Warren & Brandeis (1890)

- *"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone"*
- *Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons;*

What is it?

- The right to be let alone
- The right to individual autonomy
- The right to a private life
- The right to control information about oneself
- The right to limit accessibility
- The right to minimize intrusiveness
- The right to secrecy
- The right to enjoy solitude
- The right to enjoy intimacy
- The right to enjoy anonymity

A. F. Westin

- Defined privacy as
  - "The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others"

Privacy as a social value (A.F. Westin)

- Autonomy
  - "The most serious threat to individual's autonomy is the possibility that someone may penetrate the inner zone and learn his ultimate secrets, either by physical or psychological means. This deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who knew his secrets"

Privacy as a social value (A.F. Westin)

- Self evaluation and decision making
  - Solitude and the opportunity for reflection are essential to creativity.
  - If every conversation among organizational leaders, if every draft memo, if every proposal for action were public, frank discussion would be severely inhibited and thoughtful decision making undermined

Privacy as a social cost (A.F. Westin)

- Privacy can conflict with other important values within the society:
  - Preventing and punishing crime
  - Figthing against terrorism
  - It facilitates the diffusion of false and misleading information

Our society

- People demand:

  - high-speed transactions

  - high-level personalised service

  - high usability and interconnectivity of products

  - anywhere, anytime, technology

- Individuals have been eager to "explore new opportunities of the digitisation in everyday life", TRADING DATA FOR PRODUCTS AND SERVICES

Personally Identifiable Information

- *PII* allow the immediate identification of a person: address, code, credit card number, name, phone number, etc
- *Non-PII* not entirely sufficient to identify a person: personal preferences such as books read, movies, music, food, gender (male/female)
- *Location Data* again, the data is not sufficient to identify a person: a certain place is usually shared by multiple people,
- *Device/Network Data* not sufficient to identify a person: IP address, mac address, mail address

We constantly give up data about ourselves

- Closed Circuit Cameras can track where we go and what we do
  - The United Kingdom is estimated to have one closed-circuit television camera for every 10-15 people.
- As we consume most of our media electronically or directly online, our reading and viewing habits are now very easy to track.
  - The government or a corporation can review which ebooks we read,which newspaper sites we visit, what music we listen to, and which movies and tv shows we watch

And computers do the rest

- Big Data – The ability to store massive amounts of information and the ability to combine data from many different sources gives both commercial and government users capabilities previously unseen.
- Computers provide Analysis – Computers allow us to process data in ways not previously available. License plate reading can be combined with traffic cameras to track our vehicles. Face recognition combined with closed-circuit television (CCTV) cameras makes it easy to track our movements

Our Data

- When you are using a commercial service, usually you are both the customer or the product
- This is the tech equivalent of "there's no such thing as a free lunch."
- While some may argue that this oversimplifies the situation, we can certainly agree that companies must make money somehow.
  - If you're using a service and not paying for it, one common approach is for the company to sell your information either directly or via targeted advertising.
  - Unfortunately, you can be a paying customer and still have your data sold for further profit.
  - As of April 2017, Internet Service Providers can now sell information on your browsing habits to others.

Surveillance

- As consumers our transactions are monitored by financial institutions to detect fraud and our preferences are monitored by loyalty programmes to enable future marketing campaigns to target us.
- As mobile(cell) phone users our movements and communications can be tracked for use by the emergency services: some people use location based services, such as GPS, to find their way around new places.
- Surveillance is something which can confer access, entitlement and benefit as well as something which is dangerous, oppressive and discriminatory. Individuals now actively manage their own data profiles knowing they will be able to customize and improve their services as they do so

Surveillance

- The danger is that surveillance power becomes ubiquitous: embedded within systems, structures and the interests they represent. Its application becomes taken for granted and its consequences go un-noticed.
- As data travel silently across international boundaries, between national states and within transnational corporations, the impact of surveillance becomes even harder to identify, regulate and debate.
- It is important that this power, based on the oversight of activities and of personal data, is wielded fairly, responsibly, and with due respect to human rights, civil liberties and the law

Surveillance Society (surveillance-studies.net)

- Surveillance societies are societies which function, in part, because of the extensive collection, recording, storage, analysis and application of information on individuals and groups in those societies as they go about their lives.
- Retail loyalty programmes, website cookies, national identity schemes, routine health screening and no-fly lists all qualify as surveillance.
- Each features, in different measure, the routine collection of data about individuals with the specific purpose of governing, regulating, managing or influencing what they do in the future.

The issue

- Perhaps I'm perfectly happy to use Google for free, and I prefer to see advertisements from the DoubleClick advertising network for products I might be interested in over advertisements for things I have no interest in. Should I still care about commercial use of my information?
- One classic example of abuse of information is, what happens if you visit websites related to cancer. Would you be concerned if your ISP passed that information on to your insurance company and they raised your insurance rates?
- Legal and Illegal Access to Information - When you provide information online, keep in mind that your information may be accessed legally or it may be accessed illegally.
- It is only as safe as the computer security of whoever is holding it.
- Let's take a look at a few example

Data Breach

- A data breach is a security incident in which information is accessed without authorization. Data breaches can hurt businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair
  - Spyware
  - Keylogger
  - Cookies
  - Sniffing (wardriving)
  - Employee monitoring
  - Manipulation of business transactions
  - Theft of information from large institutions

Ashley Madison

- In 2015 the Ashley Madison website for adulterous affairs was hacked.
- 30 million names of users on the website were leaked.
- Even if you trust a business not to expose your information directly, do you trust their computer security experts enough to be sure that hackers won't get your information?

Facebook

- Data from over 50 million profiles was taken and then sold to Cambridge Analytica (Facebook later confirmed that it actually had data on potentially over 87 million users, with 70.6 million of those people from the United States.)
- Facebook users were falsely told by a Cambridge professor that their data would only be used for academic purposes.
- Data taken included not only those who agreed to participate in a survey, but those of their friends as well.
- The Cambridge professor was dishonest and violated Facebook's rules. However, nevertheless the data was exposed.

Cambridge Analytica

- The data was collected through an app called thisisyourdigitallife, built by academic Aleksandr Kogan, separately from his work at Cambridge University
- However, the app also collected the information of the test-takers' Facebook friends, leading to the accumulation of a data pool tens of millions-strong

Which kind of Information

- Facebook sent a message to those users believed to be affected, saying the information likely included one's "public profile, page likes, birthday and current city".
- Some of the app's users gave the app permission to access their News Feed, timeline, and messages. The data was detailed enough for Cambridge Analytica to create psychographic profiles of the subjects of the data. The data also included the locations of each person.
- For a given political campaign, each profile's information suggested what type of advertisement would be most effective to persuade a particular person in a particular location for some political event

More Data Breaches

Making up the biggest portion was a 2016 breach of Yahoo! where over 3 billion pieces of data were leaked. At the time it ranked as the biggest data breach in history, says the study.

Top 10 largest data breaches by organization:

1.	Yahoo!	3,500,000,000
2.	River City Media	1,370,000,000
3.	FriendFinder	412,000,000
4.	MySpace	360,000,000
5.	Exactis	340,000,000
6.	Marriot International	327,000,000
7.	Epsilon	250,000,000
8.	Deep Root Analytics	198,000,000
9.	LinkedIn.com	167,000,000
10.	Under Armour	150,000,000

S. Rodotà (2004)

- "L'intero orizzonte dei temi di questi tempi difficili è davanti a noi. Emerge un legame profondo tra libertà, dignità e privacy, che ci impone di guardare a quest'ultima al di là della sua storica definizione come diritto ad essere lasciato solo. "

S. Rodotà

- Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale della società dell'eguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l'appartenenza a partiti, sindacati, associazioni, i cittadini rischiano d'essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione.
- Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo diventa così evidente che: la privacy è uno strumento necessario per difendere la società della libertà, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale..

Privacy & Security

- Forms of cyberattack can be directed at individuals to acquire personal information
  - Information collection: collecting personal information
  - Information processing: storing processing and use of the collected information
  - Information dissemination: dissemination of personal information
  - Invasion: intrusion into a person's private life
- System protection techniques can therefore also be effectively used to protect this data

PET

- An initial response to these problems was provided by the research world by making available to users the appropriate technologies called Privacy Enhancing Technologies
- PET provide mechanisms for people to hide the content of their information (for example GPG) and hide their identity on the net (anonymity)

- May be we don’t really care if someone can read my emails as we don’t have anything to hide.
- However, there are wider issues at stake.
- Consider the following examples:
  - Online anonymity helps drug traffickers and terrorist organizations.
  - Anonymity allows online harassment of individuals often with no recourse available.
  - Anonymity allows women’s rights, human rights activists to operate in countries where they might face harassment or worse from the government

What is it ?

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU)
- It comes into play on **25th May 2018**
- **It aims to give people more control over their data and allows them to request to see the personal data held on them**

What is GDPR?

- Governs the type of notice that must be provided to people regarding how their identifiable data is used
- Governs how companies are allowed to use and process identifiable data
- Has stricter requirements for using sensitive data

To Whom Does GDPR Apply?

Those who offer goods or services to persons in the EU/EEA

- European Economic Area (EEA) = European Union (EU) + Iceland, Liechtenstein, Norway, & UK

Those who control and process data about persons in the EU/EEA

- Personal Data = any information that can identify a person
- Sensitive Data = race/ethnicity, political opinions, religious/philosophical beliefs, union membership, genetic data, biometric data, health data, data concerning a person's sex life or sexual orientation.

What is Data Processing?

- Processing of data involves any and all of the following:

  - Adapting
  - Altering
  - Collecting
  - Combining
  - Consulting
  - Destroying
  - Disclosing

  - Erasing
  - Organizing
  - Recording
  - Retrieving
  - Storing
  - Structuring
  - Using

What is Needed to Process Data?

- A "lawful basis" for doing so
- A "lawful basis" can be:
  - When required for a contract
  - When required for public interest
  - When required to comply with a law
  - When required to protect an individual's life
  - When required for the legitimate interests of a third party *(no sensitive data)*
  - When freely given consent for a specific purpose has been provided
- If sensitive data is being processed, explicit consent for those data elements is required.

What Elements of Consent are Needed?

- Name and/or title of the data processor
- The purpose and basis for processing of the subject's data
- The type of data to be processed

  Remember: When sensitive data are going to be processed, these data elements must be explicitly listed in the consent.

- If data will be transferred to a less secure country (i.e. the U.S.)

I Got Consent! Now What?

- Processors and Controllers must ensure privacy:

  Limit access to the data

  Code or encrypt the data where possible

  Limit processing to only the necessary data

  Retain the data for the least amount of time possible

  Incorporate data protection into the processing activities

What Are the Subject's Rights Under GDPR?

- Rectification of the personal data
- Notice when their personal data is used
  Includes modifications and erasures
- Can restrict how their data are processed
- Can reject automated individual decision-

- Access to their personal data collected about them
- Must be able to receive their data and transfer it to a third party

Key areas of GDPR?

- Individuals will have –
  - The right to access
  - The right to be forgotten
  - The right to data portability
  - The right to be informed
  - The right to have information corrected
  - The right to restrict processing
  - The right to object
  - The right to be notified

Individual's right to access – what do you need to do?

- Current Privacy Notices will provide individuals with certain information such as your identity and how you intend to use their information
- GDPR requires you to explain your lawful basis for processing data and your retention periods.
- You must be able to provide electronic copies of private records to individuals, where it is stored and for what purpose.
- You cannot charge for providing these and you will have a month to comply
- You can refuse but they must be told why and that they have a right to complain

What Happens if I Don't Follow GDPR?

- Fine of either €20,000,000 or 4% of annual revenue (whichever is more) for:
  - Not having a "lawful basis" to process data or getting insufficient consent
  - Not being able to allow individuals to exercise their rights
- Fine of 2% of annual revenue for:
  - Not having records in order
  - Not providing proper notification of a breach

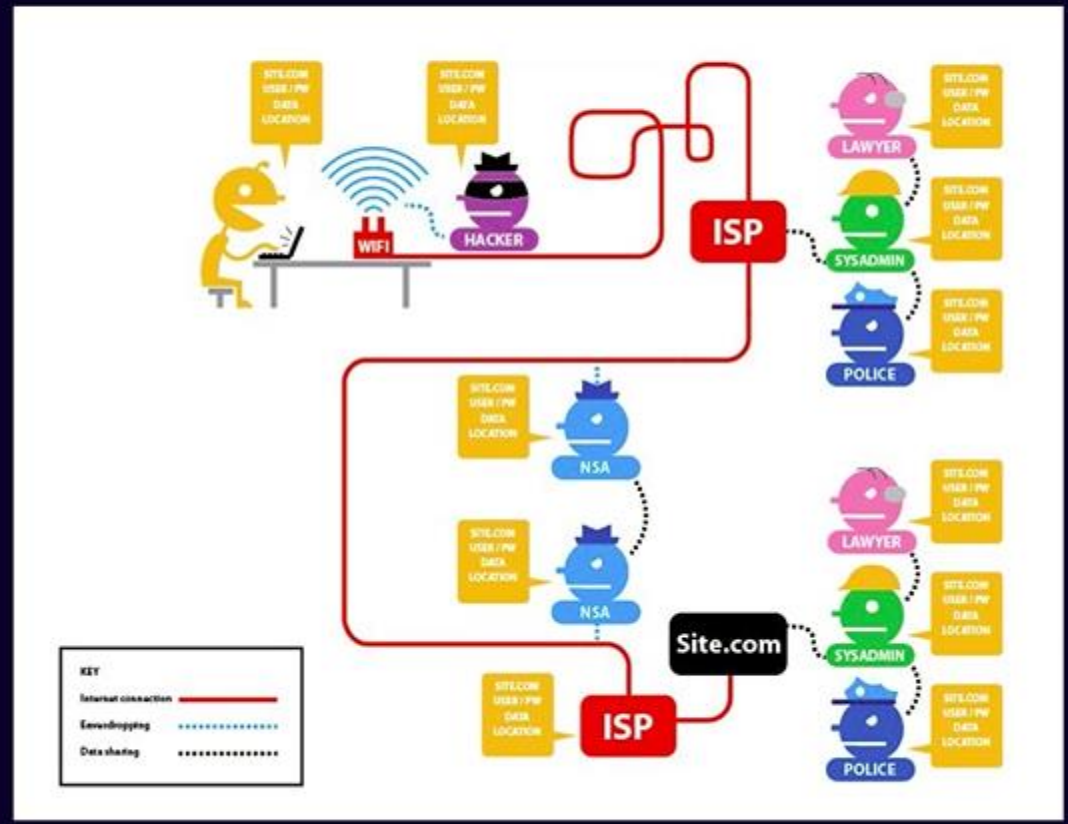
google image

TOR

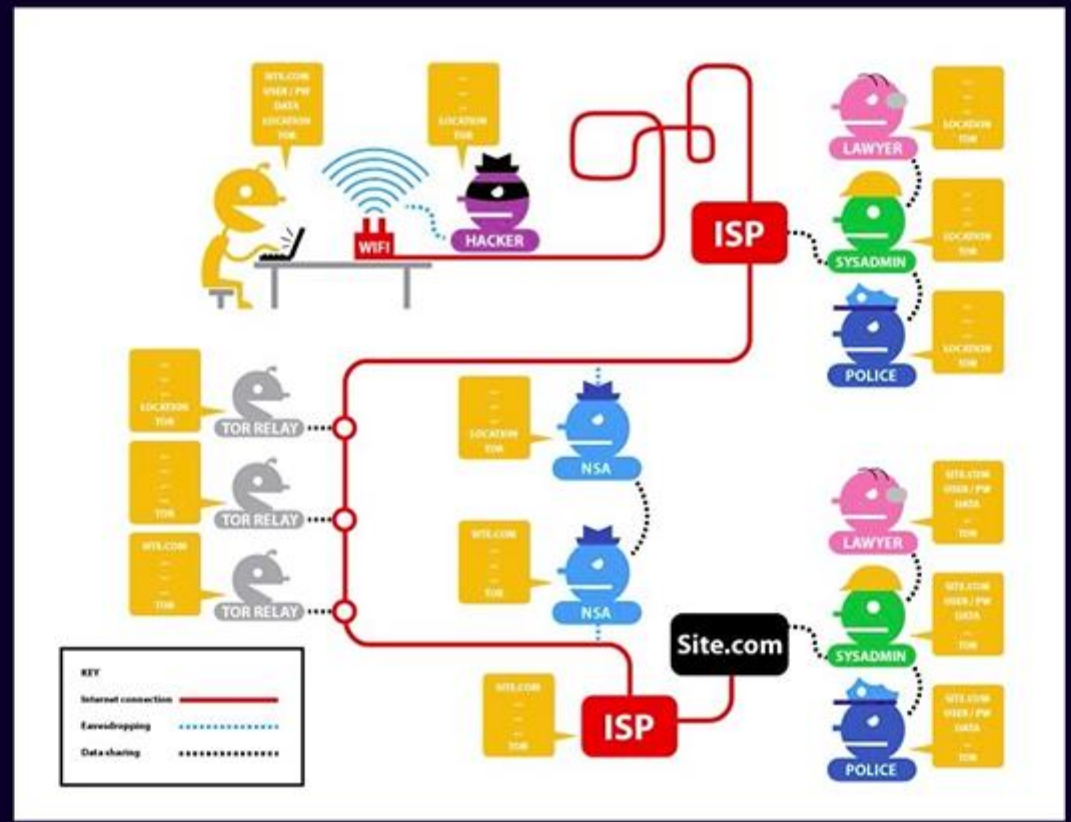
The onion routing, deep web

Matteo Zoia, PhD student @ Unimi
Davide Rusconi, PhD student @ Unimi

TOR browser


WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
NSA
NSA
Site.com
ISP
LAWYER
SYSADMIN
POLICE
KEY
Internet connection
Eavesdropping
Data sharing

TOR browser


WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
TOR RELAY
TOR RELAY
TOR RELAY
NSA
NSA
Site.com
ISP
LAWYER
SYSADMIN
POLICE
KEY
Internet connection
Eavesdropping
Data sharing

TOR, the onion routing

- Tor (The Onion Router) is an implementation of the onion routing developed in the mid 90s by US Naval reserch.
- The idea: the messages bounces around connections between different routers so that they’re hard to track and it provides anonymity.

- Very different from confidenciality which is usually associate with encryption. An encrypted message can be see by somebody but it can't be read, in this case we don’t even want people to see that we sent message at all.

TOR

- Tor
  - Allows anyone to use the internet while hiding the IP address by ensuring privacy
- Tor browser
  - Protects you from browser fingerprinting
  - Doesn’t leave a trace of your browsing history
- It is used for
  - Censorship circumvention
  - Defense against survelliance
  - Private browsing

TOR

- The idea is essentially confuse people who are trying to work out what's going on right now and gain privacy.
- Tor, in it's implementation uses 3 hop, middle hosts where the message get through before arriving to the destination.
- Everyone that runs tor can also be a node. The project is free and open-source and the people are invited to sign up and become these intermediate nodes.
- Distribuited nodes that join in and out of the tor network makes all the system more secure.