Privacy & GDPR

The regulation of privacy is a continuous attempt to find a balance between freedom of speech and the material protected by privacy. But what does privacy protect? The first definition of privacy as it is intended today in the U.S. was proposed in the year 1890 in an article by Warren & Brandeis. In this paper, "The Right to Privacy", privacy was pictured as "a right to be let alone".

During the 1960s, two points of privacy view can be delineated: one expressed by the U.S. Supreme Court (1965, Griswold v. Connecticut), and the other by Prof. Prosser (1960, Privacy, 48 Call. L. Rev. 383). While the Court believed that the right to privacy was implicitly guaranteed by the Constitution, Prof. Prosser elaborated on this right by discussing four major domains: identity theft, false light in the public eyes, publication of private facts, and intrusion.

False light in the public eye means the untruthful depiction of an individual, e.g. in the Lega Nord example, while for intrusion an example was given about an Italian newscaster that was photographed while sunbathing.

During class, also the fifth dimension of oblivion was introduced by citing the case of the republication of a news article of a man who was convicted of murder decades before. The newspaper was sued and lost since that republication did not contain any information not useful to the public and as such the right to oblivion applied to the murderer.

On the other hand, the first European unified expression of privacy came in the early 1980s, and it was published in the European Convention on Human Rights (ECHR). In particular, article 8 §2 reads that everyone has a right to respect for his private and family life, but also, §2 reads that such right holds between individuals and authorities, and it is not specified to which extent it applies between fellow individuals.

Meanwhile, in Italy, a right to privacy was enforced thanks to the interpretation of the laws that protected name, public image, honor, and reputation.

To harmonize the legislation of the European states, the European Community introduced a directive in 1995 on the protection of individuals' personal data and the free movement of such information. This directive was put in place to level the field between corporations that reside in different states. Everyone must manage data in the same way.

After this first directive, the General Data Protection Regulation (GDPR) was approved in 2016. The articles discussed during class are the following:

- `article 4`: contains 26 definitions, such as the ones of "personal data", "processing", "pseudonymization", and "consent".
- `article 5`: describes the principles to abide by while processing personal data. Also, the contraposition of transparency in computer science and law was discussed during class. Furthermore, the case of Cambridge Analytica was introduced as a violation of art.5 §1 letter B. Finally, the case of Zoom was discussed as a violation of "data minimization".
- `article 9`: prohibits the processing of personal data. Exceptions are made and listed in §2.
- `article 16`: force the data controller to rectify any untruthful data about a given individual that asks for such rectification.
- `article 17`: enables an individual to ask the data controller for the erasure of personal data whenever such data are no longer necessary to the relation between the controller and the individual.
- `article 25`: defines generic guidelines to follow when implementing privacy in a system. In short, judges will try to balance the requirements of privacy by design and the costs of designing the processing implementation that fulfills these requirements.

Software as a Service (SaaS)

Traditional IT services and infrastructures come with a high cost of maintenance, updates, disaster recovery, and management. For such reasons, in recent years SaaS gained a lot of popularity. This

distribution model can outsource infrastructures, e.g. AWS, platforms, e.g. NextCloud, and services, e.g. e-mail services.

Outsourcing limits the expenses above listed but comes at a price. Other than the fee one must pay to the provider of the service, one can't access the source code of the outsourced software, and lose some control over the data shared with the service provider. Furthermore, the service is not accessible when offline, and also, integration with local systems is usually far from simple, see SAP as an example.

Software patents

Patents are fundamentally different from copyright. Patents protect an idea, and copyright is a tangible expression of said idea. Copyright applies as default, patents are granted by state offices and are subject to fees. Copyright lasts longer than patents. Furthermore, to obtain a patent, the invention must be disclosed to verify if the inventor is eligible for a patent.

Software patentability has been a reason for discussion since the 1970's. During this decade, the United States Patent and Trademark Office(USPTO), deemed all the inventions that were the product of a computer calculation not patentable. This state line remained unchallenged until 1981 when the sentence of the U.S. Supreme Court in the court case Diamond v. Diehr. The court ruling stated that algorithms are not patentable, but devices using such algorithms are.

Successively, in 1994, the United States Court of Appeals for the Federal Circuit (Fed.Cir.) in the legal case In re Alappat, 33 F.3d 1526, ruled that a general-purpose computer programmed for a specific task could be patented.

Finally, in 1996 the USPTO issued the Final Computer Related Examination Guidelines establishing the guidelines for software patentability.

Differently, in Europe, Article 52 of the European Patent Convention(EPC) excludes software from patentability but still deems inventions that make a non-obvious contribution to non-obvious technical problems in a non-obvious way patentable even if the solution is found by running a computer program.

Digital Right Management & Trusted Computing

In the States, DRM systems are regulated by Article 11 and Article 12, §1 and §2, of the WIPO Copyright Treaty of 1996. In particular, Article 11 binds member states into providing legal protection against the circumvention of DRM systems. Furthermore, Article 12 §1 and §2 protect against the illegal modifications of the right management information, i.e. the digital translation of the distribution license.

Meanwhile, in the EU, the WIPO Treaty is implemented via the European Directive 2001/29/EC. In particular, Article 6 §1 and §2 grant similar protection to the WIPO ones discussed above.

In the same class, also an introduction to Trusted Computing and TPM was given. The Trusted Platform Module is a protected memory area where (some) certificates used to sign software are stored. These certificates are used to ensure the integrity of the software that is being loaded in memory. Furthermore, a significant part of the discussion was about remote attestation and its implications. In short, remote attestation enables a remote third party to check the certificates and signature of a given application, see the example provided for the use of the FM chip in cell phones under Italian legislation. In the end, while this technology ensures high levels of integrity, it also is a menace to the liberty of action (lawful or unlawful) that the end-user should have over his property, i.e. the device.

Computer Ethics

Ethics is a branch of philosophy that deals with what is morally right or wrong. Computer Ethics is an application of ethics to Computer Science. During this last lecture, not only an introduction to ethics was proposed, but also time for reflection and brainstorming was allocated to discuss what our views and opinions on ethics were.