Edge Computing

Lecture 9: Ethics, Privacy & Security

Recap

- Paper presentations
  - + diverse topics,
    - Workout detection, agriculture, smarthome, etc.
  - + going above and beyond the class,
    - CNN, FedML, LSTM, TinyML, Efficient ML, etc.
  - + good practice of getting to know the topic/field you are working on
    - use as reference, baseline for comparison in your final project
  - + presentation skills
    - volume, pace, clarity, animation, flow, timing

Agenda

- Ethics
  - ACM, IEEE, code of conduct
- Privacy & Security
  - GDPR
  - CCPA

ACM Code of Ethics and Professional Conduct

- ACM: Association for Computing Machinery
  - Largest scientific and educational computing society (they have student memberships ;-))
- IEEE: Institute of Electrical and Electronics Engineers
  - Largest technical professional organization dedicated to advancing technology for the benefit of humanity (they have student memberships too ;-))
- *“The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way.”*
- ACM Code of Ethics and Professional Conduct
- IEEE Code of Conduct

Ethical Principles

1. Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
2. Avoid harm
3. Be honest and trustworthy
4. Be fair and take action not to discriminate
5. Respect the work required to produce new ideas, creative works, and computing artifacts
6. Respect privacy
7. Honor confidentiality

Example

- Say you are given the task of designing a security system that will detect if a person whose face matches a face from a criminal database. The system will have several cameras and send the information to a cloud server. The user will receive a report and video of people had positive matches.

- Which codes could be broken and how can you mitigate it?

Privacy & Security

- Security has a broad meaning within computer science. For this scope we focus on personal data security, keeping personal data secured

- Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

The Law

- Unlike a Code of Ethics, privacy and security are required and guidelines by law and therefore enforceable.

LAW

- EU General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)

General Data Protection Regulation (GDPR)

Implemented in 2018, its objectives are:

- Modernize EU’s legal system in response to new technologies
- Strengthen the user’s data ownership
- Improve the clarity and coherence of current rules

EU Law?

- GDPR applies for any business that interacts with EU residents regardless of origin
- It establishes a framework and design requirements from early phases of development
- Countries rapidly implemented their own regulation modeled after GDPR

Terms in GDPR

- Personal Data
- Data Subject
- Controller
- Processor

16.4.1.1 Personal Data

It could be any information relating to an identified or identifiable natural person such as name, identification number, location data, and online identifier or to one or more indicators specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

16.4.1.2 Data Subject

The subject is a natural person, who is identified or identifiable. The identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to his or her personal data.

16.4.1.3 Controller

A natural or legal person, public authority, agency or other body can play this role. This new element under the GDPR is that the controller determines also the conditions of the processing of personal data.

16.4.1.4 Processor

The processor is also an important actor, who is also a natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.

Terms in GDPR

- Pseudonymization
- Limitation
- Consent

16.4.1.5 Pseudonymization

It is a new term, which means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

16.4.1.6 Limitation

What has a great importance among the principles relating to personal data processing is the limitation. Purpose of the collection, the quality of the data, and the duration of the storage are all limited based on their necessity. New elements are, in particular, the transparency principle, the clarification of the data minimization principle, and the establishment of a comprehensive responsibility and liability of the controller.

16.4.1.7 Consent

In order for personal data processing to be lawful, it has to be on the basis of the consent of the data subject for one or more specific purposes. The processing should be necessary for the performance of a contract in which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. More specifically:

Terms in GDPR

- Right to be forgotten
- Data Portability

16.4.1.8 Right to Be Forgotten

The GDPR further elaborates and specifies the data subject's right of erasure and provides the conditions of the right to be forgotten, when the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. Another case is when the data subject withdraws consent on which the processing is based, or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data.

16.4.1.9 Data Portability

The GDPR introduces the data subject's right to data portability (i.e. to transfer data from one electronic processing system to, such as a social network, into another, without being prevented from doing so by the controller). As a precondition and in order to improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format. This option could apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.

GDPR Principles

- Transparent processing
- Limitation of collected data
- Minimize collected and stored data
- Personal data must be accurate
- Limit storage of personal data
- Integrity and confidentiality
- Accountability

https://www.progress.com/blogs/gdpr-eu-personal-data

GDPR Obligations

- The controller must identify itself, the purpose of data collection and all parties that will have contact with it
- The processor must only act under the controller’s supervision and under strict confidentiality, and have a mechanism for data deletion at the controller’s demand
- Both work together to ensure compliance
- Any security breach or risk of breach must be communicated to the Data Subject within 72 hours

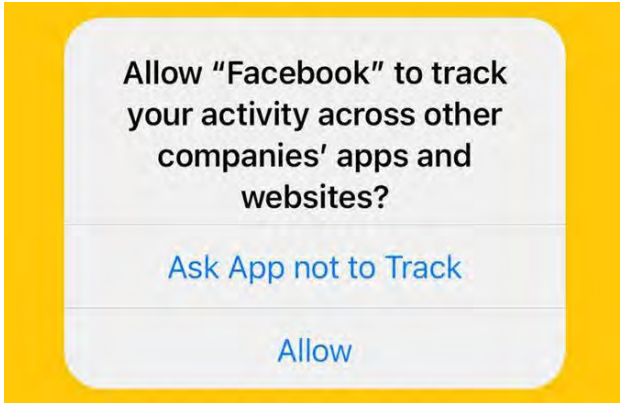
GDPR Impact

- Meta
  - Charged $1.5B from nine cases
    - Data collection practices
    - Mishandling children’s data
    - Leaks…
- Tiktok
  - Charged $16.7M
- Amazon
  - Charged 748M euros
- Google
  - Charged 216M euros

https://observer.com/2023/05/gdpr-europe-meta-fines/

GDPR Impact

- Some free services profit from data
  - Selling personal data
  - Targeted advertising



- Google’s [statement]

We don’t sell your personal information to anyone

We use your personal information to make our products more helpful to you. It’s how we can autocomplete your searches, get you home faster with Maps, or show you more useful ads based on your interests. But we never sell your personal information to anyone and you can use many of our products without signing in or saving any personal information at all.

California Consumer Privacy Act (CCPA)

- Signed a month after GDPR’s implementation, went into effect on January 1st, 2020.
- There are a lot of ideological similarities with GDPR, though the way they are implemented are slightly different
- Note that businesses that interact with residents of California, and the EU, must abide to both laws

GDPR vs CCPA: Key Differences

CCPA adds the following as some of the key differences to GDPR:

- The subject has a right to know and access all the data is being collected from them
- At any time, the subject can opt-out from selling or profiting from their information
- Services must be equal regardless of consent
- Users 13-16 must provide consent while users under 13 require the parent’s consent
- Only businesses that earn $25 MIL or more, has more than 50k consumers, or more than 50% of their profit comes from selling information, must comply

Summary

- Ethics
  - ACM, IEEE, code of conduct
- Privacy & Security
  - GDPR
  - CCPA

Week	Day	Date	Lecture	Lab Issue Date	Lab Due (End of Day)	Project Due (End of week)
1	Mon	01/06	Introduction			
	Wed	01/08	Edge Computing and Its Applications	Lab 0: Setup		
2	Mon	01/13	Edge Systems: Architecture			
	Wed	01/15	Edge Systems: Design and Optimization	Lab 1: Profiling Tools for Jetson	Lab 0	
3	Mon	01/20	Holiday	Final Project Description		Exam 1
	Wed	01/22	Edge ML: Basics of ML	Lab 2: Object Recognition	Lab 1	
4	Mon	01/27	Edge ML: Quantization and Pruning			Proposal
	Wed	01/29	Edge Computing Hardware: Architectures	Final Project Consultation		
5	Mon	02/03	Edge Computing Hardware: Special Accelerators	Lab 3: Client-Server Communica	Lab 2	Paper Pres.
	Wed	02/05	Edge & Cloud: Middleware			Slides & Quiz
6	Mon	02/10	Paper Presentation			
	Wed	02/12	Paper Presentation	Lab 4: Connecting to the Cloud	Lab 3	
7	Mon	02/17	Holiday			Deployment
	Wed	02/19	Paper Presentation			
8	Mon	02/24	Ethics, Privacy & Security		Lab 4	
	Wed	02/26	Edge Computing Research			
9	Mon	03/03	Project Presentation			
	Wed	03/05	Project Presentation			
10	Mon	03/10	Project Presentation			Report
	Wed	03/12	Project Presentation			

Next Lectures

- Guest lecture(s)
- Final presentations
  - Week 9-10