

# Operationalizing data privacy regulations/Inclusive Privacy and Security

Mainack Mondal

CS 60081  
Autumn 2022



# Roadmap

- Security advice
- Security and privacy warnings
- Dark patterns
- **Privacy consent**
- Inclusive security and privacy

# First: GDPR

- General data protection Regulation in Europe
  - Also adopted in the UK
  - Attempt to regulate data collection companies to respect user privacy

# GDPR regulations

- Principle (a): lawfulness, fairness and transparency
- Principle (b): purpose limitation
- Principle (c): data minimization
- Principle (d): accuracy
- Principle (e): storage limitation
- Principle (f): Integrity and confidentiality
- Principle (g): Accountability principle

# The principles

- **Lawfulness, fairness and transparency** - a lawful basis for processing + 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 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.
- **Accountability** - take responsibility and keep records showing compliance.

# Right to be forgotten (Art 17 (2))

“personal data must be **erased immediately** where the **data are no longer needed** for their **original processing purpose**, or the **data subject has withdrawn his consent** and there is no other legal ground for processing, the **data subject has objected and there are no overriding legitimate grounds for the processing**, or erasure is required to fulfil a statutory obligation under the EU law or the right of the Member States. In addition, data must naturally be erased if the processing itself was against the law in the first place.”

- <https://gdpr-info.eu/issues/right-to-be-forgotten/>

# Right to an explanation (Art 22)

- data subject shall have the right not to be subject to a decision based **solely** on **automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- “at least” right to obtain human intervention express point of view context the decision
- data subject shall have right to obtain... the following information: “meaningful” information about the logic involved “at least in” cases of “automated decision making”, including profiling”.

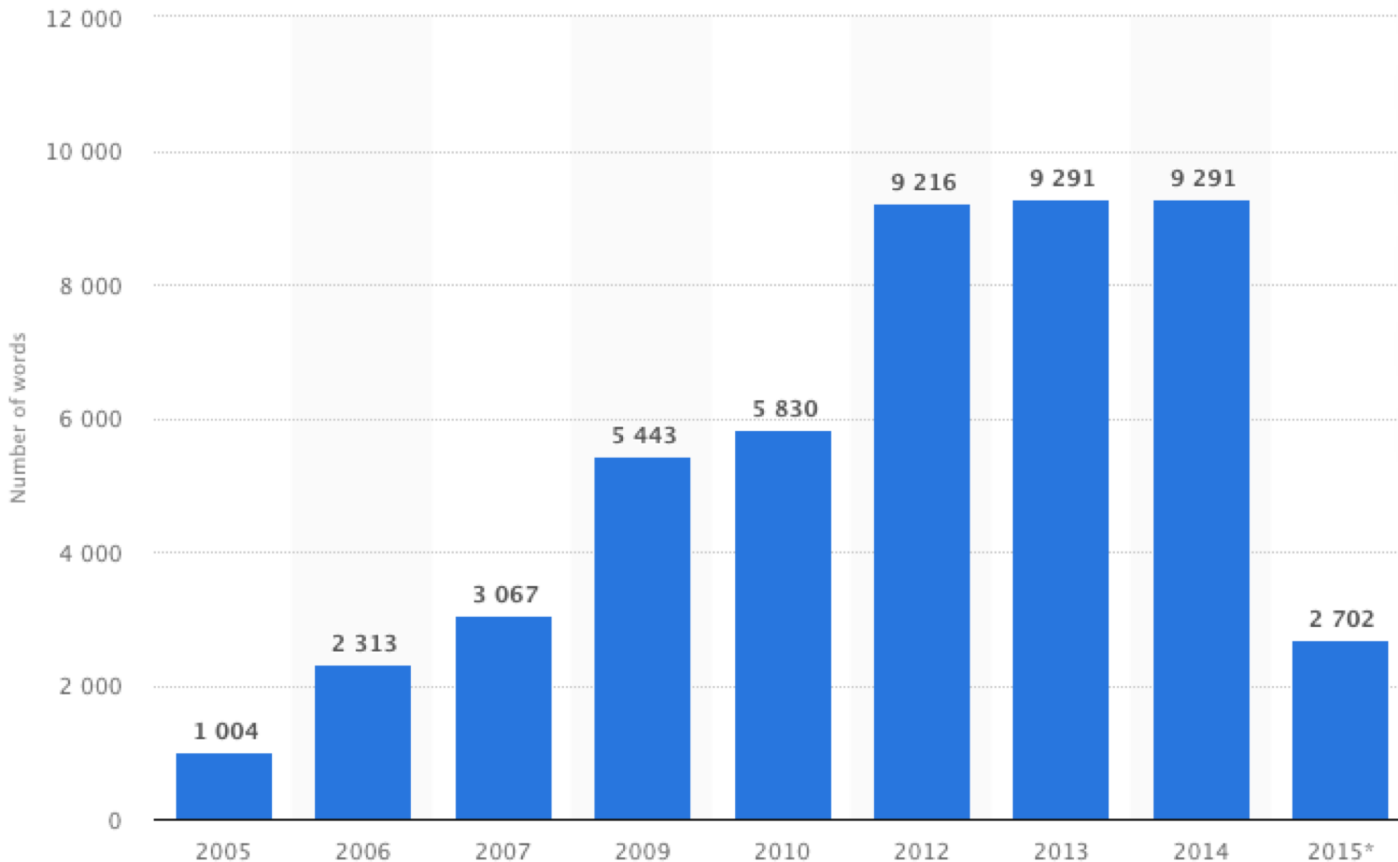
# Data processing requirements under GDPR

- GDPR encourages organizations to find a legal basis for processing (+ obtaining consent).
  - Consent
  - Contract
  - Legal obligation
  - Vital interest - the processing is necessary to protect someone's life.
  - Public task
  - Legitimate interests



How to get consent: privacy policies?

# How to get consent: privacy policies?



For reference: #words in Magna Carta = 4594

# How to get consent: privacy policies?

- Remember previous lecture's lesson
  - What is the cost on the user for reading these privacy policies?
  - “The cost of reading privacy policies”, McDonald et al.
  - <https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>

# How to get consent: privacy policies?

- Remember previous lecture's lesson
  - What is the cost on the user for reading these privacy policies?
  - “The cost of reading privacy policies”, McDonald et al.
  - <https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>

Posed the question: if website users were to read the privacy policy for each site they visit just once a year, what would their time be worth?

# How to find answer

- $\text{Cost} = \text{Annual time to read online privacy policies} * \text{average wage in unit time}$
- $\text{Annual time to read online privacy policies} = \# \text{internet users} * \text{avg. reading rate of privacy policy (words per minute)} * \text{\$unique sites visited per user per year}$

# How to find answer

- $\text{Cost} = \text{Annual time to read online privacy policies} * \text{average wage in unit time}$
- $\text{Annual time to read online privacy policies} = \text{\#internet users} * \text{avg. reading rate of privacy policies (words per minute)} * \text{\#unique sites visited per user per year}$
- Factors – reading in home vs. work, people might just skim, privacy policy vary in length

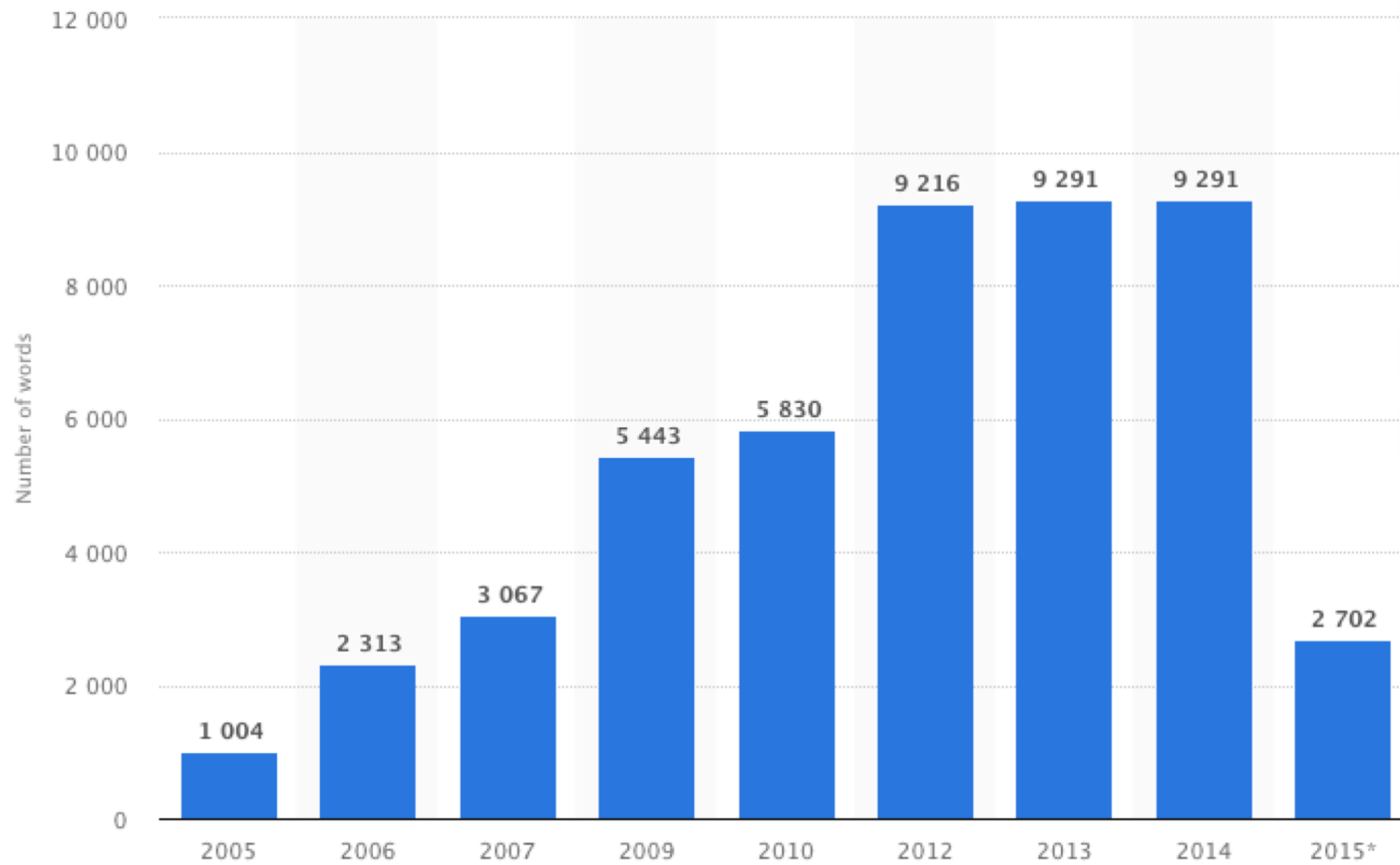
# Result

<b>Estimate</b>	<b>Individual time to read</b>	<b>Individual time to skim</b>	<b>National time to read</b>	<b>National time to skim</b>
<b>Lower bound</b>	181 hours / year	81 hours / year	39.9 billion hours / year	17.9 billion hours / year
<b>Point Estimate</b>	244 hours / year	154 hours / year	53.8 billion hours / year	33.9 billion hours / year
<b>Upper bound</b>	304 hours / year	293 hours / year	67.1 billion hours / year	64.8 billion hours / year

**Table 7: Annual time estimates for reading and skimming online privacy policies.**

So the cost is HUGE, we need better privacy policies





# Short structured privacy policy

- Write the privacy policy in a structured format
  - Personal information collected by XYZ corporation?
  - Why? What? How?
- Force all companies address same questions
  - Have a table with rows on who would these companies share your person with with and columns as Yes/No

# Issues

- Requires policy makers to make laws and set standards
- Must decide what factors people care about before the standard is created
- Nuances are lost
  - And people still don't normally read these

# Issues

15:43 0.01 KB/s 44%

airtel.in/privacy-policy/

airtel Airtel Store Login

and/or representatives of the Third party.

We may also collect your personal information when you use our services or websites or otherwise interact with us during the course of our relationship.

Personal information collected and held by us may include but not limited to your name, father's name, mother's name, spouse's name, date of birth, current and previous addresses, telephone number, mobile phone number, email address, occupation and information contained in the documents used as proof of identity and proof of address. airtel and its authorized third parties may collect, store, process following types of Sensitive Personal Information such as Genetic Data, Biometric Data, Racial or Ethnic Origin, Political opinion, Religious & Philosophical belief, Trade union membership, Data concerning Health, Data concerning natural personal's sex life or sexual orientation, password, financial information (details of Bank account, credit card, debit card, or other payment instrument details), physiological information for providing our products, services and for use of our website. We may also hold information related to your utilization of our services which may include your call details, your browsing history on our website, location details and additional information provided by you while using our services.

We may keep a log of the activities performed by you on our network and websites by using various internet techniques such as web cookies, web beacons, server log files, etc. for analytical purposes and for analysis of the amiability of various features on our site. This information may be used to provide you with a better experience at our portal along with evidentiary purposes. At any time while you are browsing our site, if you do not wish to share browsing information, you may opt out of receiving the cookies from our site by making appropriate changes to your browser privacy settings. Please

# Issues

“Personal information collected and held by us may include but not limited to your name, father’s name, mother’s name, spouse’s name, date of birth, current and previous addresses, telephone number, mobile phone number, email address, occupation and information contained in the documents used as proof of identity and proof of address. airtel and its authorized third parties may collect, store, **process following types of Sensitive Personal Information such as Genetic Data, Biometric Data, Racial or Ethnic Origin, Political opinion, Religious & Philosophical belief, Trade union membership, Data concerning Health, Data concerning natural personal's sex life or sexual orientation, password**, financial information (details of Bank account, credit card, debit card, or other payment instrument details), physiological information for providing our products, services and for use of our website. We may also hold information related to your utilization of our services which may include your call details, your browsing history on our website, location details and additional information provided by you while using our services.”

- Airtel changed it after the backlash two months back
- [https://www.reddit.com/r/india/comments/jc40d7/airtels\\_privacy\\_policy/](https://www.reddit.com/r/india/comments/jc40d7/airtels_privacy_policy/)

# Issues

- Requires policy makers to make laws and set standards
- Must decide what factors people care about before the standard is created
- Nuances are lost
  - And people still don't normally read these

# Another approach: P3P

- Idea: make privacy policies machine readable and compare if the policies match user expectation
  - Platform for privacy preferences (P3P)
  - Machine readable structured privacy policy
  - Sent by web servers when you visit a domain, parsed by a browser
  - Didn't really take off
    - IE implemented it
    - Google's domain evaded it

# Problem with P3P: human vs. machine

- IE checked P3P policies
  - Google sends the following policy

P3P:CP="This is not a P3P policy!"

See <http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=15165>  
for more info."

- Valid policy for machines, of course invalid policy for humans
- FB does the same:  
[https://www.techpolicy.com/Cranor\\_InternetExplorerPrivacyProtectionsBeingCircumvented-by-Google.aspx](https://www.techpolicy.com/Cranor_InternetExplorerPrivacyProtectionsBeingCircumvented-by-Google.aspx)



# Okay, so what do we do?

- Work on using ML + text analysis to mine privacy policies
  - Client side
- Privacy policy is reflective of data collection/storage/process practices in your system (Designer side)
  - Use privacy by design

# Privacy by design

- **Minimize**: Limit the processing of personal data.
- **Separate**: Separate processing of personal data
- **Abstract**: Limit the granularity in which personal data is processed.
- **Hide**: Protect personal data, or make it unlinkable or unobservable.
- **Inform**: Inform data subjects about data processing in timely and adequate manner
- **Control** : Provide data subjects control over the data processing
- **Enforce** : Enforce processing personal data in a privacy-friendly way
- **Demonstrate** : Demonstrate you are processing personal data in a privacy-friendly way

# Roadmap

- Security advice
- Security and privacy warnings
- Dark patterns
- Privacy consent
- **Inclusive security and privacy**

# Some considerations for inclusivity

- Cognitive impairments
  - Illiteracy
  - Difficulty in remembering
- Visual impairments
  - Sightedness
  - Color-blindness
- Dexterity impairments
- Hearing impairments

# Screen readers

- software program that allows blind or visually impaired web users to “read” the content of a page with either a speech synthesizer or braille display.
- user will send commands to the screen reader interface by pressing different keys on their keyboard or braille display
- But as a designer you might want to make your system easier for screen readers

# Solution : “alt” text

- ``
- Used by screen-readers for visually impaired people

# Solution : video captions/subtitles


YouTube Help

🔍 Describe your issue

## Add your own closed captions

Closed captions allow you to share your videos with a larger audience, including deaf or hard-of-hearing viewers and viewers who speak another language. If you already have captions, get help [editing or removing existing captions](#).

### Create closed captions

1. Sign in to [YouTube Studio](#) .
2. From the left menu, select **Subtitles**.
3. Click the video that you'd like to edit.
4. Click **ADD LANGUAGE** and select your language.
5. Under subtitles, click **ADD**.

---

[Upload a file](#)



# Solution : design fonts and text for accessibility

- Websites / apps should still work when magnified to a large size
- Don't use color to convey meaning
  - Screen readers do not interpret it
- Use high-contrast color combinations
- Don't include placeholders in form fields
- Make form fields easy to find



# Make your text accessible

- Standard metrics for measuring readability of text
  - [https://en.wikipedia.org/wiki/Readability#Popular\\_readability\\_formulas](https://en.wikipedia.org/wiki/Readability#Popular_readability_formulas)
- Follow accessibility guidelines
  - <https://developer.gnome.org/accessibility-development-guide/stable/gad-ui-guidelines.html.en>

# More inclusivity: Age

- Facebook requires the users to be 13 before signing up
  - Why is 13 a magic number?
  - Simple: COPPA says parental consent is needed before that
  - Protecting security/privacy of young users is challenging

# More inclusivity: Age

- Facebook requires the users to be 13 before signing up
  - Why is 13 a magic number?
  - Simple: COPPA says parental consent is needed before that
  - Protecting security/privacy of young users is challenging
- Senior citizen – a different challenge
  - Knowledge of technology?
  - Different mental models (due to different experiences)?
  - Particular vulnerability to scams

# More inclusivity: Culture

- What is culture?
  - Country?
  - Demographics?
- Why does culture matter in usable security and privacy research?
  - Social norms
  - Laws
  - Infrastructures
  - Attack models

———— THE END ————

Best of luck for the exam!