Privacy

CSC 326



© NC State Software Engineering Faculty

1

Basics about Privacy

2

Impact of Digitalization to Privacy Crisis



3

3

Why do we care about privacy?

Much of what we do in today's society involves information exchange

- e.g. government, commerce, healthcare

For people to be comfortable and willing to take full advantage of IT services we need to:

- Safeguard their privacy
- **Let them understand we're safeguarding their privacy**

"Americans Have Overwhelming Disdain For Personal Data Collection" [IAPP News, 12 Oct 2005]

- "A CBS/New York Times poll found that **83% view growing databases of personal information as a bad thing.**"

© NC State Software Engineering Faculty

4

4

Why is privacy important?

Privacy helps us maintain our:

- Individuality
- Autonomy
- Freedom of choice

Anonymity is one form of protection of our privacy

Once lost it can seldom be fully recovered!

© NC State Software Engineering Faculty

5

Privacy



- Privacy
  - **The right to be left alone**
  - Control over what information about you is revealed, and to whom
- Invasions of Privacy
  - Private facts (disclosing non-public information)
  - Intrusion (intrude into private affairs)
  - Appropriation (acquiring name or photos)
  - False light (make look inappropriately bad to public)

© NC State Software Engineering Faculty
https://www.buzzfeed.com/claudiarosenbaum/downfall-of-the-paparazzi?utm_term=.jlkMBnD3GK#.ydRByDE948

6

Computer systems are the key



- Systems can either protect privacy or not …
- A system may enable the revealing of private information because we didn't think about privacy protection and who would want the data
- We need to think about it …

© NC State Software Engineering Faculty

7

Personally Identifiable Information (PII)



© NC State Software Engineering Faculty

8

Personally Identifiable Information (PII)

- Name
- All geographic subdivisions smaller than state
- Birth date
- Telephone/Fax numbers
- E-mail addresses
- Social Security Number
- Medical Record Number
- Health Plan Number
- Account Number
- Certificate / license number
- Vehicle identifier/serial number
- Device identifier/serial number
- Uniform Resource Locators (URLs)
- IP addresses
- Biometric identifiers
- Photos
- Other unique characteristics
- Full face photograph





© NC State Software Engineering Faculty

Rosie Callender, RHIA, web.msm.edu/**hipaa**/An%20**Intro**duction%20to%20**HIPAA**.**ppt**

9

9

Privacy Policy



10

10

Privacy Policy

- A **privacy policy** is a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data.
- A **privacy policy** fulfills a legal requirement to protect a customer or client's privacy.

- **… a system's implementation must comply with its privacy policy … which is not trivial … a stated requirement may be non-compliant**

© NC State Software Engineering Faculty https://en.wikipedia.org/wiki/Privacy_policy

11

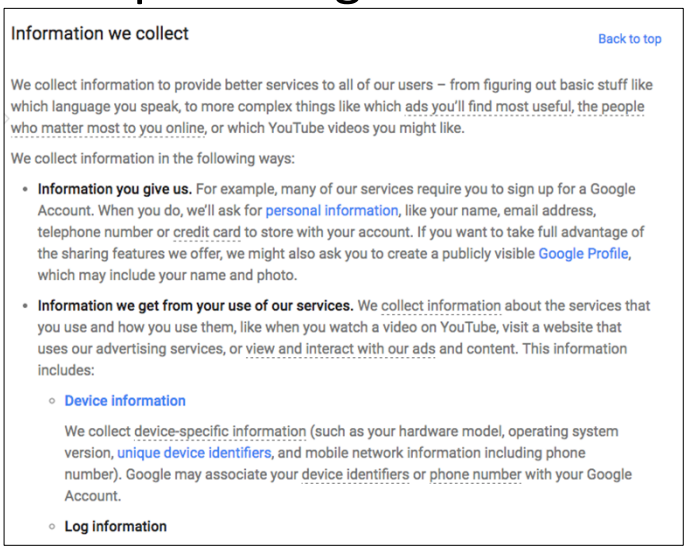
Better Business Bureau Template for **Privacy Policy**

- **Policy** (what personal information is being **collected** on the site)
- **Choice** (what **options** the customer has about how/whether their data is collected and used)
- **Access** (how a customer can **see** what data has been collected and change/correct it if necessary)
- **Security** (state how any data that is collected is stored/**protected**)
- **Redress** (what customer can do if privacy policy is **not met**)
- **Updates** (how policy **changes** will be communicated)

© NC State Software Engineering Faculty https://www.bbb.org/dallas/for-businesses/bbb-sample-privacy-policy1/

12

Example: Google



Information we collect

Back to top

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like.

We collect information in the following ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.
- **Information we get from your use of our services.** We collect information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or view and interact with our ads and content. This information includes:
  - **Device information**

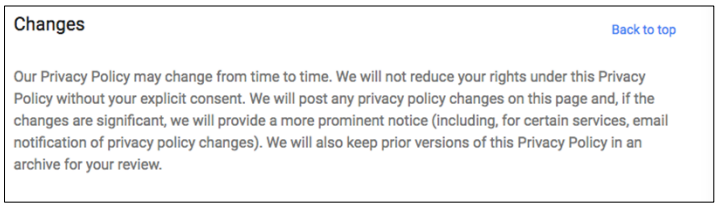
    We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.
  - **Log information**

Policy
Choice
Access
Security
Redress
Updates

© NC State Software Engineering Faculty

https://www.google.com/policies/privacy/

Example: Google



Changes

Back to top

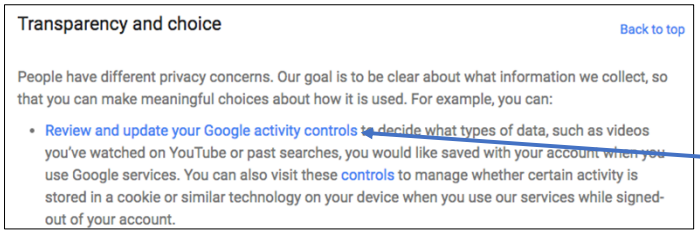
Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Policy
Choice
Access
Security
Redress
Updates

© NC State Software Engineering Faculty

https://www.google.com/policies/privacy/

Example: Google



Policy
Choice
Access
Security
Redress
Updates

© NC State Software Engineering Faculty

https://www.google.com/policies/privacy/

Privacy Policy Exploration

Exercise 18.01: Privacy Policy Exploration

- Identify the template categories for the privacy policy statements

© NC State Software Engineering Faculty

Freedom for a system's privacy policy

- Some of the policy is up to the discretion of the system author/owner
  - Business model related to data
  - What customers will tolerate
- Some of the privacy policy is stipulated, e.g.
  - Fair Information Practices (more on this)
  - COPPA (kids)
  - HIPAA (health)
  - GLBA (finance)
  - …

© NC State Software Engineering Faculty

Code of Fair Information Practices (FIPs) - 1

FIPs are **a set of internationally recognized practices** for addressing the privacy of information about individuals*

- No <u>secret</u> personal data record-keeping systems

* U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)

© NC State Software Engineering Faculty
http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

Code of Fair Information Practices (FIPs) - 2

- A person must be able to find out what information about the person is in a record and how it is used.
- A person must be able to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

* U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)

© NC State Software Engineering Faculty
http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

Code of Fair Information Practices (FIPs) - 3

- Must be a way for a person to correct or amend a record of identifiable information about the person.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

© NC State Software Engineering Faculty
http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

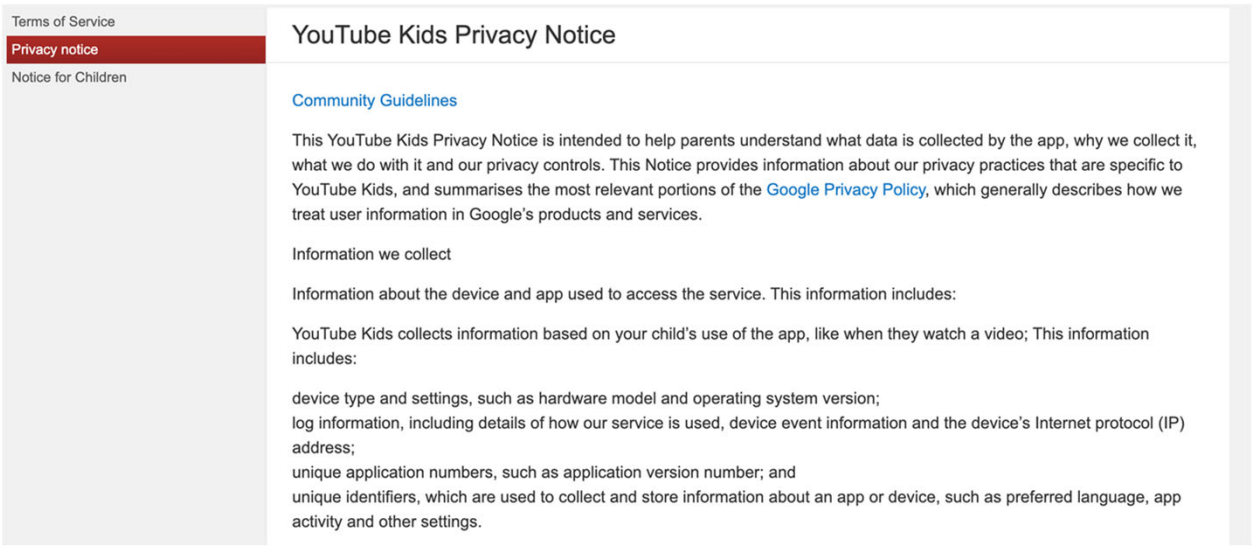
Children's Online Privacy Protection Act (COPPA)

- Applies to the online collection of personal information for those **under 13**.
- Operators must:
  - Clear and comprehensive online privacy policy
  - Obtain parental consent prior to any collection
  - Provide a way for a parent to review collected data
  - Ensure technical security of collected data

© NC State Software Engineering Faculty

https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

21



https://kids.youtube.com/t/privacynotice

22



23

23

Healthcare Privacy: HIPAA

- In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA).
- Three components:
  - Protection for the privacy of Protected Health Information (PHI – more on this)
  - Protection for the security of Protected Health Information
  - Standardization of electronic data interchange in healthcare transactions

© NC State Software Engineering Faculty

24

24

Protected Health Information (PHI)

- PHI is any health information that can be used to identity a patient and that relates to the patient, health care services provided to the patient, or the payment for these services
- PHI includes
  - All medical records and other information that identifies the patient, including demographic, medical, and financial information
  - The above information in any form – electronic, paper or spoken

© NC State Software Engineering Faculty

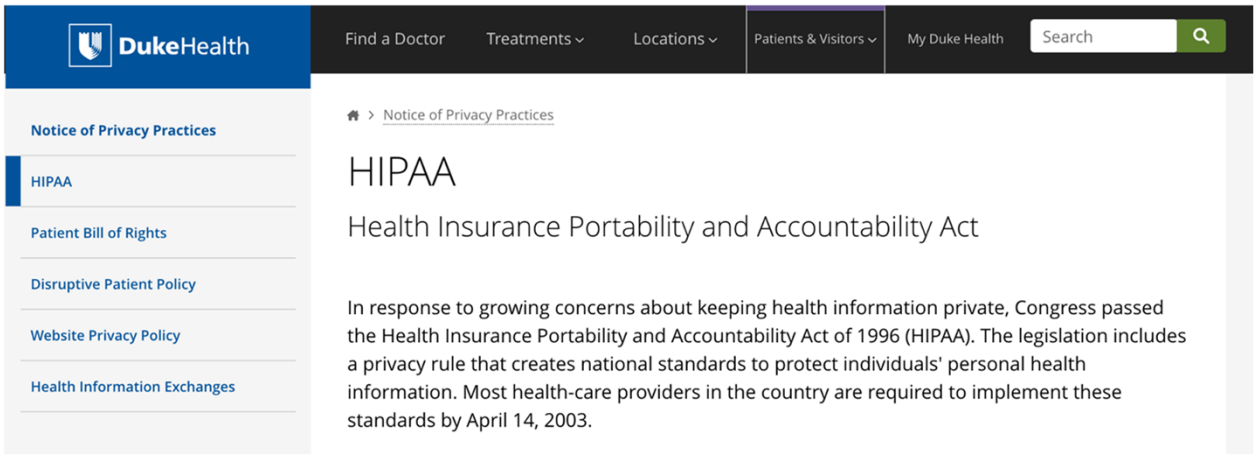
25

PENALTIES For Non-compliance

	Monetary Penalty	Term of Imprisonment	Offense
CIVIL PENALTIES	$100	N/A	Single violation of provision
	Up to $25,000	N/A	Multiple violations of identical requirement or prohibition made during the calendar year
CRIMINAL PENALTIES	Up to $50,000	Up to one year	**Wrongful disclosure** of individually identifiable health information
	Up to $100,000	Up to five years	**Wrongful disclosure** of individually identifiable health information committed under false pretenses
	Up to $250,000	Up to 10 years	**Wrongful disclosure** of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm

© NC State Software Engineering Faculty

26



https://www.dukehealth.org/privacy/HIPAA

27

27

Technical Requirements of HIPAA

- **Access Control**. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).
- **Audit Controls**. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- **Integrity Controls**. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
- **Transmission Security**. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

© NC State Software Engineering Faculty

http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

28

28

Financial Privacy: GLBA

- **The Gramm-Leach Bliley Act (GLBA)** of 1999 includes provisions to protect consumers' personal financial information held by financial institutions.
- **Financial institutions** include: banks, securities firms, insurance companies, and companies providing many other types of financial products and services to consumers (such as lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns).
- There are three principles parts:
  - Financial Privacy Rule
  - Safeguards Rule
  - Pretexting Provisions

© NC State Software Engineering Faculty

GLBA-2

- **Financial Privacy Rule** governs the collection and disclosure of customers' "non-public" personal financial information
  - requires companies to give consumers privacy notices that explain the institutions' information-sharing practices.
  - consumers have the right to limit some - but not all - sharing of their information.
- **The Safeguards Rule r**equires all financial institutions to design, implement and maintain safeguards to protect customer information.
- The **Pretexting** provisions protect consumers from individuals and companies that obtain their personal financial information under false pretenses
  - Linked to identity theft
  - Often social engineering

© NC State Software Engineering Faculty

Example: Wells Fargo, privacy for individuals

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 employment information
- Account balances and transaction history
- Credit history and investment experience

Policy
Choice
Access
Security
Redress
Updates

© NC State Software Engineering Faculty
https://www.wellsfargo.com/privacy-security/privacy/individuals/

Example: Wells Fargo, privacy for individuals

Reasons we can share your personal information	Does Wells Fargo 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 — with service providers we use to offer our products and services to you (please see below to limit the ways in which we contact 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

Policy
Choice
Access
Security
Redress
Updates

© NC State Software Engineering Faculty
https://www.wellsfargo.com/privacy-security/privacy/individuals/

Example: Wells Fargo, privacy for individuals

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. For more information, visit wellsfargo.com/privacy-security

Privacy Policies and Notices

Understand how we use and protect personal information.

- Wells Fargo U.S. Consumer Privacy Notice
- Digital Privacy and Cookies Policy
- Social Security Number Protection Policy
- Wells Fargo Financial National Bank Privacy Notice (PDF)
- Wells Fargo Bank, N.A. Dillard's Privacy Notice (PDF)
- Health Information Notice
- Wells Fargo International Privacy Notices
- Wells Fargo Insurance, Inc. Privacy Notice (PDF)

Policy
Choice
Access
Security
Redress
Updates

© NC State Software Engineering Faculty

https://www.wellsfargo.com/privacy-security/privacy/individuals/

EU General Data Protection Regulation (GDPR)

- Data protection rules for the European Union (May 2018)
  - People control their personal data
  - Level-playing field for businesses (all follow the same regulation)

© NC State Software Engineering Faculty



35

35

Principles of GDPR

The type and amount of personal data a company/organisation may process depends on the reason for processing it (legal reason used) and the intended use. The company/organisation must respect several key rules, including:

- personal data must be processed in a **lawful and transparent manner**, ensuring fairness towards the individuals whose personal data is being processed ('lawfulness, fairness and transparency');
- there must be **specific purposes** for processing the data and the company/organisation must indicate those purposes to individuals when collecting their personal data. A company/organisation can't simply collect personal data for undefined purposes ('purpose limitation');
- the company/organisation must collect and process **only the personal data that is necessary to fulfil that purpose** ('data minimisation');
- the company/organisation must ensure the personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and correct it if not ('accuracy');
- the company /organisation can't further use the personal data for other purposes that aren't **compatible** with the original purpose;
- the company/organisation must ensure that personal data is **stored for no longer than necessary** for the purposes for which it was collected ('storage limitation');
- the company/organisation must install appropriate **technical and organisational safeguards** that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology ('integrity and confidentiality').

From: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en

© NC State Software Engineering Faculty

36

36

GDPR – Rights for Individuals

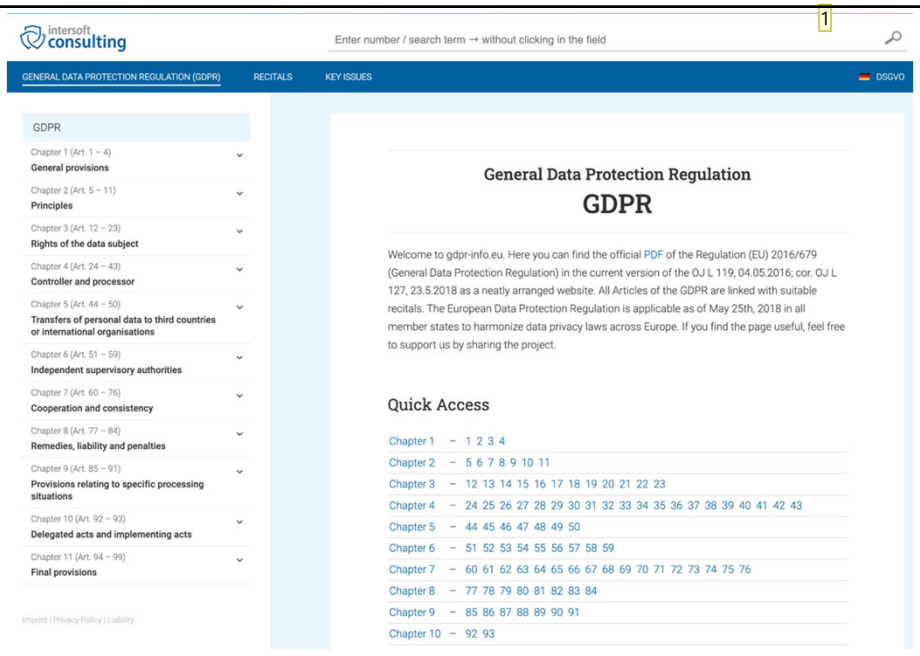
You have the right to:

- **information** about the processing of your personal data;
- **obtain access to** the personal data held about you;
- ask for incorrect, inaccurate or incomplete personal data to be **corrected**;
- request that personal **data be erased** when it's no longer needed or if processing it is unlawful;
- **object** to the processing of your personal data for marketing purposes or on grounds relating to your particular situation;
- request the **restriction** of the processing of your personal data in specific cases;
- receive your personal data in a machine-readable format and send it to another controller ('**data portability**');
- request that decisions based on **automated processing** concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision.

From: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en

© NC State Software Engineering Faculty

37



https://gdpr-info.eu/

38

Slide 38

1 newly added
Bowen Xu, 3/19/2024

2



Legal Notice

A. Fulfillment of the contractual obligation to provide updates for software used in vehicles (Art. 6(1) lit. (b) GDPR)

For the provision of this service, the following potentially personal information is processed for the provision of services by BMW and commissioned service providers:

- Contact Data (e.g. IP address)
- Unique visitor ID
- Geolocation
- Account Data (e.g. VIN)

https://www.bmw.com/en/footer/legal-notice.html#:~:text=We%20will%20take%20reasonable%20measures,in%20place%20to%20support%20this.

39

39

Up to the discretion of the company

- Business model
- Customer tolerances
- Privacy settings/options
- Opt in – Opt out (what is the default?)
- Readability of policy
  - "A privacy policy that consumers are unlikely to read or understand provides no protection whatsoever." (Center for Plain Language, non-profit)

© NC State Software Engineering Faculty

40

40

Slide 39

2 newly added, lead student to read BMW's privacy policy and link to GDPR.
Bowen Xu, 3/19/2024

Policies/Standards vs. Requirements

Similarities

- express desire or worth, rather than fact
- primarily statements in the optative mood, they specify what must or ought to be done

Differences

- scope of policies is broader than requirements and standards often have legal implications
- privacy policies and standards are more charged with societal values
- policies and standards are more open-ended than requirements
- requirements cover one system; policies often cover several and standards cover many

Alignment

- Need to bring policy, stakeholder values, requirements, and standards into agreement

© NC State Software Engineering Faculty

41

Create your own privacy policy

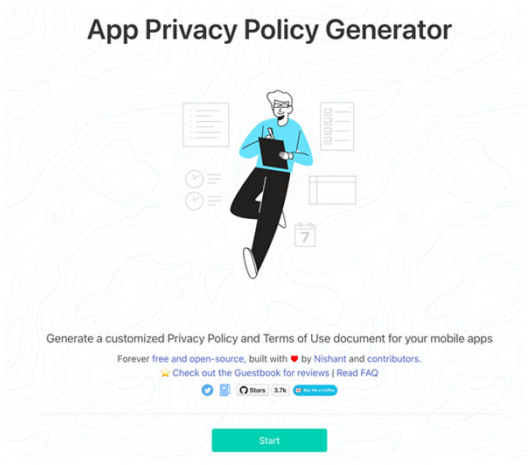
42



43

43

Play with Template-based Policy Generator



1. Identify at least one limitation of generated policy based on what you learned today.
2. Share the limitations.

https://app-privacy-policy-generator.firebaseapp.com/

44

44

Using AI for writing privacy policy

1. Think about an application in your mind.
2. Tell AI tool (your choice) as much as you can about what is your application.
3. Ask AI tool to generate a privacy policy to you.
4. Identify at least one limitation of AI-generated policy based on what you learned today.
5. Share the limitations.
6. Are the limitations different for different AI tools?

Exercise 18.02: Template vs. AI-based Privacy Policy Generator

45

45

Team Project: Better Business Bureau Template for **Privacy Policy**

- **Policy** (what personal information is being **collected** on the site)
- **Choice** (what **options** the customer has about how/whether their data is collected and used)
- **Access** (how a customer can **see** what data has been collected and change/correct it if necessary)
- **Security** (state how any data that is collected is stored/**protected**)
- **Redress** (what customer can do if privacy policy is **not met**)
- **Updates** (how policy **changes** will be communicated)

Your Team Project Privacy Policy should NOT use AI or Template tools. You should have these ^ items in the one you write.

© NC State Software Engineering Faculty

https://www.bbb.org/dallas/for-businesses/bbb-sample-privacy-policy1/

46

46