plans were guaranteed to last for life or as long as the customer wanted to remain with that plan, each Plaintiff and the Class Members agreed to these plans for wireless cellphone service from T-Mobile," said the complaint filed in US District Court for the District of New Jersey. "However, in May 2024, T-Mobile unilaterally did away with these legacy phone plans and switched Plaintiffs and the Class to more expensive plans without their consent."

The complaint, filed on July 12, has four named plaintiffs who live in New Jersey, Georgia, Nevada, and Pennsylvania. They are seeking to represent a class of all US residents "who entered into a T-Mobile One Plan, Simple Choice plan, Magenta, Magenta Max, Magenta 55+, Magenta Amplified or Magenta Military Plan with T-Mobile which included a promised lifetime price guarantee but had their price increased without their consent and in violation of the promises made by T-Mobile and relied upon by Plaintiffs and the proposed

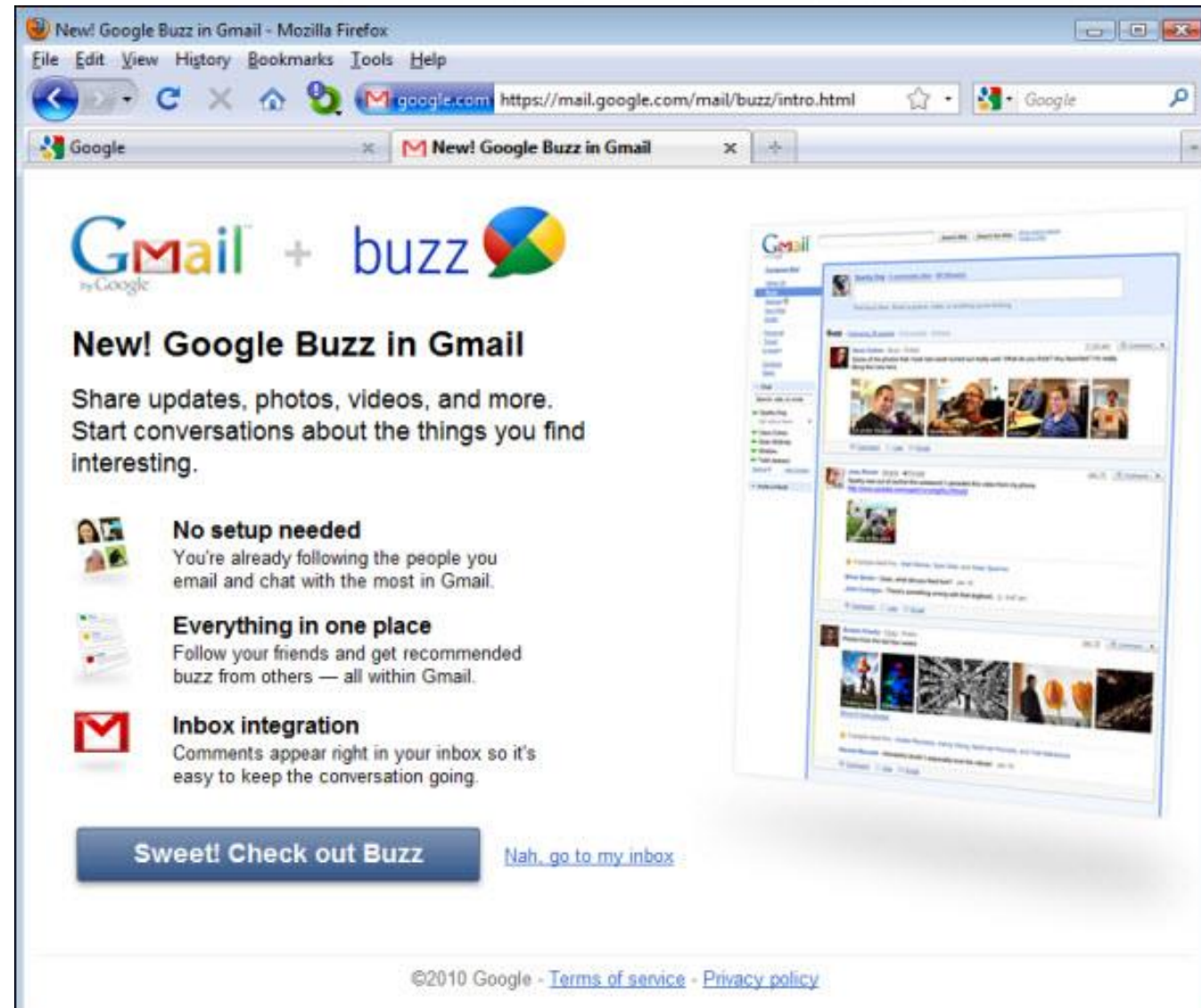
# FTC vs Google Buzz

- 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





# Think-pair-share

- Snapchat marketing material
  - “Snap an ugly selfy or a video, add a caption, and send it to a friend (or maybe a few). They’ll receive it, laugh, and then the snap disappears.”
- Snapchat privacy policy:
  - “Although we attempt to delete image data as soon as possible after the message is received and opened by the recipient . . . we cannot guarantee that the message contents will be deleted in every case.”
  - “users may take a picture of the message contents with another imaging device or capture a screenshot of the message contents on the device screen.”



The screenshot shows the FTC website header with the logo and navigation links. The main content area displays a press release titled "Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False". Below the title is a sub-headline: "Snapchat Also Transmitted Users' Location and Collected Their Address Books Without Notice Or Consent". There are social media sharing icons for Facebook, Twitter, and LinkedIn. A "FOR RELEASE" banner is visible, along with the date "May 8, 2014". The "TAGS" section lists: "deceptive/misleading conduct | Technology | Bureau of Consumer Protection | Office of International Affairs | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security". The main text of the press release states that Snapchat, the developer of a popular mobile messaging app, has agreed to settle FTC charges that it deceived consumers with promises about the disappearing nature of messages sent through the service. The FTC case also alleged that the company deceived consumers over the amount of personal data it collected and the security measures taken to protect that data from misuse and unauthorized disclosure. In fact, the case alleges, Snapchat's failure to secure its Find Friends feature resulted in a security breach that enabled attackers to compile a database of 4.6 million Snapchat usernames and phone numbers. A quote from FTC Chairwoman Edith Ramirez is also present: "If a company markets privacy and security as key selling points in pitching its service to consumers, it is critical that it keep those promises," said FTC Chairwoman Edith Ramirez. "Any company that makes misrepresentations to consumers about its privacy and security practices risks FTC action."

**FEDERAL TRADE COMMISSION**  
PROTECTING AMERICA'S CONSUMERS

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE

Home » News & Events » Press Releases » Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False

## Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False

**Snapchat Also Transmitted Users' Location and Collected Their Address Books Without Notice Or Consent**

SHARE THIS PAGE

**FOR RELEASE**

May 8, 2014

**TAGS:** [deceptive/misleading conduct](#) | [Technology](#) | [Bureau of Consumer Protection](#) | [Office of International Affairs](#) | [Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#)

Snapchat, the developer of a popular mobile messaging app, has agreed to [settle Federal Trade Commission charges that it deceived consumers](#) with promises about the disappearing nature of messages sent through the service. The FTC case also alleged that the company deceived consumers over the amount of personal data it collected and the security measures taken to protect that data from misuse and unauthorized disclosure. In fact, the case alleges, Snapchat's failure to secure its Find Friends feature resulted in a security breach that enabled attackers to compile a database of 4.6 million Snapchat usernames and phone numbers.

According to the FTC's complaint, Snapchat made multiple misrepresentations to consumers about its product that stood in stark contrast to how the app actually worked.

"If a company markets privacy and security as key selling points in pitching its service to consumers, it is critical that it keep those promises," said FTC Chairwoman Edith Ramirez. "Any company that makes misrepresentations to consumers about its privacy and security practices risks FTC action."

[Home](#)[Your data matters](#)[For organisations](#)[Make a complaint](#)[Action we've taken](#)[About the ICO](#)

## Properties raided in Brighton and Birmingham

Businesses suspected of making millions of nuisance calls.

### Speech: Elizabeth Denham at the ICIC

11 March 2019

### Blog: Adtech fact finding forum shows consensus on need for change

7th March 2019

### Blog: The right of access to patient data needn't be a headache

7 March 2019

[More news and blogs](#) →

## Take action

[Pay fee, renew fee or register a DPO](#) →

[Report a breach](#) →

[Make a complaint](#) →

[Meet the Commissioner](#)



## → Your data matters

Practical information about your data protection and information rights



Spam emails



Does an organisation need my consent?

## → For organisations

Guidance and resources for public bodies, private sector organisations and sole traders

## → Guide to Data Protection

## → General Data Protection Regulation (GDPR)

# 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 dark header with the Canadian coat of arms on the left, and the office's name in English and French on the right. Below this, a navigation bar contains links for 'For individuals', 'For businesses', 'For federal institutions', and 'Report a concern'. The main content area features the office's name in large purple text, followed by the subtitle 'Protecting and promoting privacy rights'. A paragraph explains the office's role in providing advice and enforcing federal privacy laws. A link to 'our Office' is provided. Below the text is a large image of a young girl looking at a smartphone, with three orange speech bubbles overlaid containing a checkmark, an exclamation mark, and a question mark. At the bottom, a purple banner contains the text 'Call for comments' and 'Privacy and age assurance - Exploratory consultation'.

Office of the Privacy Commissioner of Canada  
Commissariat à la protection de la vie privée du Canada

For individuals For businesses For federal institutions Report a concern

## 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: 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

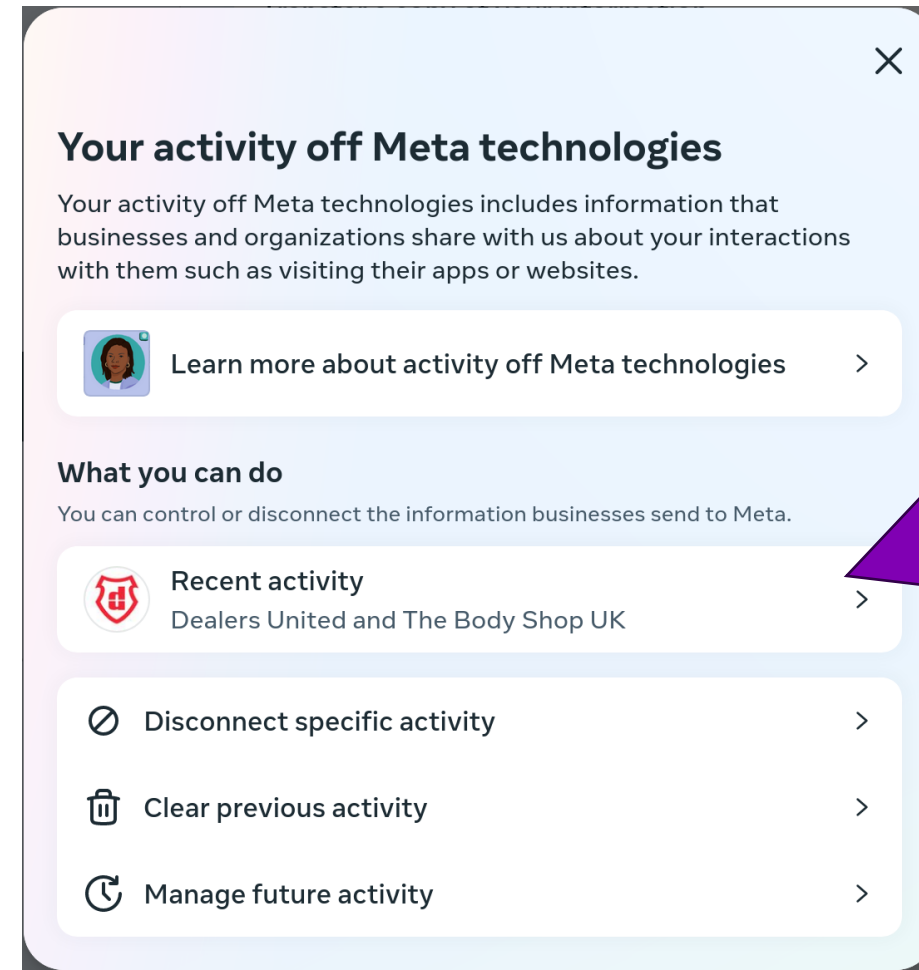
The Complainant alleged that Home Depot of Canada Inc. ("Home Depot") disclosed his personal information to Facebook (now Meta Platforms, Inc., "Meta") without his knowledge and consent. Specifically, the complainant claimed that while he was deleting his Facebook account, he learned that Meta had a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



My recent  
car  
purchase  
attempt


# 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.

Cancel

Confirm

# 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 has a right to know how their data will be used.

**Purpose limitation** - data must be collected with a purpose and only used for it or compatible purposes.

**Data minimisation** - 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”.

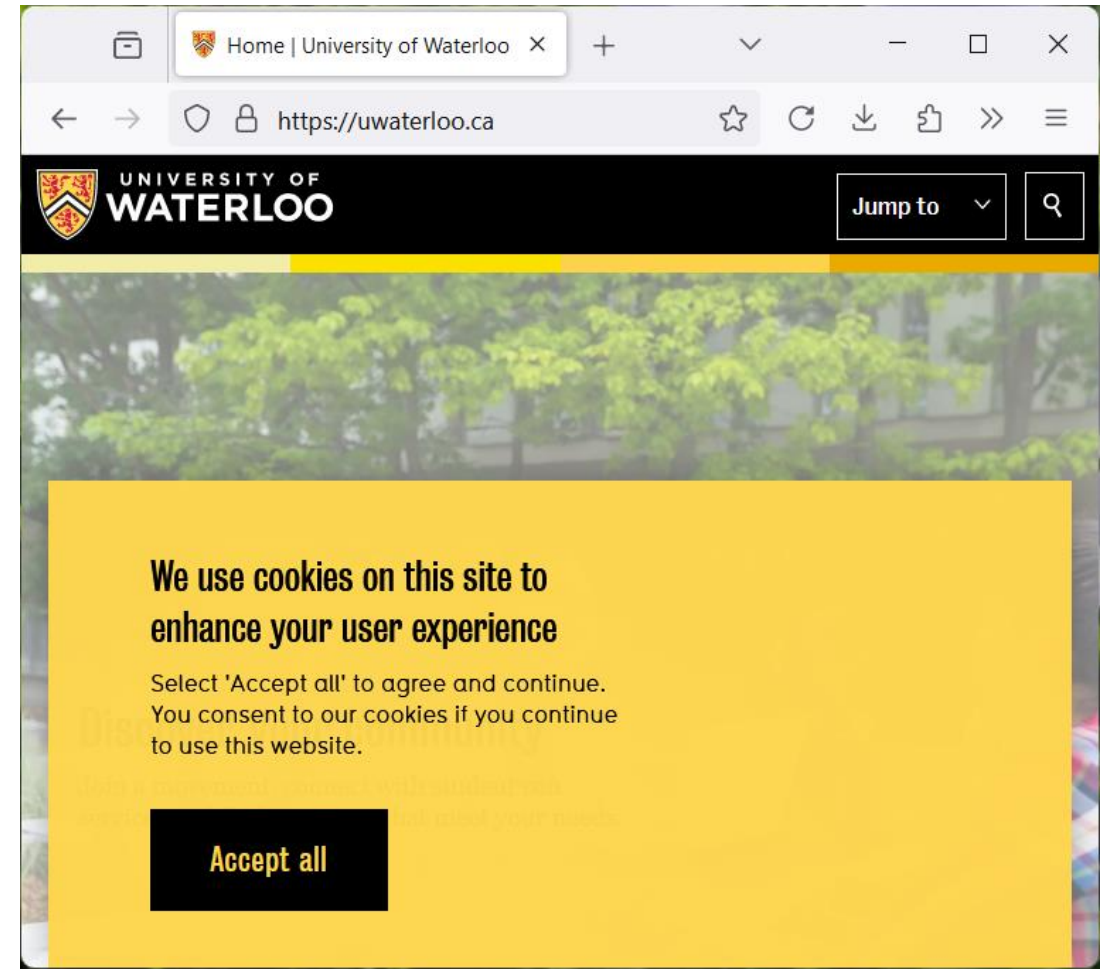
**Accountability** - take responsibility and keep records showing compliance.

**I will cover GDPR in a separate lecture**

# DESIGNING FOR NOTICE AND CHOICE

# Notice and Choice: the idea

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

**Notice and choice/consent is based on the consumer having easy access to decision-altering information.**

**Aka Privacy policies**

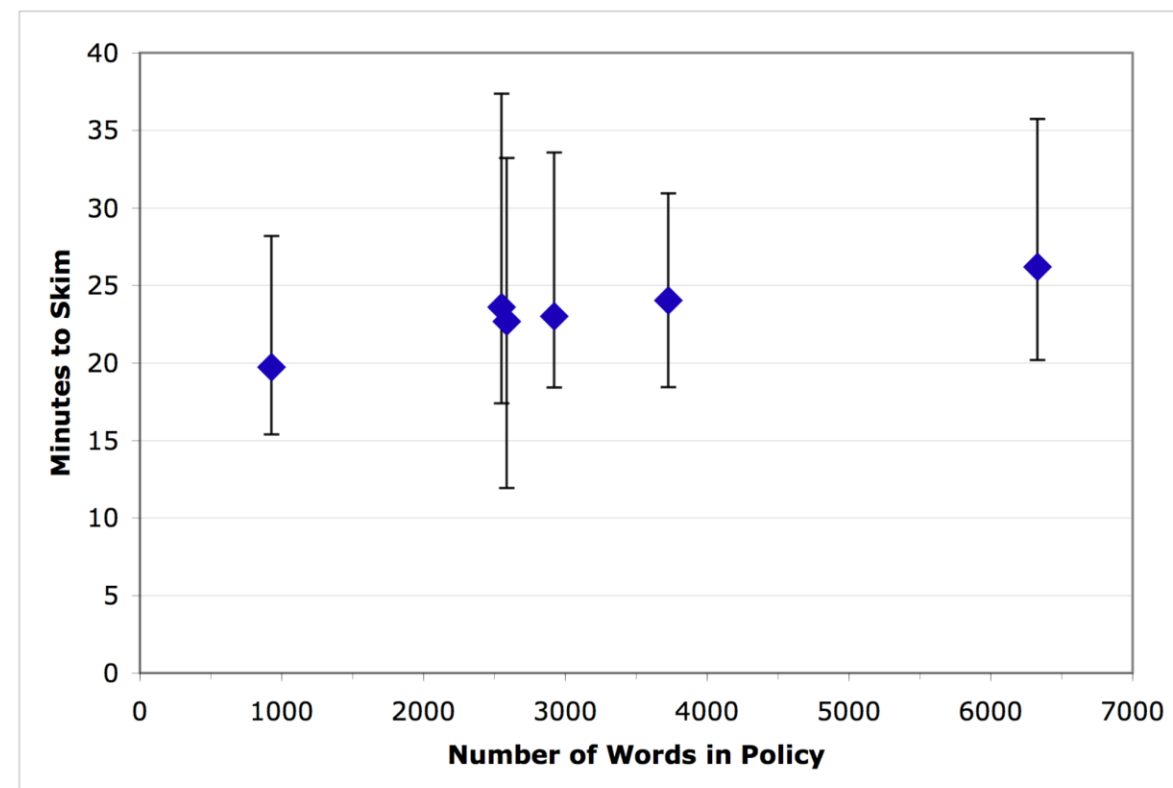


# How much money would it cost the US economy if everyone read through privacy policies?

- Notice and choice is dependent on awareness of content of privacy policies
- People do not read all the privacy policies, but what if they did?
- 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

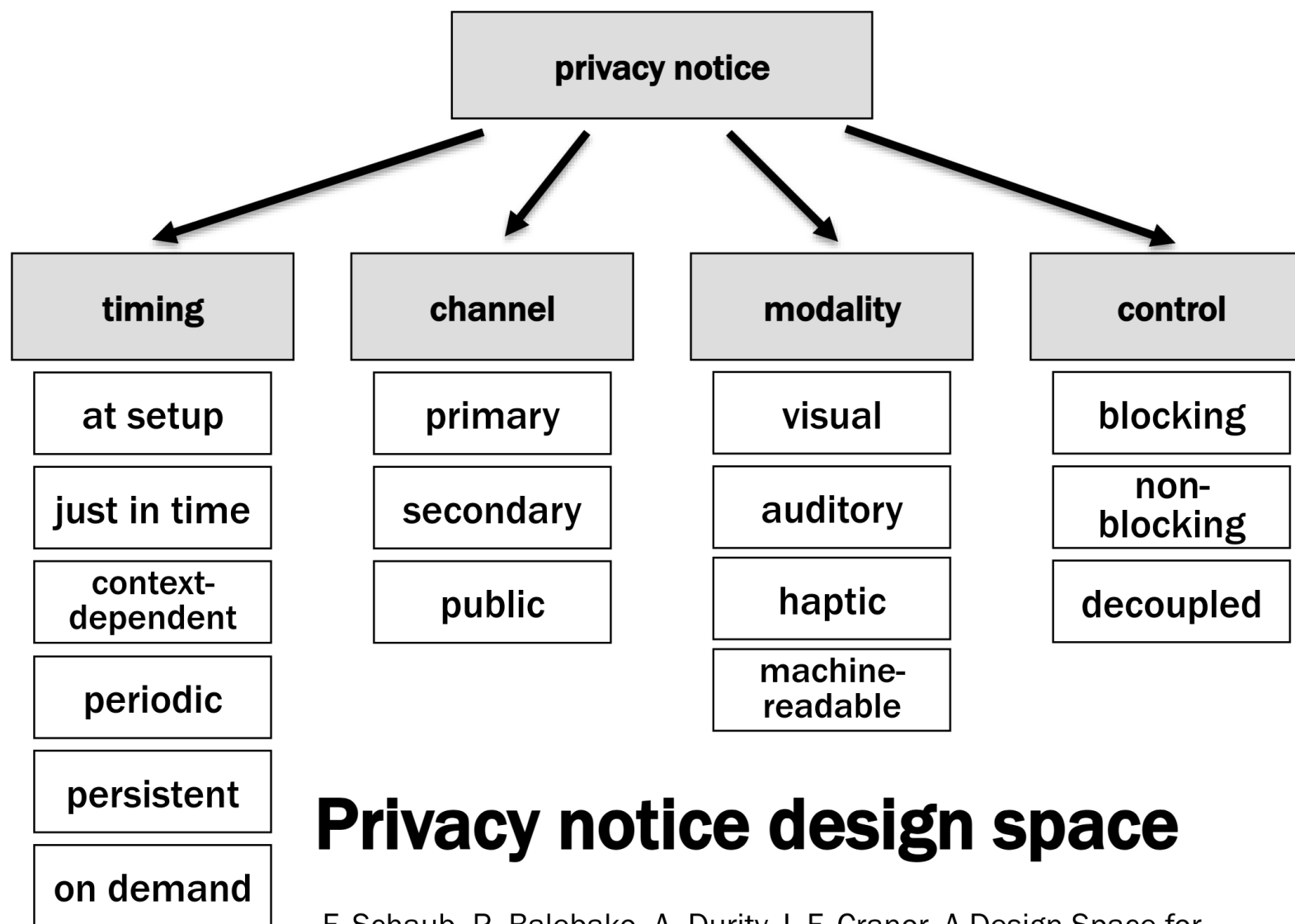
# Amount of time needed to skim a policy

- 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.



# Cost of notice and choice: \$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	\$1,140 / year	\$559.7 billion / year	\$251.9 billion / year
	(work: \$1,970; home: \$563)	(work: \$886; home: \$253)	(work: \$435 B; home: \$124 B)	(work: \$196 B; home: \$56 B)
Point	\$3,534 / year	\$2,226 / year	\$781 billion / year	\$492 billion / year
	(work: \$2,791; home: \$743)	(work: \$1,758; home: \$468)	(work: \$617 B; home: \$164 B)	(work: \$389 B; home: \$103 B)
Upper bound	\$5,038 / year	\$4,870 / year	\$1.1 trillion / year	\$1.1 trillion / year
	(work: \$4,203; home: \$835)	(work: \$4,063; home: \$807)	(work: \$929 B; home: \$184 B)	(work: \$898 B; home: \$178 B)



## 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