Privacy Policy

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

22/03/2024

THE UNIVERSITY *of* EDINBURGH

Overview

- No more blog; coursework due on Monday noon, submission via **Gradescope**; Guest lecture next week
- Trust and E-commerce
- Privacy policy
- Privacy regulation

Apps

X's privacy policy confirms it will use public data to train AI models

Sarah Perez @sarahpereztc / 6:34 PM GMT+1 • September 1, 2023

Comment

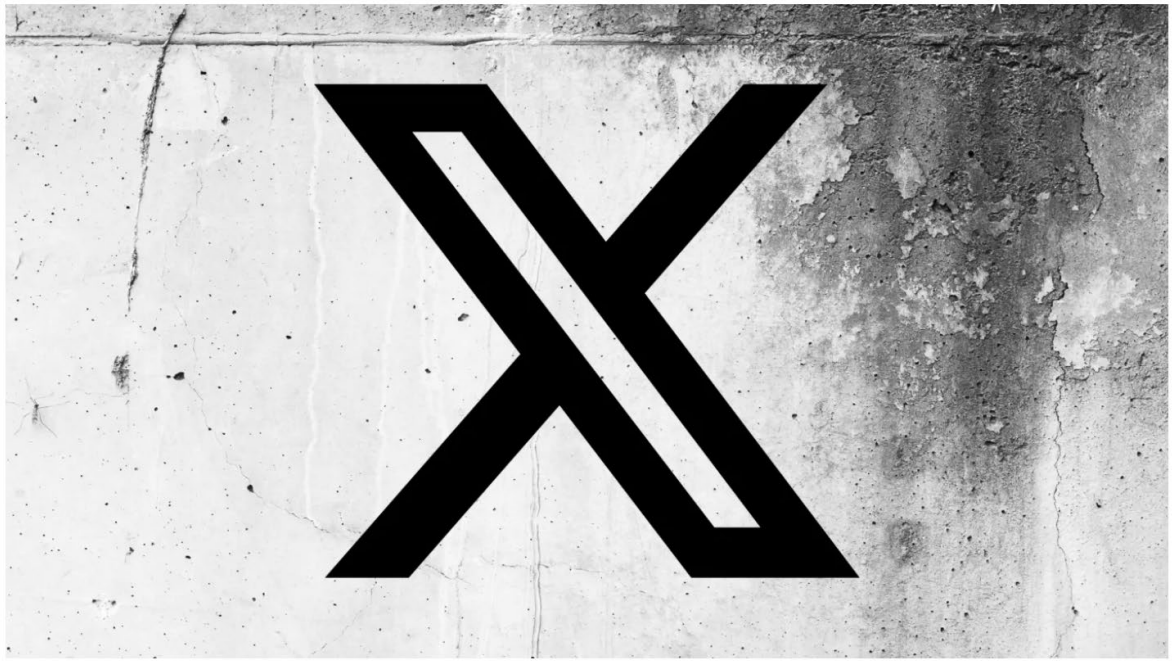


Image Credits: TechCrunch

X's recently updated privacy policy informed its users it would now collect biometric data as well as users' job and education history, Bloomberg spotted earlier this week. But it appears

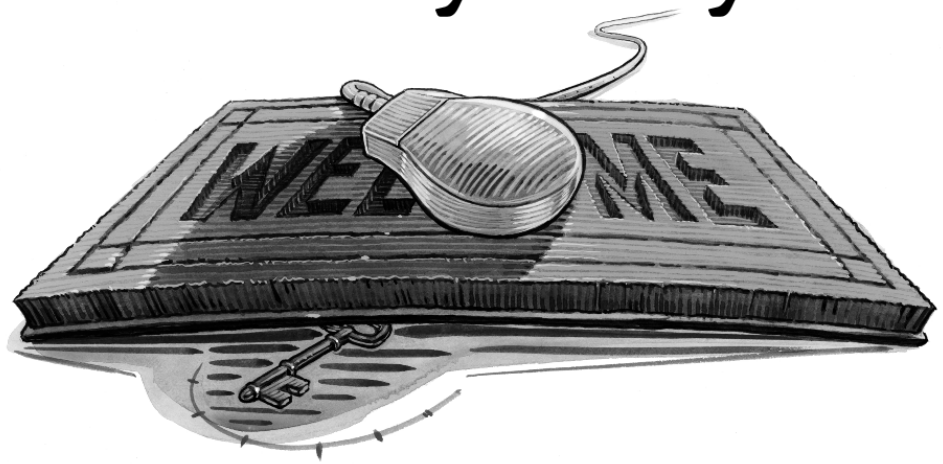
https://techcrunch.com/2023/09/01/xs-privacy-policy-confirms-it-will-use-public-data-to-train-ai-models/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEAWusmF9KoL7dpxc_Pp6atqyBdMOg4frDlwGc36qpmPxLiwp0QchMKfsAhmMbqR-aGuxPJ_kprIJLhppc-q9lWqyfbYLrgFs-n2QI501ADMuKUJZ2r4DVTTFholuPiBwZhsFMXnKj1N0dRaxrucaQJNuMp9yGCDg_3Y9SjAAvw_

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."

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

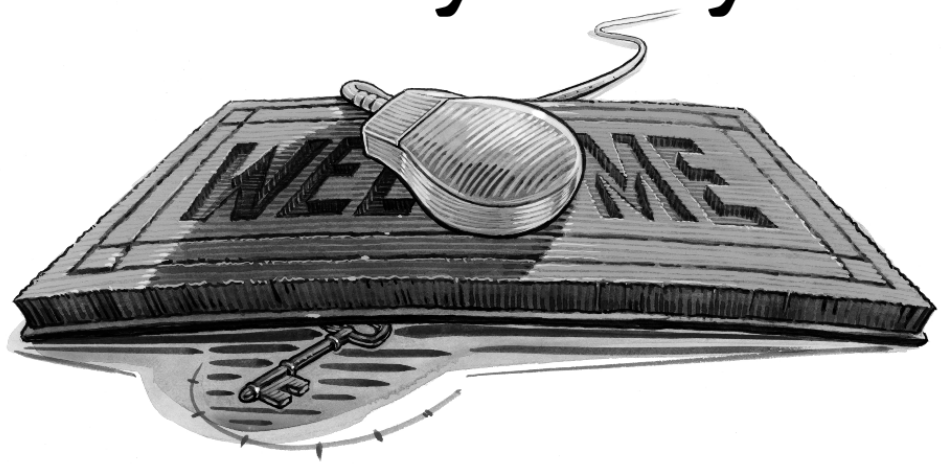
ILLUSTRATION BY DOUGLAS JONES

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."

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

ILLUSTRATION BY DOUGLAS JONES

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?

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 a 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 perceived

Table 1. Risks in e-Commerce

1. Risks that stem from the Internet include:
a) whether credit card data gets intercepted;
b) whether the data is transmitted correctly;
c) their own interaction with the system- i.e. whether they use it correctly
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;
b) whether the online-vendor will actually deliver the products or services.

Riegelsberger, Jens, and M. Angela Sasse. "Trustbuilders and trustbusters." *Towards the E-Society*. Springer, Boston, MA, 2001. 17-30.

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

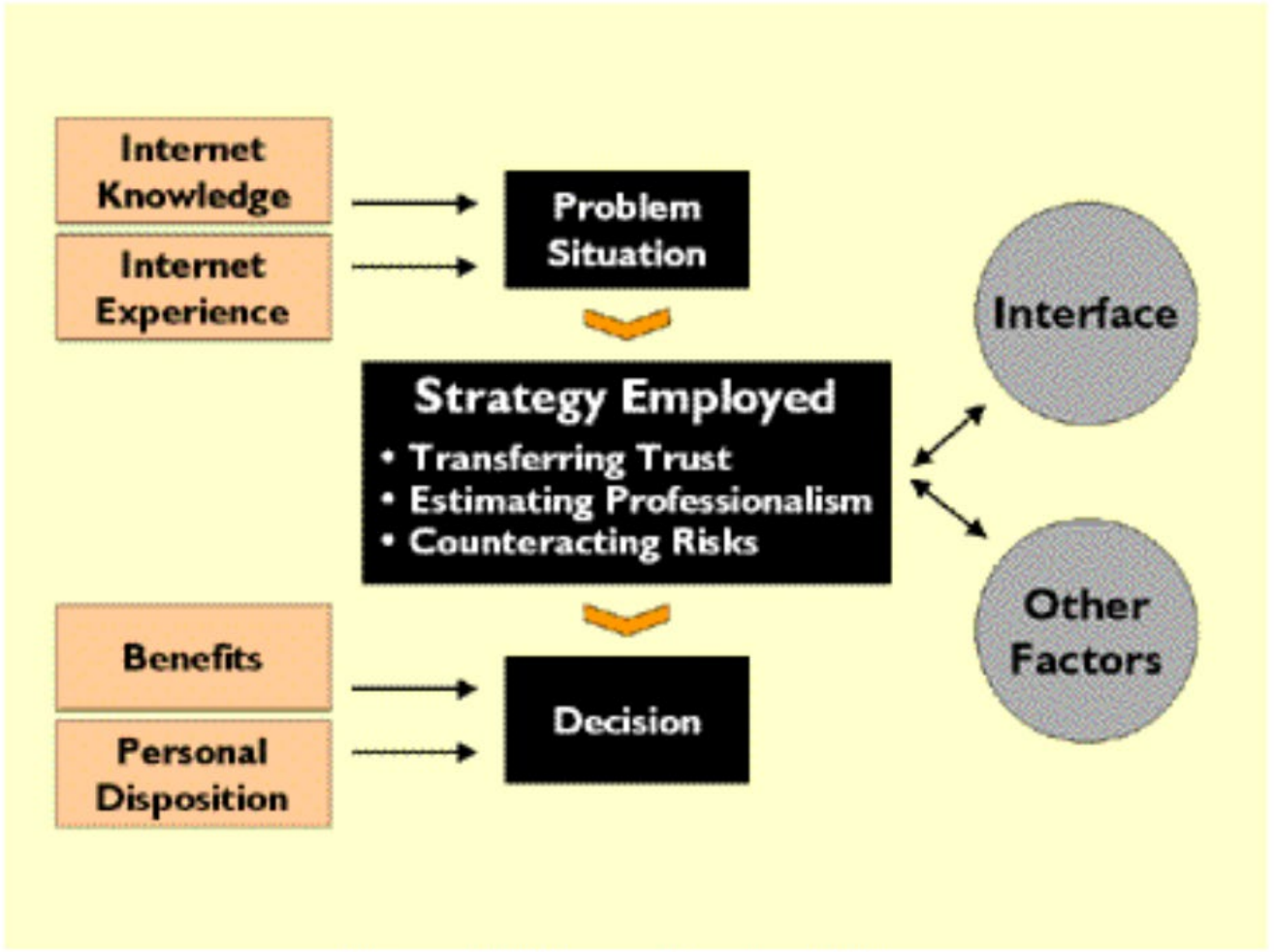


Figure 1. E-Shopper Decision Making

Riegelsberger, Jens, and M. Angela Sasse. "Trustbuilders and trustbusters." *Towards the E-Society*. Springer, Boston, MA, 2001. 17-30.

Trust transfer

- Inexperienced shoppers tend to transfer trust. One thing worked, so they look for something else that looks simil thy.

- Collective approaches
  - TRUSTe seal
  - Being part of a more trusted retail group
  - “well they would say that, wouldn’t they”...
- Individual site approaches
  - Hard to build trust on just one site.
  - Things like customer testimonials first require trust in the company that they are true

[12] Riegelsberger, Jens, and M. Angela Sasse. "Trustbuilders and trustbusters." *Towards the E-Society*. Springer, Boston, MA, 2001. 17-30.

Help people reduce the risks

Table 1. Risks 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

Riegelsberger, Jens, and M. Angela Sasse. "Trustbuilders and trustbusters." *Towards the E-Society*. Springer, Boston, MA, 2001. 17-30.

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

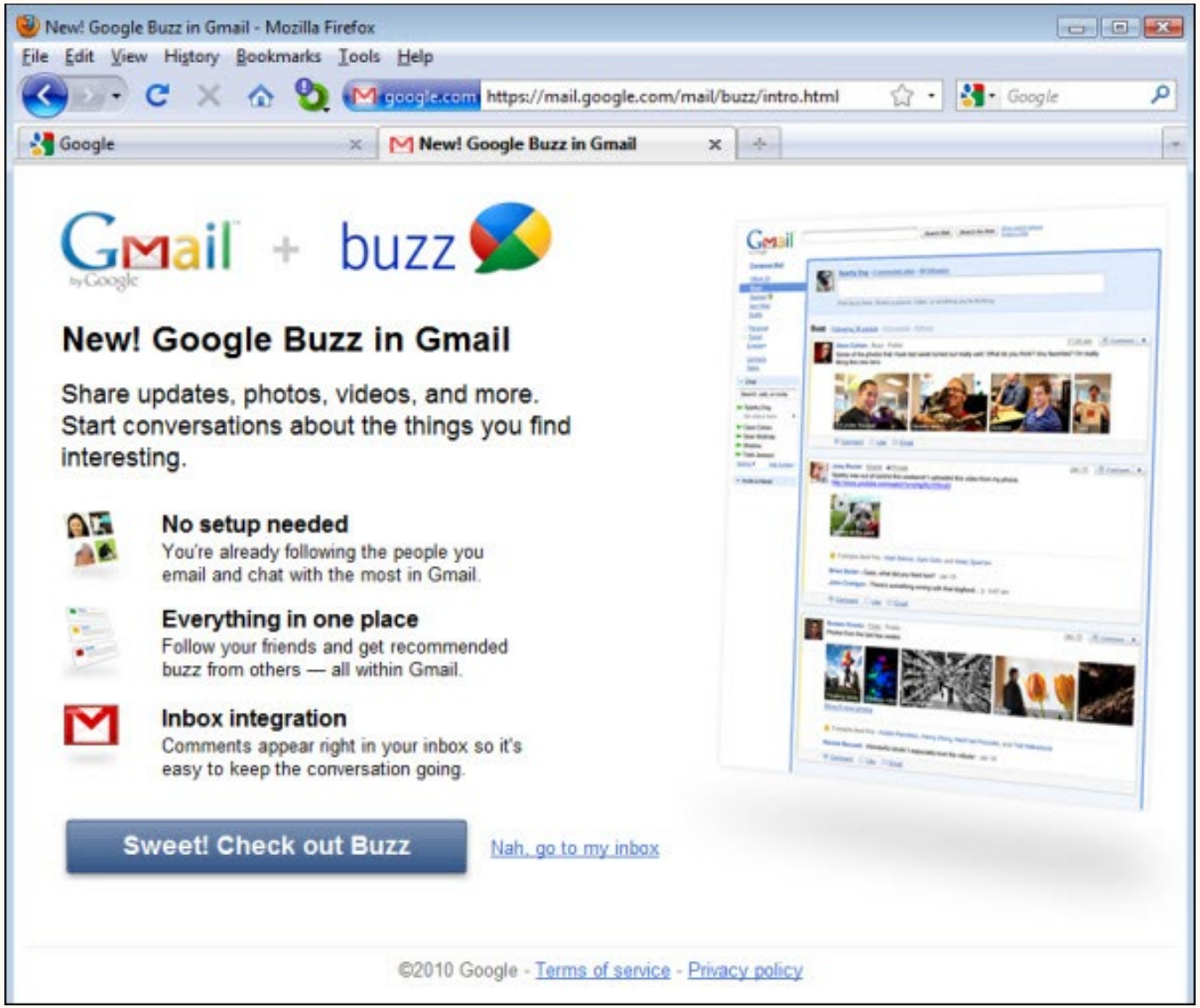
Roughly: The FTC declared that if an organization said it did X in its privacy policy, but then was shown to not be doing X, then the FTC could levy a large fine.

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 that 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 selfor 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.”

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connec

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.”

ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

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)

Privacy 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.

Legal documents tend to be broken up into Articles, sections, and subsections. These are labeled using a notation like Art. 2 a, which means Article 2, section a.

provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity; (Art. 2 a)

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

"Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information"
- U.S. President Donald Trump, Executive Order, 2017

"In the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities."
- Maximillian Schrems, 2015

General Data Protection Regulation (GDPR) superseded the Data Protection Directive. GDPR is a regulation, not a directive. Which means it is directly binding and applicable.

1998 Act:	GDPR:
Principle 1 – fair and lawful	Principle (a) – lawfulness, fairness and transparency
Principle 2 – purposes	Principle (b) – purpose limitation
Principle 3 – adequacy	Principle (c) – data minimisation
Principle 4 – accuracy	Principle (d) – accuracy
Principle 5 - retention	Principle (e) – storage limitation
Principle 6 – rights	No principle – separate provisions in Chapter III
Principle 7 – security	Principle (f) – integrity and confidentiality
Principle 8 – international transfers	No principle – separate provisions in Chapter V
(no equivalent)	Accountability principle

Lawful basis for processing

- The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:
- **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **(d) Vital interests:** the processing is necessary to protect someone's life.
- **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Personal data in GDPR

The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data.

Consent in GDPR

“‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”

- Consent must be explicit
- Obtained for each purpose the data is used for
- Specific, plainly worded, and freely given
- An online form which has consent options structured as an opt-out selected by default is in violation
- Withdrawing consent must be possible, and no more challenging than giving it

Google Privacy & Terms

Overview | Privacy Policy | Terms of Service | Technologies | FAQ

Introduction

Information Google collects

Why Google collects data

Your privacy controls

Sharing your information

Keeping your information secure

Exporting & deleting your information

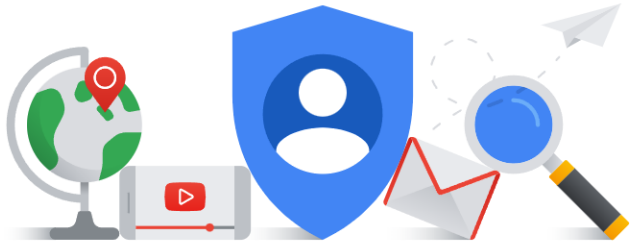
Retaining your information

Compliance & cooperation with regulators

European requirements

About this policy

Related privacy practices



GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

If European Union or United Kingdom data protection law applies to the processing of your information, you can review the European requirements section below to learn more about your rights and Google's compliance with these laws.

https://policies.google.com/privacy?hl=en-US

Google Privacy & Terms

Overview | Privacy Policy | Terms of Service | Technologies | FAQ

Introduction

Information Google collects

Why Google collects data

Your privacy controls

Sharing your information

Keeping your information secure

Exporting & deleting your information

Retaining your information

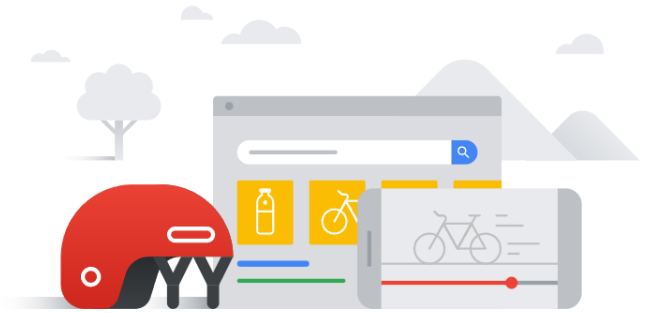
Compliance & cooperation with regulators

European requirements

About this policy

Related privacy practices

Provide personalized services, including content and ads



We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And, depending on your available settings, Google Play could use information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests and activity across Google services. For example, if you search for "mountain bikes," you may see ads for sports equipment on YouTube. You can control what information we use to show you ads by visiting your ad settings in My Ad Center.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health

Privacy Policy

Data transfer frameworks

Key terms

Partners

Updates

the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

California requirements

The California Consumer Privacy Act (CCPA) requires specific disclosures for California residents.

This Privacy Policy is designed to help you understand how Google handles your information:

- We explain the categories of information Google collects and the sources of that information in Information Google collects.
- We explain how Google uses information in Why Google collects data.
- We explain when Google may share information in Sharing your information. Google does not sell your personal information.

The CCPA also provides the right to request information about how Google collects, uses, and discloses your personal information. And it gives you the right to access your information and request that Google delete that information. Finally, the CCPA provides the right to not be discriminated against for exercising your privacy rights.

We describe the choices you have to manage your privacy and data across Google's services in Your privacy controls. You can exercise your rights by using these controls, which allow you to access, review, update and delete your information, as well as export and download a copy of it. When you use them, we'll validate your request by verifying that you're signed in

Privacy Policy

Data transfer frameworks

Key terms

Partners

Updates

the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

California requirements

The California Consumer Privacy Act (CCPA) requires specific disclosures for California residents.

This Privacy Policy is designed to help you understand how Google handles your information:

- We explain the categories of information Google collects and the sources of that information in Information Google collects.
- We explain how Google uses information in Why Google collects data.
- We explain when Google may share information in Sharing your information. Google does not sell your personal information.

The CCPA also provides the right to request information about how Google collects, uses, and discloses your personal information. And it gives you the right to access your information and request that Google delete that information. Finally, the CCPA provides the right to not be discriminated against for exercising your privacy rights.

We describe the choices you have to manage your privacy and data across Google's services in Your privacy controls. You can exercise your rights by using these controls, which allow you to access, review, update and delete your information, as well as export and download a copy of it. When you use them, we'll validate your request by verifying that you're signed in

Back to offerings

U.S. | ALL INDUSTRIES

COPPA (U.S.)

The Children's Online Privacy Protection Act of 1998 (COPPA) is a U.S. regulation applicable to the collection of personal information from children under the age of 13. COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

Google Workspace for Education:

Google Workspace for Education Core Services can be used in compliance with the Children's Online Privacy Protection Act (COPPA). Google contractually requires that

Quick links

Google Workspace for Education Privacy and Security Center

Federal Trade Commission (FTC) website

Children's Privacy (FTC) website

Are privacy policies easy to make?


How to Create a
Privacy
Policy