Security and privacy notices/Dark patterns

Mainack Mondal

CS 60081
Autumn 2022

Roadmap

- Security advice

- Security and privacy warnings

- Dark patterns

- Privacy consent

- Inclusive security and privacy

Roadmap

- **Security advice**

- Security and privacy warnings

- Dark patterns

- Privacy consent

- Inclusive security and privacy

Example of security advice

For Security non-experts

1. Use antivirus software

2. Use strong passwords

3. Change passwords frequently

4. Only visit websites they know

5. Don't share personal information

Example of security advice

For Security non-experts

1. Use antivirus software

2. Use strong passwords

3. Change passwords frequently

4. Only visit websites they know

5. Don't share personal information

For Security experts

1. Install software updates

2. Use unique passwords

3. Use two-factor authentication

4. Use strong passwords

5. Use a password manager

Ignoring security advice

- "So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users"

  - https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SoLongAndNoThanks.pdf
  - Cormac Herley, MSR, Redmond
  - Take away: "Ignoring security advice is rational"

Externalities vs. internalities

- Externality
  - The costs or benefits of an activity effect other groups or people or (the user in the long run)
  - Indirect costs/benefits – you will be *secure,* no one *get* into your network

- Internality
  - The costs or benefits of an activity effect the user themselves immediately
  - How would I choose and remember a strong password every time?

Example: online fraud

	Direct Costs	Indirect costs (*i.e.* externalities)
Attackers	Gain	Don't Care
Banks	Loss	Reputation
Victim Users	Possible Loss	Effort
Non-victim Users	None	User education

Table 1: Costs of online financial fraud. The direct costs are zero-sum: the attacker gain as much as the banks and victims lose. The externalities are indirect costs imposed on banks and non-victim users as they seek to avoid and deal with the consequences of the attacks. For many forms of fraud the externalities are many times greater than the direct costs.

Example: URL

Address	Message to users
192.34.23.1	Numeric IP addresses are suspect
www.paypa1.com	Address-bar typos
www.paypal.so	Incorrect top-level domain
www.geocities.com/www.paypal.com	Institution should appear in path rather than host
www-paypal-com.evil.com	Punctuation matters: '-' $\neq$ '.'
www.paypal.com.evil.com	Domains are read right to left

Table 2: Increasing sophistication of phishing URLs requires increasing complexity of the security advice to users.

- US annual phishing cost = $60 million

- US online pop. = 180 million

- Average benefit of advice = 0.33 cents

- Cost of reading/acting on advice (for more than 3 minutes) > $7.25 * 3/60 = 0.36 cents

To summarize

- Costs
  - Re-training users constantly with recent attacks
  - Training organizations to ensure advice is true and makes sense

- Benefits (Potential)
  - Less phishing susceptibility

- Benefits (actual)
  - Often none: Most large companies absorb financial loss from phishing

Roadmap

- Security advice

- **Security and privacy warnings**

- Dark patterns

- Privacy consent

- Inclusive security and privacy

What are warnings?

- A type of advice

- The given advice tells the user what the developers think is important or broken

- Almost any deployed systems has warning/advices

  - Remember possible warnings in your PDS course while compiling?

Warnings/Advice: problems

Warnings/Advice: problems

- A zillion

  - Walk only when traffic-light is green (people don't care)

  - Complicated instructions to operate a machine (A/V problems during lectures)

  - …

Warning/Advice

- Involve users in decisions

Warning/Advice

- Involve users in decisions

Warning/Advice

- Involve users in decisions

- They have contextual knowledge

Warning/Advice

Good security warnings are contextual and the designer should balance risks with benefits

Things you need to communicate

- Questions – "did you just log in from "Lyon, France"?"

- Warnings – "the website is known to distribute malicious software"

- UI passive indicators – the padlock icon on the address bar

- UI active indicators – "This password is weak (red bar)"

- Task-relevant information – "Passwords should be 8 characters long and must have a capital letter."

- Educational – "10 security behaviors you should do to protect yourself online"

- Awareness – "This email seems like a spam, please don't click any links on it."

So how to design good warnings?

- NEAT and SPRUCE
    - Developed at Microsoft research
    - Guidance on how to create effective security messaging for end users

NEAT

- **N**ecessary – Can you change the system design to eliminate or defer this user decision?

- **E**xplained - Does your system present all the information the user needs to make this decision?

- **A**ctionable – Have you determined a set of steps the user will realistically be able to take to make the decision correctly?

- **T**ested – Have you tested that your user experience is NEAT for all scenarios -- benign, malicious, outside your team

Example

Your connection is not private

Attackers might be trying to steal your information from **grey-dev.ece.cmu.edu** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Advanced

Back to safety

- Necessary, Explained, Actionable, tested

Example

Your connection is not private

Attackers might be trying to steal your information from **grey-dev.ece.cmu.edu** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

| Hide advanced | Back to safety |

This server could not prove that it is **grey-dev.ece.cmu.edu**; its security certificate is from **grey-dev.andrew.cmu.edu**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to grey-dev.ece.cmu.edu (unsafe)

- Necessary, Explained, Actionable, tested

SPRUCE

- **S**ource – Who or what is asking the user to make a decision

- **P**rocess –actionable steps to follow to make a good decision

- **R**isk – Explain what bad thing could happen if they user makes a wrong decision

- **U**nique – Tell the user what information user bring to the decision

- **C**hoices – List available options and clearly recommend one

- **E**vidence – Highlight information the user should factor in or exclude in making a decision

Roadmap

- Security advice

- Security and privacy warnings

- **Dark patterns**

- Privacy consent

- Inclusive security and privacy

What are dark patterns?

"Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions that if fully informed and capable of selecting alternatives — they might not make"

- https://webtransparency.cs.princeton.edu/dark-patterns/
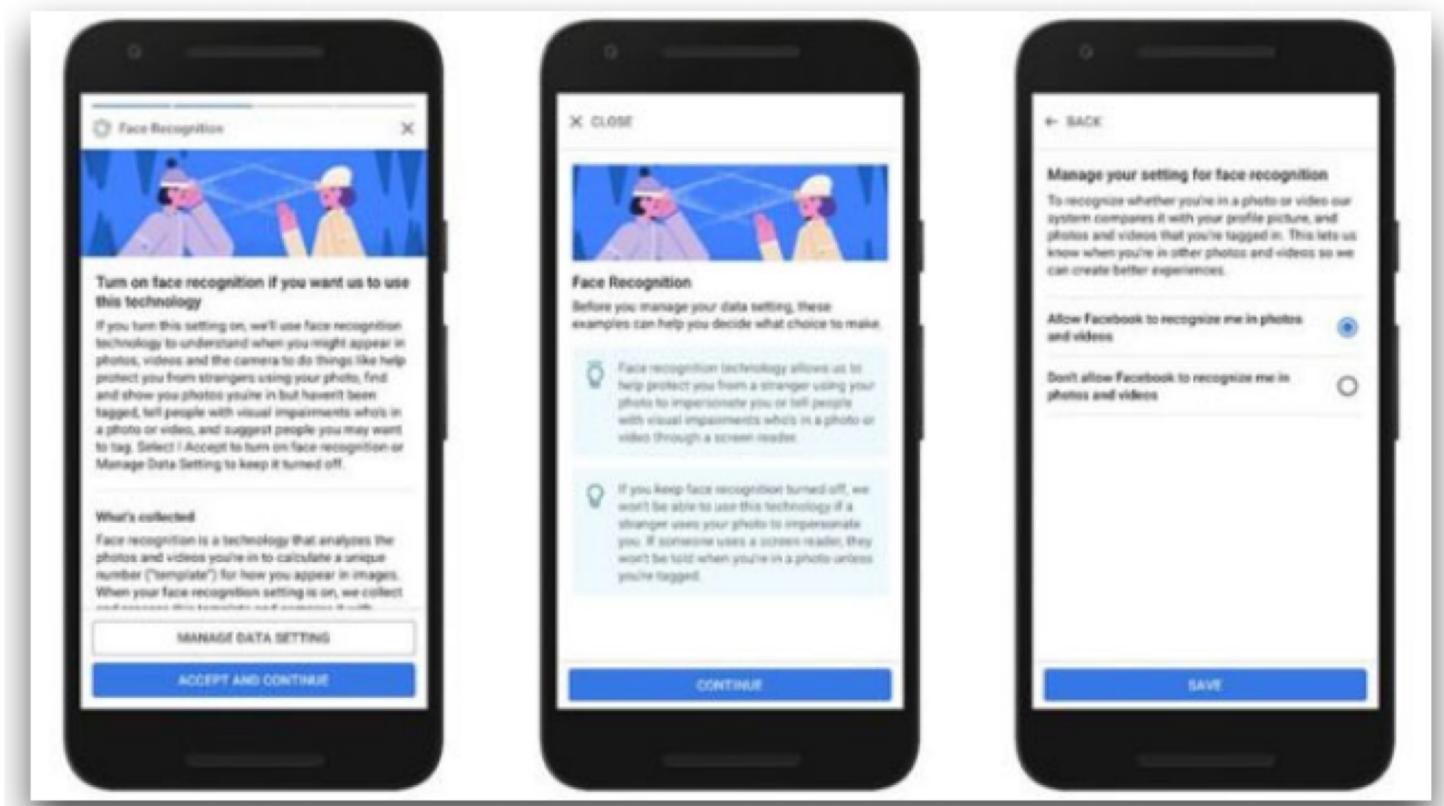
Dark patterns: Where usability goes rouge

- The designers force users to make unwise choices

  - For the benefit of the company

  - "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites.", Mathur et al., CSCW 2019

  - https://arxiv.org/pdf/1907.07032.pdf

Example: Instagram ad on mobile

Example: Facebook consent for facial recognition

3 clicks – consent, 14 clicks – revoke consent

How to find such patterns at scale?

- Study design

  - Create a list of around 11k shopping websites

  - The created a shopping bot which attempts to buy content

  - Stops before the payment page

  - Scrape each page along the way

  - Separate out page segments: HTML sources, HAR files, screenshots, HTTP requests, HTTP responses

  - Took only text data

  - Then cluster and finally manually label the clusters

Design summary
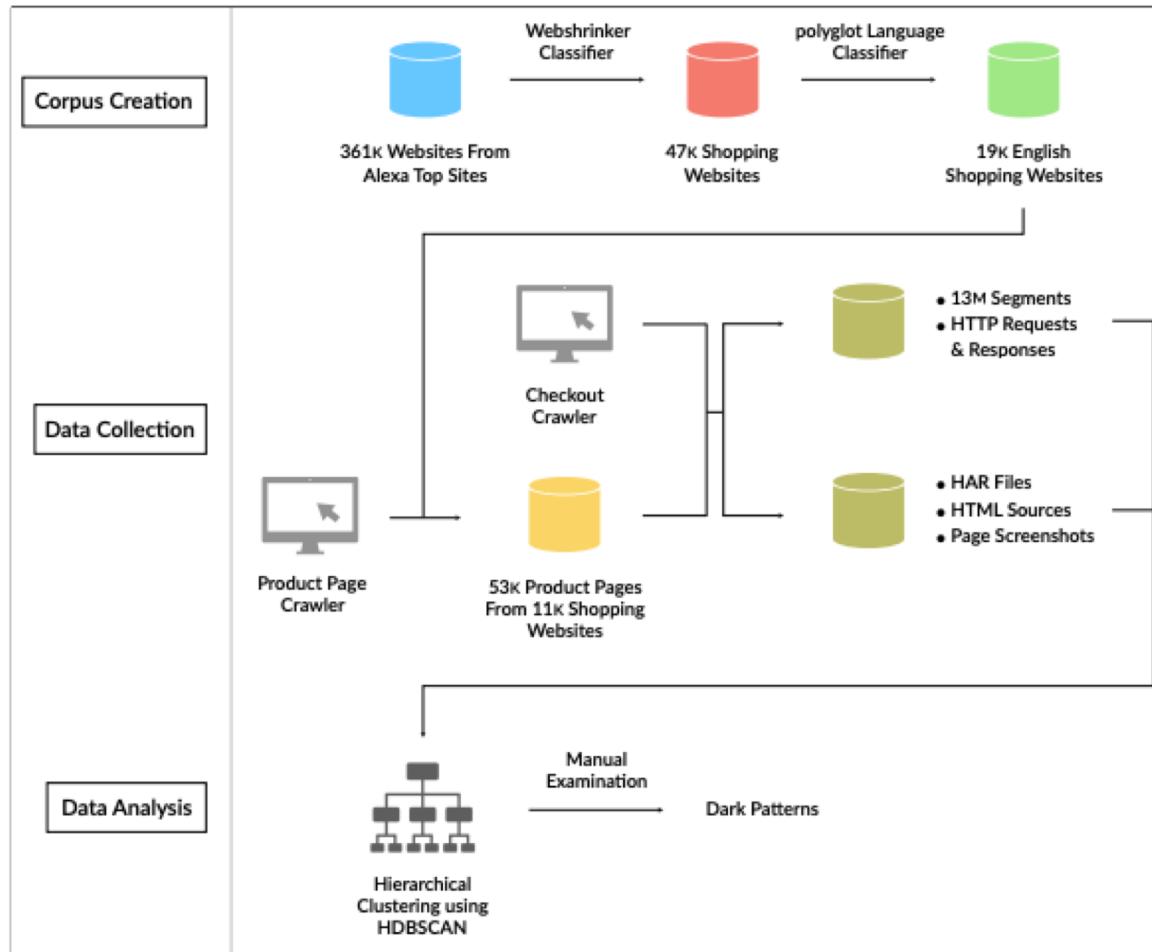
Fig. 1. Overview of the shopping website corpus creation, data collection using crawling, and data analysis using hierarchical clustering stages.

Dark pattern: Sneaking

- Attempting to misrepresent user actions, or delay information that if made available to users, they would likely object to

Dark pattern: Urgency

- Imposing a deadline on a sale or deal, thereby accelerating user decision-making and purchases

Dark pattern: Misdirection

- Using visuals, language, or emotion to steer users toward or away from making a particular choice

CONTACT PREFERENCES

Please select **Yes** below if you are happy to receive email notifications of **exclusive member offers** from M8 Group companies. You will always have the option to unsubscribe from any emails you decide you would rather not receive.

☐ **YES** I do want to hear about exclusive offers & discounts
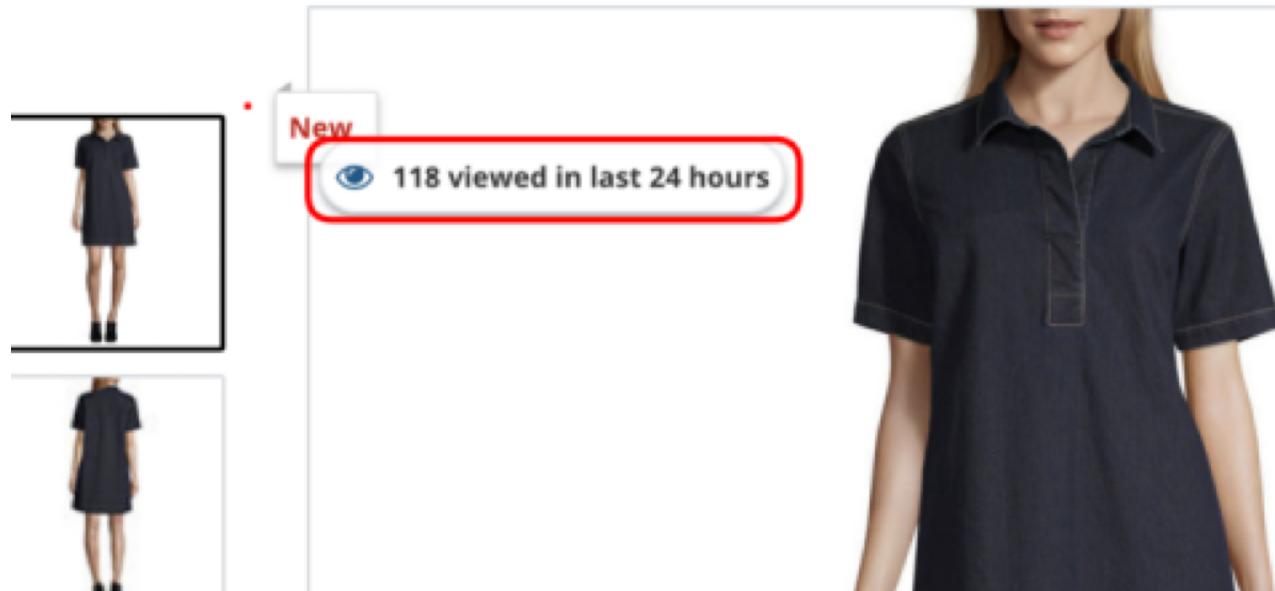
☐ NO I'd rather NOT hear about exclusive offers & discounts

Don't worry, we will never sell or rent your personal information, it's part of our privacy policy. Also, you can update your preferences and unsubscribe from 'My Account' at any time.
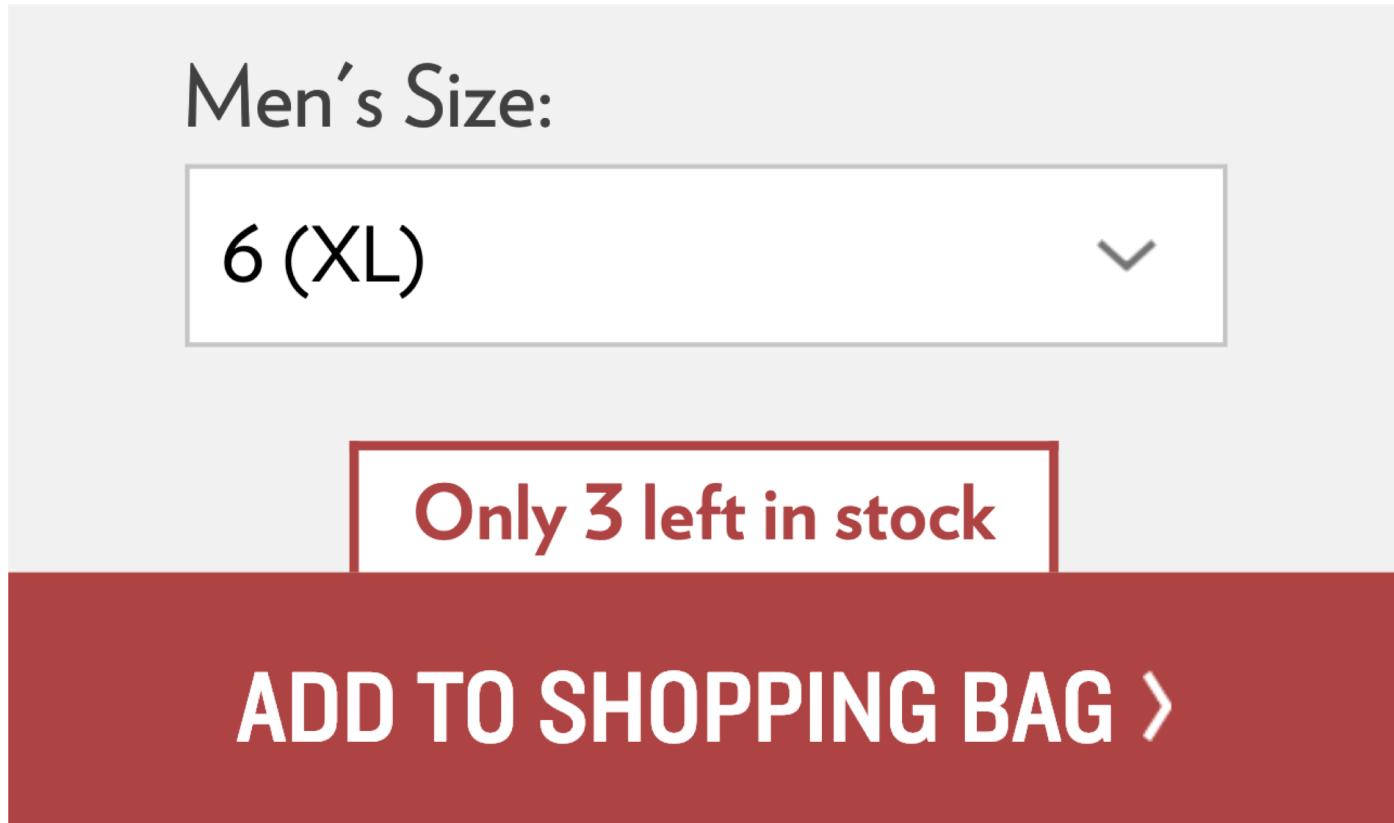
Dark pattern: Social proof

- Influencing users' behavior by describing the experiences and behavior of other users

Dark pattern: Scarcity

- Signaling that a product is likely to become unavailable, thereby increasing its desirability to users

Dark pattern: Obstruction

- Making it easy for the user to get into one situation but hard to get out of it

Dark pattern: Forced action

- Forcing the user to do something tangential in order to complete their task

Solutions

- Design extensions

  - Warn users about dark patterns

- Legal solutions

  - Viewing this as "deception"

- Policy proposal

  - "Proposed Deceptive Experiences To Online Users Reduction (DETOUR) act reins in more broadly against design that "obscures, subverts, or impairs user autonomy and decision-making".