Online privacy and security

Dan Ionita

UTwente, Services and cybersecurity (scs.utwente.ewi.nl)

Outline

Introduction to informational privacy

The privacy-technology duality
Identity in the digital age
Privacy and information technology

3

Privacy intrusive Tools and technologies

The Internet
Big Data
Mobile devices
Ubiquitous computing

28

Privacy Enhancing Tools and technologies

Privacy by design
Cryptography
Encrypted communication technologies
Anonymous communication technologies

57

Introduction to informational privacy

The privacy-technology duality

Identity in the digital age

Privacy and information technology

The privacy-technology duality

Technology is a major factor when it comes to the way we perceive privacy

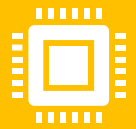
This is because certain technological developments disrupt the way we communicate and share information

Which leads to new ways in which privacy can be breached; but also protected.

Technology: trigger of the privacy debate

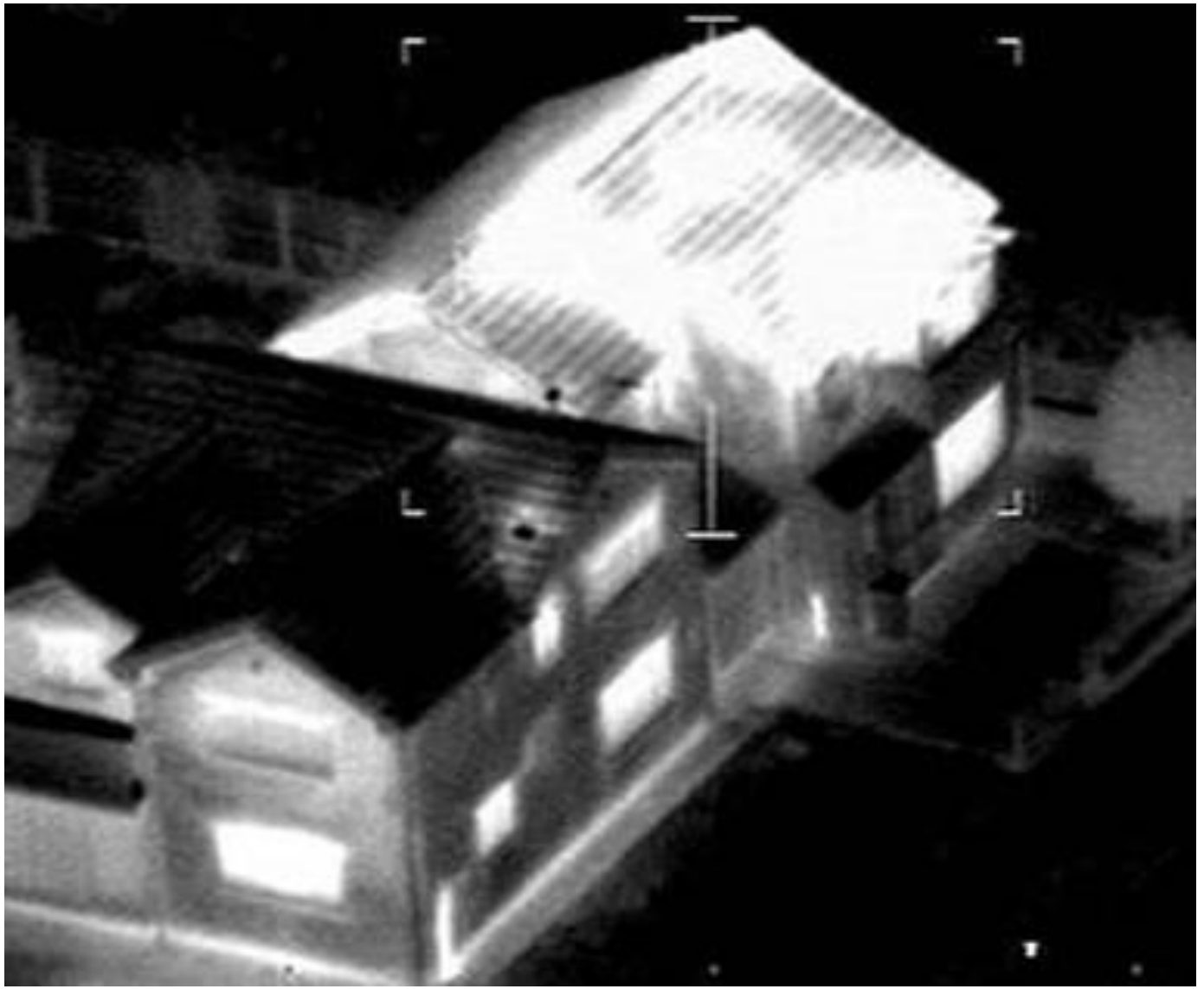
The first publication explicitly discussing privacy was “The Right to Privacy”, by The Harvard Law Review in 1890.

This coincided with the advent of popular press (i.e. newspapers), made possible by advancements in printing and photography technologies.



In fact, most modern privacy legislation dates to the widespread adoption of faxes (junk faxes), digital telephony (auto dialers), email (phishing) and body sensors (polygraphs).

Example 1



Example 2


Use the Automatic
During the Convention
Make the Automatic Telephone Station at the Coliseum your headquarters. A reception room, booths and uniformed pages at your service on the main floor of the Annex.
Let us facilitate your work —and let us demonstrate to you the wonderful efficiency of the Automatic telephone—
The ONE Phone That Gives SECRET SERVICE
Automatic Telephone Service is pulling the biggest popular vote in history! Local Chicago traffic has more than doubled, and long distance increased 80%, since January 1, 1912.
Because of its very low cost, its instantaneous connections, its secrecy, its splendid carrying powers, the Automatic is the only logical telephone. By all means take advantage of this special convention service.
Local Calls 5c
Long distance calls at remarkably low rates
Illinois Telephone & Telegraph Co.
(Successor to Illinois Tunnel Co. Telephone Department)
162 W. Monroe St.
Commercial Dept. 33-111
Information 892
Long Distance Call (O) on the Dial
AUTOMATIC
CHICAGO, ILL.
INDEPENDENT
TELEPHONE
IT
C

Information technology and privacy

- Most innovations were designed to be privacy-enhancing.

- But **overall**, Information and Communication Technology (ICT) has had **negative implications** for privacy:
  - Partly due to the insecurity of some IT systems (e.g. hacks, leaks);
  - But mostly due to the **sheer quantity** of data *transmitted*, *processed* and *gathered* exceed the ability of the individual to understand or control the flows of personal information.

Internet

100 GB / day (1992)

26600 GB / second (2016)

Devices

0,06 GFLOPS (Pentium PC)

13.4 GFLOPS (Galaxy S8)

Storage

$4000 / GB (1992)

$0,03 / GB (2016)

Constitutional vs. informational privacy

Constitutional (decisional) privacy

- Make personal or intimate decisions without interference.

Tort (informational) privacy

- Control who has access to private information.
- Subtypes: politcial, medical, corporate, online privacy.

In this lecture, we look at **informational privacy:**

- *What is privacy in the digital age?*
- *How do modern tools and technologies protect or endanger it?*

New technology comes with new risks

Mobile devices:

- Radio communication is vulnerable;
- Location tracking promises convenience but threatens privacy.

The Internet Of Things

- Smart things allow for ubiquitous data collection or tracking;
- Smart things are actually not very smart.

Big Data

- Analytics is big business

As with most new technology, privacy and security are often after-thoughts…

Privacy vs. security

Definitions

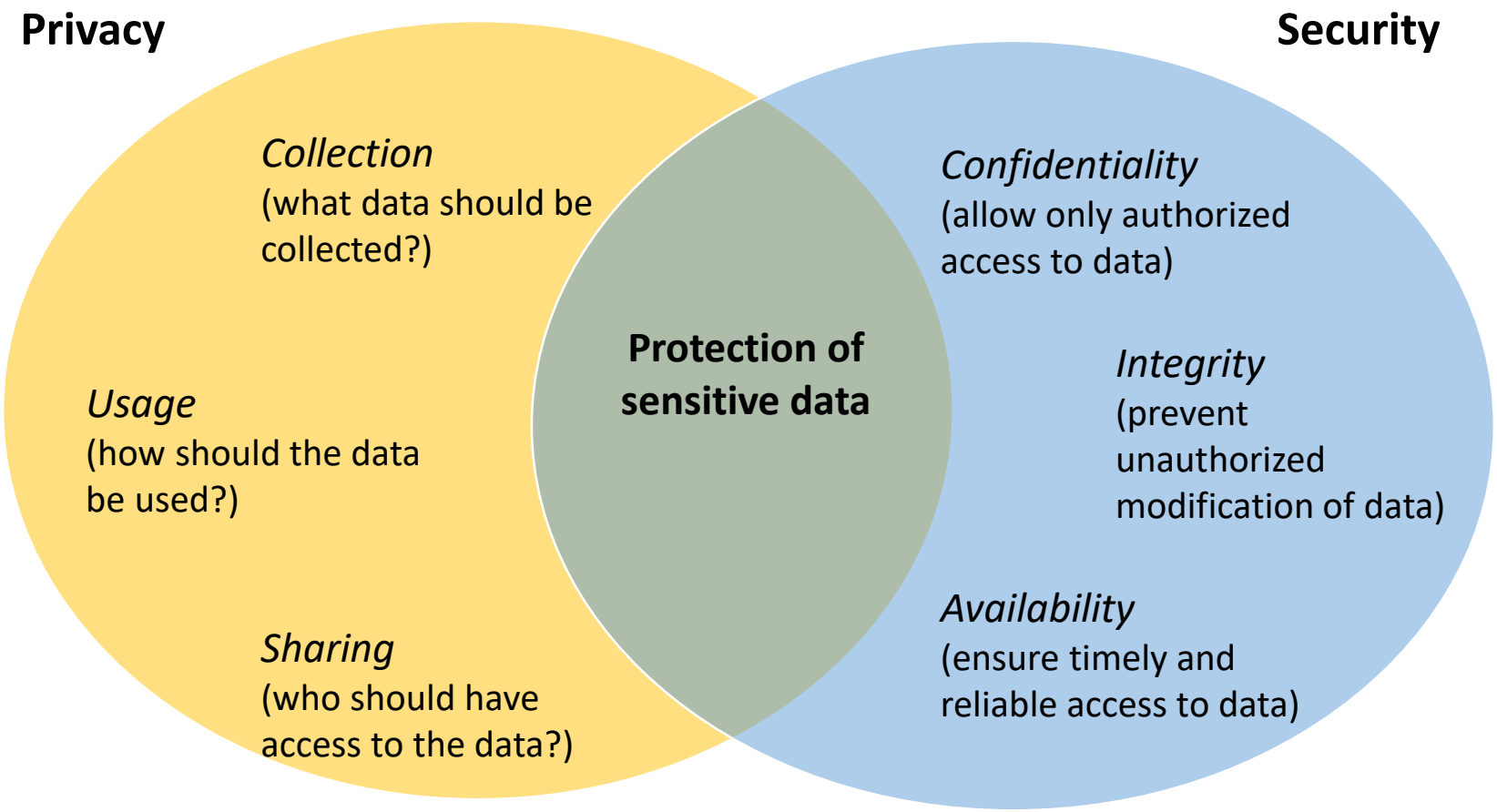
(Information) Security:

The state of being free from danger.

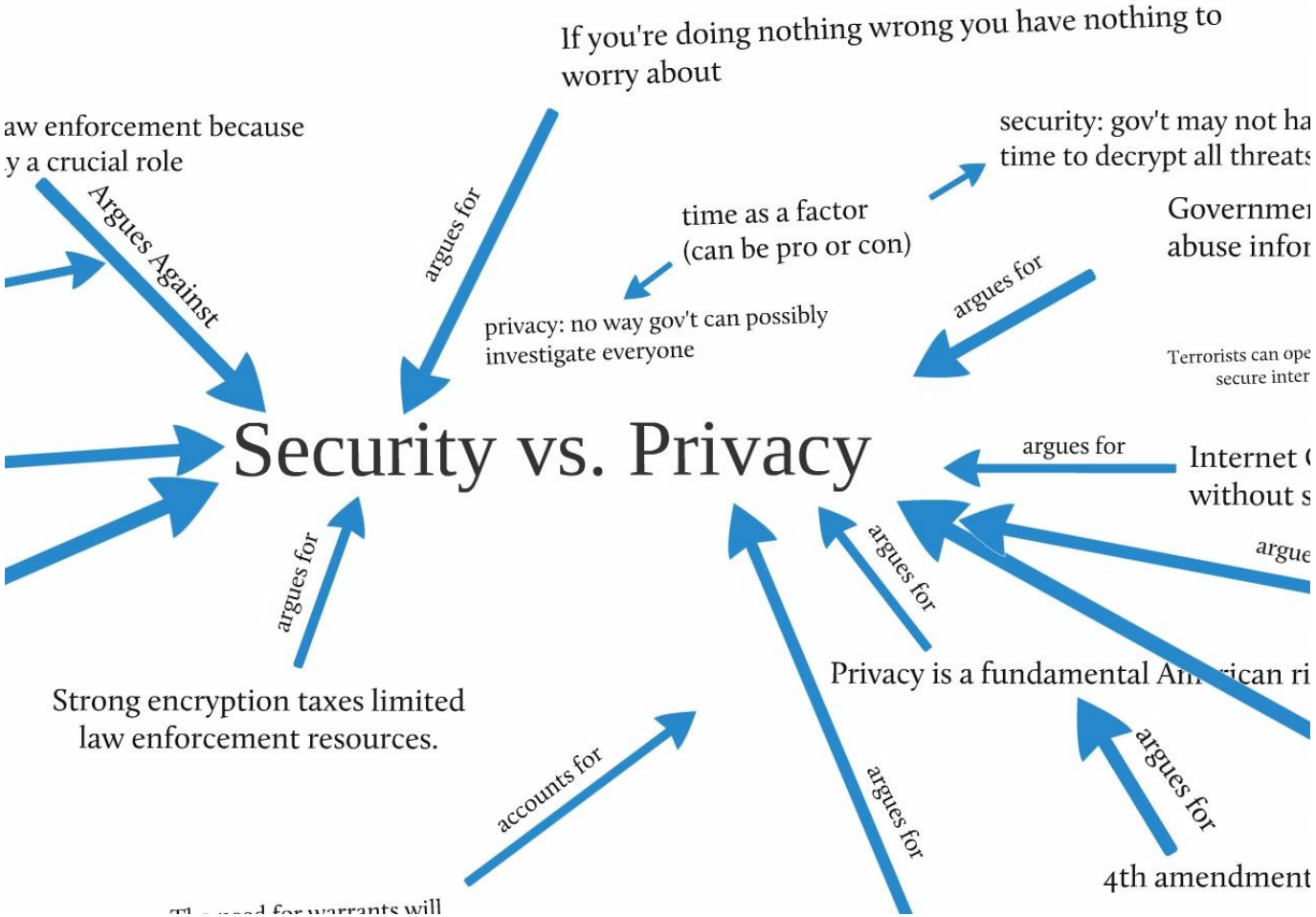
(Information) Privacy:

The state of being free from observation or disruption.

An IT perspective



The privacy vs. Security debate



Credit: http://derekbruff.org

Are privacy and security a trade-off?

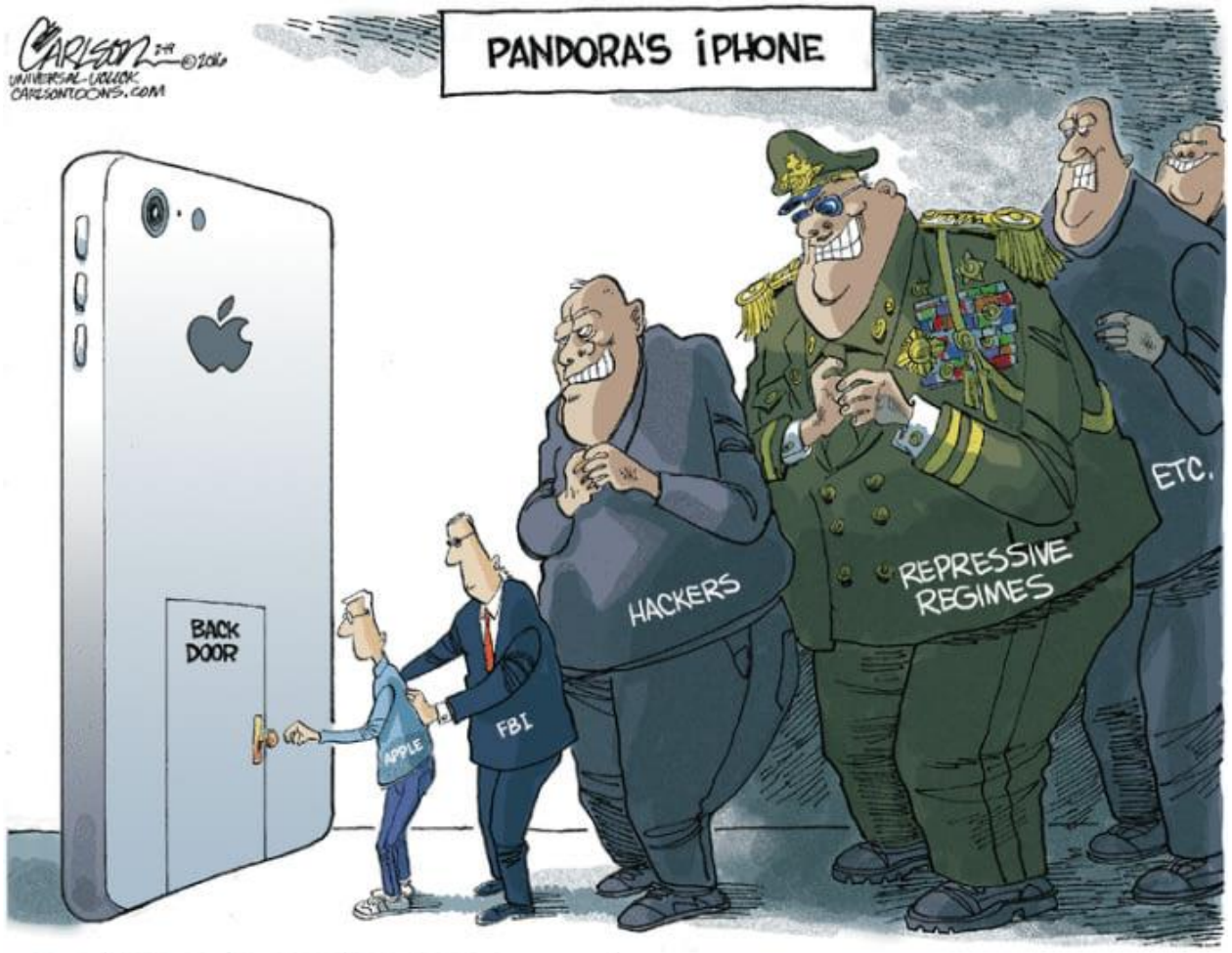
Privacy may appear to hamper security (e.g. locked iPhone of terrorist)

- But is it really a trade-off?
- Are security and privacy conflicting or opposed?

Not really…

- Security affects privacy when based on identity (more on this later):
  - *B. Schneier: "Security and privacy are not opposite ends of a seesaw; you don't have to accept less of one to get more of the other. "*
  - *B. Franklin: "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety"*
- Weak privacy can even erode security.

The privacy vs. Security debate



Credit: http://www.gocomics.com/

Identity in the digital age

"Identity will be the most valuable commodity for citizens in the future, and it will exist primarily online."

Eric Schmidt (Google chairman), 2013

Digital vs. “real” identity

Different types of identity:

- Personal identity (who you are)
- Social identity (what your social group or role is)
- Legal identity (what kind of citizen you are)
- Digital identity (what information is available about you online)

Digital identity = "set of attributes related to an entity“ (a.k.a. a profile)

- These attributes can reveal (a version of) your personal, social or civil identity.

For an information system, identity is a means of **controlling access.**

Identification
claiming identity

Who are you?

Authentication
verifying identity

Are you really who you say you are?

Authorization
providing access

What rights do you have?

Authentication factors

- **Proof of knowledge**: something you know

  e.g. PIN, password, secret
- **Proof of ownership:** something you have

  e.g. key, card, device
- **Proof of inheritance:** something you are

  e.g. fingerprint, voice, DNA

Two-factor authentication (2FA) or multi-factor authentication (MFA): combinations of the above

Anonymity

The size of the *discrepancy* determines the level of **anonymity**;

- Complete online anonimity (i.e. unlinkability) impractical, undesired-able, illegal and/or unachievable.;
- So, in practice, we make due with **pseudo-anonimity** (a.k.a. pseudonomity).
  - A **pseudonym** is a fictitious identifier which is not necessarily or immediatly associated with a real entity (e.g. Twitter handle, Facebook name, e-mail address)

Pseudonimity

	Legal identity	Digital identity
Identification:	“I’m Dan”	“I’m user123”
Authentication:	“Here is my passport”	“Here is my password”

⇒ A single person may have multiple digital identities, each with various degrees of anonimity.

⇒ A single digital identity may belong to multiple persons or to no person at all. (>83 mln Facebook and 10% of Twitter accounts are fake)

Pseudonimy is one of the ways in which the privacy vs. security “trade-off” can be avoided:

- It enables users to act without fear of reputation damage, while maintaining some degree of trace-ability.

Privacy risk management challenges

"Any privacy in public is a hard thing to negotiate"

Pete Cashmore (Mashable CEO), 2009

Online privacy is a new ball game

- Historically, there is a clear delimitation between a *private space* and a *public space*;
  - Everything inside your home is private, everything outside of it is public.

- The internet is publicly accessible, but users access it through their personal devices;
  - This blurs the line between *private* and *public*.

- So, privacy in the digital age needs to be rethough;
  - Guidelines suggests we look at how data is **collected**, for what **purpose**, in which **context**, and what **protection** is available.

Data collection

Data collection principles:

- Subjects should be notified when their data is collected
- Subjects should be informed which data is being collected

Technical challenges:

- Notifying the user
- Making sure the user reads and understands
- Data context and aggregation

Data purpose and usage

Data usage principles:

- Personal data should only be collected for a specific, explicit and legitimate purpose;
- This purpose should be communicated to the users;
- Data should never be used for any other purposes than those stated;

Technical challenges:

- Minimizing the amount of data collected
- Making sure the user agrees
- Data lifecycle
- AI discrimination

Data protection

Data protection principles:

- Private, personal or sensitive data should be kept secure from malicious or unauthorized actors;

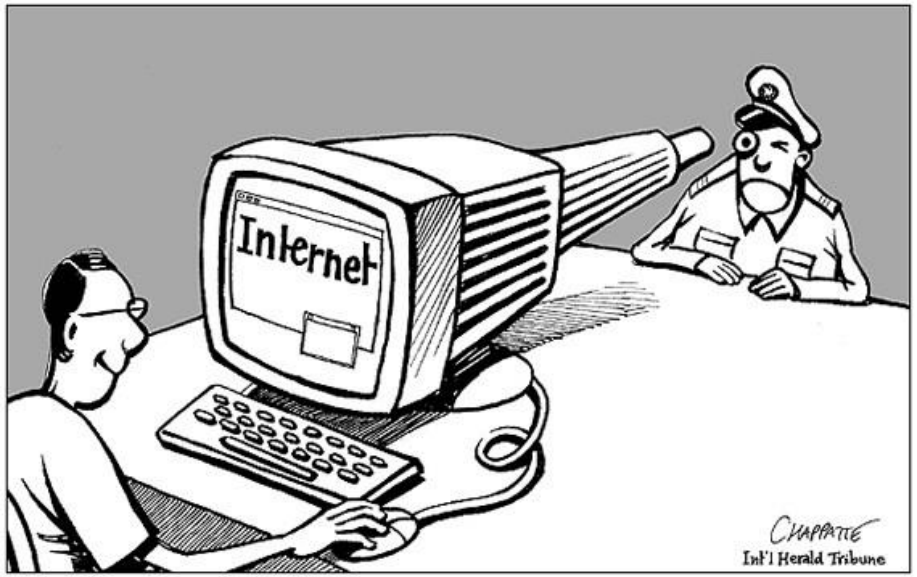
Technical challenges:

- Securing communication
- Authentication and authorization
- Cyber-security

Privacy intrusive Tools and technologies

The Internet
Big Data
Mobile devices
Ubiquitous computing

The internet



Credit:
www.chappatte.com

Fingerprinting

https://amiunique.org/

Cookies

Cookies are text files

- which web sites store on your PC
- in order to easily “recognize” you and provide advanced functionality
  - E.g. automatic login, shopping cart, third party ads, saving preferences, language setting, etc

Cookies can contain personal information

- E.g. forms, registration pages, payment pages.

Cookies (2)

Enter AdSense:

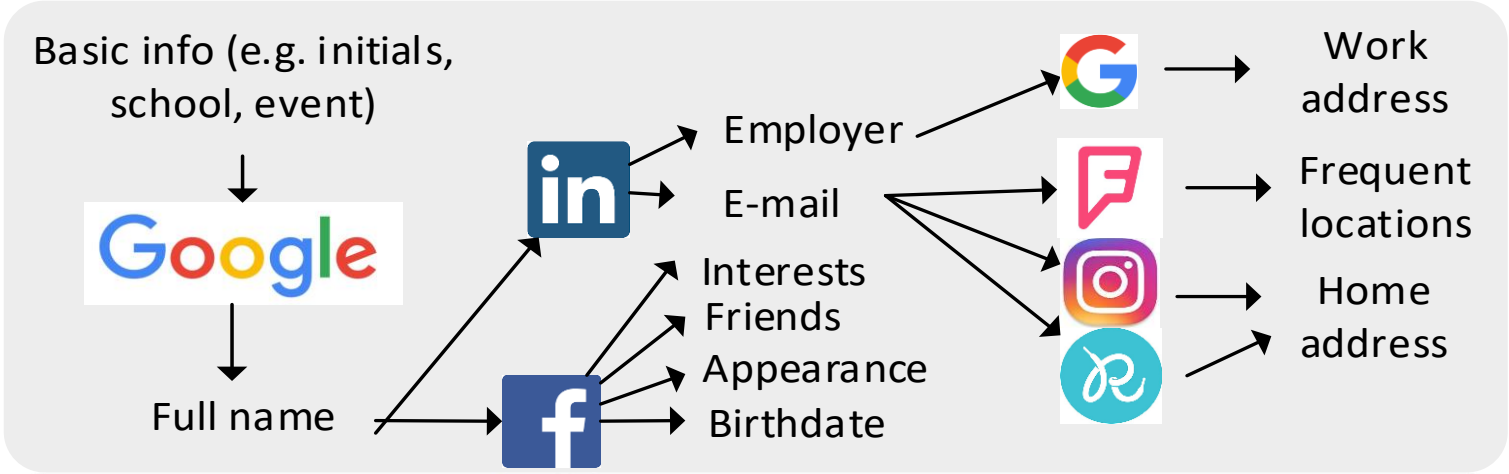
- Google's targeted ad serving platform
  - 22% of their revenue ($13.6 Billion in 2014)
- AdSense **cookies** embedded on >14 million websites
- Records user browsing history, search history and clicking habits
- Builds a profile of each user
- Serves targeted ads

Now, many other companies use cookies for **analytics** (more on this later)

Publicly accessible data

- Some institutions make public records available online;
- Many social media profiles are (partially) public
- Users often re-use pseudonyms or e-mails on multiple websites
- Users rarely delete old accounts

  => components of your digital identity can be pieced together



Publicly accessible data (2)

Crawlers = bots that systematically scan the World Wide Web and *scrapes* public content.

- used by search engines, intelligence agencies, data brokers, etc.

Data brokers aggregate, buy and sell personal information.

- E.g. pipl.com, spokeo.com, anywho.com

Open Source INTelligence (OSINT) = acquiring information from publicly accessible sources for the purpose of producing *actionable* intelligence.

- OSINT is used for the identification of *attack vectors* at a later stage. E.g. phishing, scams, fraud, social engineering.

A worst-case scenario: http://www.pbs.org/wgbh/nova/labs/lab/cyber/2/1

Spyware

Spyware = software installed without knowledge of the device's owner that:

- gathers information about a person or organization without their knowledge;
- sends private or sensitive information without consent;
- asserts control over a device without the consumer's knowledge.

An estimated 63% of Internet-connected PCs have some form of spyware.

Examples:

- tracking cookies (explained earlier)
- adware (trackers, search bars, redirectors, superimposed ads)
- Keyloggers!

Data breaches and leaks

Jan 2019:

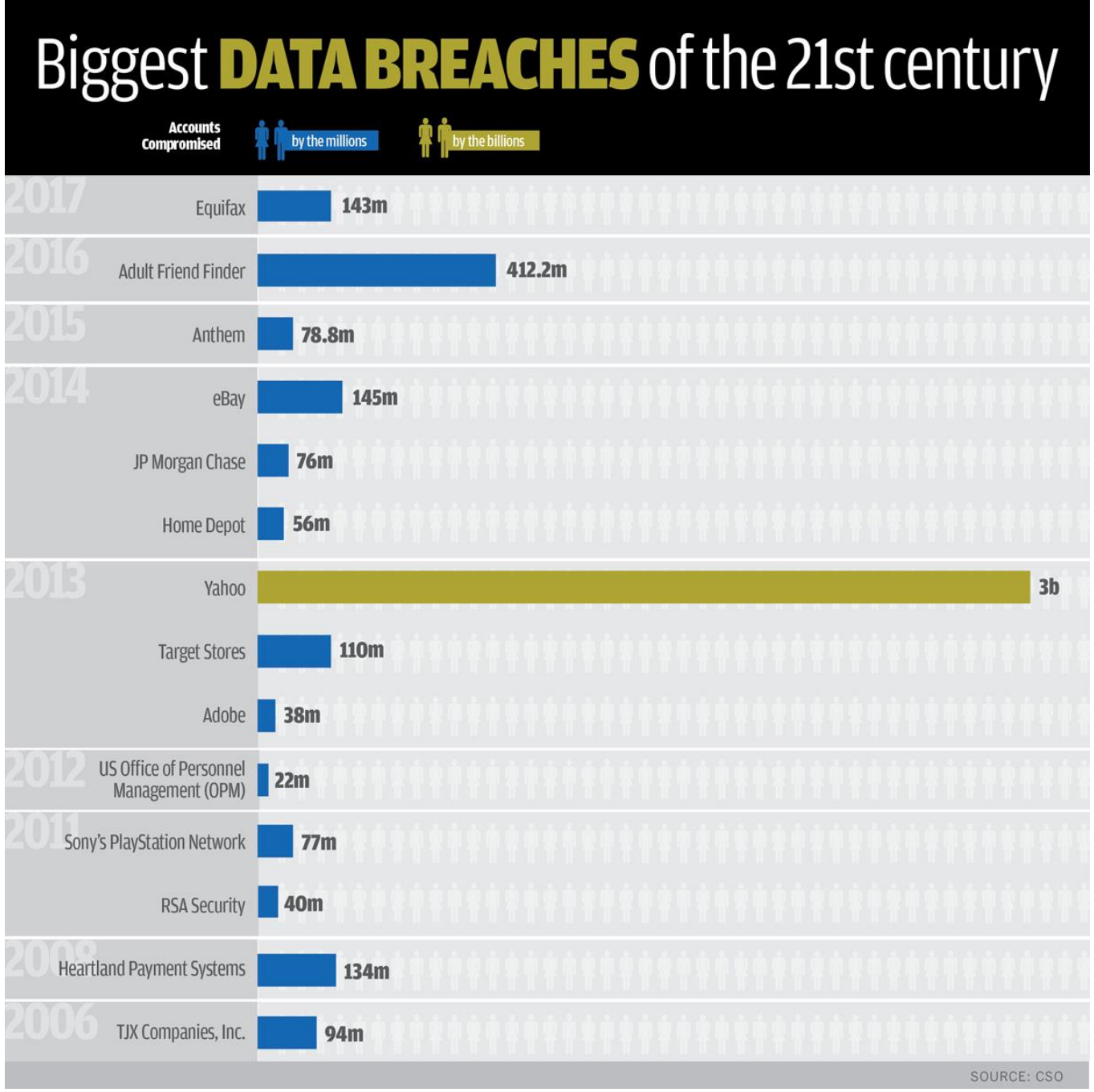
- Collection1 leak: 773 million unique e-mails

Full list of leaks:

- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

- Check if your data has ever been leaked:

https://haveibeenpwned.com



Big data

"Information is the oil of the 21st century, and analytics is the combustion engine"

Peter Sondergaard, Senior Vice President, Gartner

Analytics

Analytics = the discovery, interpretation, and communication of meaningful patterns in data. Broadly, there are three types:

- Descriptive analytics, i.e. explaining past data
- Predictive analytics, i.e. anticipating the future
- Prescriptive analytics, i.e. making decisions

<u>The more data available, the more patterns we can identify!</u>

Analytics

Practical examples:

- Marketing analytics (e.g. AdSense)
  - Build user profile in order to personalize ads
- Web analytics (e.g. Google Analytics)
  - Measure traffic and popularity for market research
- Cognitive analytics (e.g. Siri)
  - Use cognitive computing and AI to “understand” the user

Analytics have evolved past the point of simply measuring traffic.

Profiling

Profiling = the act of suspecting or targeting a person on the basis of observed characteristics or behavior.

- Profile-based predictive analytivs can lead to
  - privacy breaching (e.g. inferring medical conditions)
  - discrimination (e.g. higher premiums, or denial of coverage)
  - unconstitutional treatment (e.g. increased surveillance or even arrest)

Examples:

- Traget pregnancy coupons: sending couons for baby clothes and cribs to women who purchase certain products, with surprising accuracy;
- Google Ad Settings: show less ads for high paying jobs to women, secretly change search results for people visiting drug-related pages.

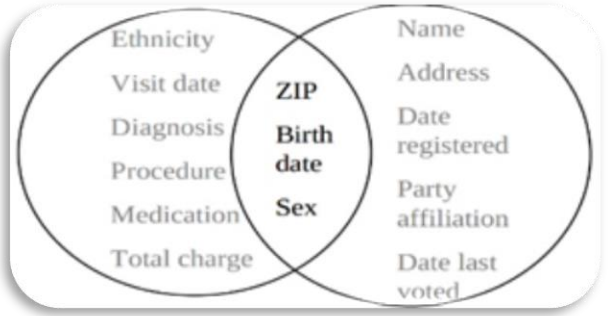
Re-identification

Person re-identification = analyzing *de-identified* information in order to discover the individual to which the data belongs to.

- Regulation and privacy policies prevent companies, health care providers and financial institutions from releasing personal data.
- But de-identified (i.e. anonymous) data is often released, e.g. for research or marketing purposes.
- However, often subjects can be identified based on *metadata*:
  - Same idea as browser fingerprinting.
  - 87% of US pop. can be identified using *gender + birthdate + zipcode*

<u>The more metadata is available, the easier it is to discern individuals.</u>

De-anonymization



Data de-anonymization = matching anonymous data sets with other sources in order to *re-identify* the subjects.

- Anonymized datasets can be cross-referenced with other (public) datasets
  - Same idea as OSINT
  - E.g. medical data and voter data in the US
  - E.g. anonymous movie ranking on Netflix with IMDB users
- Even in large datasets, very little information is needed
  - E.g. An IMDB account with 2 movie reviews and date of review +/-3 days => 68% chance of identifying the Netflix username.

<u>More datasets available => more complete profiles can be extracted.</u>

Mobile devices

“I'm not stealing my neighbor's WiFi, their WiFi is trespassing into my house.”

@ComedyPosts, Twitter

The app ecosystem

- Average number of apps: 35
- Most apps are privacy-intrusive:
  - Request unnecessary permissions
    - Easier to program and “future-proof”
  - Do not encrypt data or lack basic application security
    - Easier to program and better performance
- Burden of responsibility is on the user:
  - Identify security concerns
  - Assess the implications of permissions
- But users just want *functional, cheap, responsive, and pretty* apps…
  - 52 % seldom or never review permissions

App permissions

Most dangerous permissions

1. Read and write SMS
2. Access photo, media, files
3. Make and manage calls
4. Access contacts
5. Access calendar
6. Take pictures and record video
7. Record audio
8. Access device location
9. Sensory data and vital signs

Permissions perceived as dangerous

1. Make and manage calls
2. Sensory data and vital signs
3. Read and write SMS
4. Access photo, media, files
5. Record audio
6. Take pictures and record video
7. Access contacts
8. Access device location
9. Access calendar

How much data does **your** phone send out?

- Do you know which apps are installed on your phone?
- Do you know what data they collect?
- Do you know who has access to your data?

Download our app to find out!

(and anonymously contribute to science)

Visit **vm-thijs.ewi.utwente.nl**

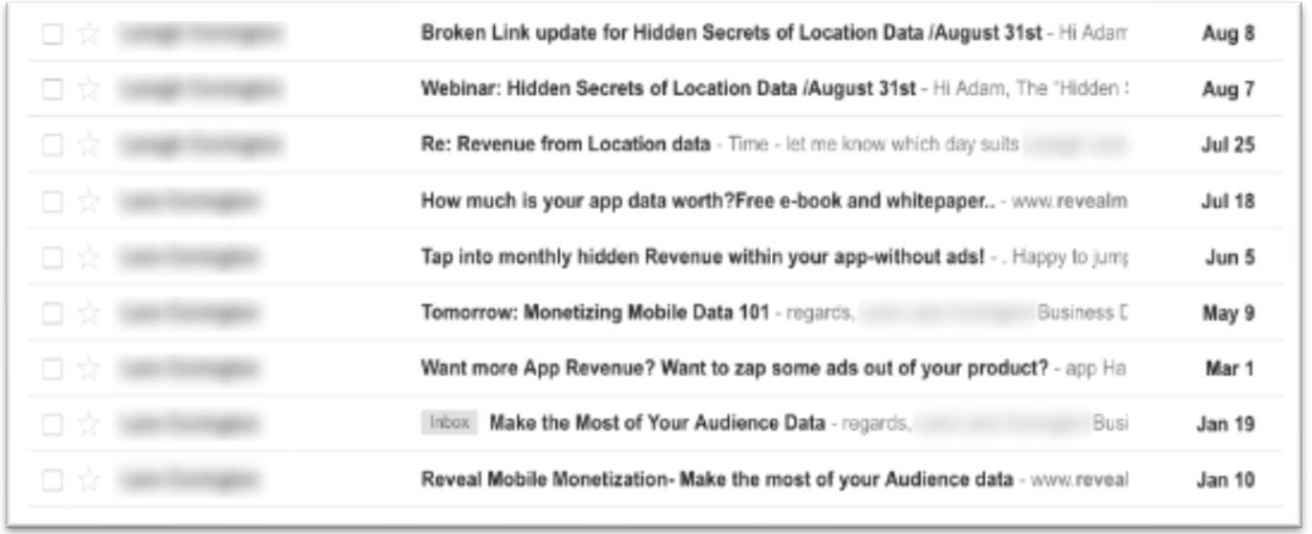
or scan the QR code:

Location-tracking

- Convenience:
  - Turn-by-turn navigation, collecting Pokémon, rain alerts, etc…
- Many options:
  - Location permission
  - WiFi (IP)
  - Bluetooth
  - Check-ins
  - Triangulation

Location-tracking

- Value: Monetization, Surveillance, Espionage



	Broken Link update for Hidden Secrets of Location Data /August 31st - Hi Adam	**Aug 8**
	Webinar: Hidden Secrets of Location Data /August 31st - Hi Adam, The "Hidden :	**Aug 7**
	Re: Revenue from Location data - Time - let me know which day suits	**Jul 25**
	How much is your app data worth?Free e-book and whitepaper.. - www.revealm	**Jul 18**
	Tap into monthly hidden Revenue within your app-without ads! - . Happy to jum	**Jun 5**
	Tomorrow: Monetizing Mobile Data 101 - regards, Business D	**May 9**
	Want more App Revenue? Want to zap some ads out of your product? - app Ha	**Mar 1**
	Inbox **Make the Most of Your Audience Data** - regards, Busi	**Jan 19**
	Reveal Mobile Monetization- Make the most of your Audience data - www.reveal	**Jan 10**

Credit: https://blog.darksky.net/location-privacy/

- Extreme example: using RunKeeper to find burglary targets

Voice control

- Voice control is becoming more accurate.
  - Because *everything* you say is recorded and sent back to a server which uses machine learning to improve accuracy;
- Voice control is becoming ubiquitos
  - Your mobile goes everywhere with you
  - And voice control is being included in other devices (e.g. Dot, Xbox, CarPlay)

<u>Risk: Potentially, every conversation you have is recorded</u>

WiFi

Wi-Fi is radio;

- This means anyone (within range) can read what you send/receive
- So how to keep things private and secure?

- Answer: *Authentication & Encryption*
  - Many options available: WEP, WPA, WPA2
  - With various configuration options: EAS, PSK, etc.
  - Most of them can be easily hacked if not configured properly!

Risks:

- Public WiFis cannot use authentication
- 25% of WiFi networks don’t use any encryption
- 50% use default or common passwords (e.g. admin/admin)

The could

Cloud storage is storing data on remote servers rather than local devices,

- operated by a Cloud Storage Provider, e.g. Dropbox;
- runs on *virtualized infrastructure;*
- often replicated in multiple locations.

Benefits:

- ✓ Accessibility
- ✓ Availability
- ✓ Scalability
- ✓ Cost savings
- ✓ Synchronization
- ✓ Security?

Risks:

- ✓ Loss of control
- ✓ Data colocation
- ✓ Leaks and hacks
- ✓ Privileged user access
- ✓ Government requests
- ✓ Security?

Pervasive computing (1)

Pervasive computing (aka Ubiquitos computing) = computing takes place everywhere, all the time.

- Refers to the Internet of Things, but also:
  - Distributed computing (e.g. Bitcoin)
  - Mobile computing (e.g. FitBit)
  - Sensor networks (e.g. CCTV, crowd monitoring)
  - Location or context-aware computing (e.g. Google search)
  - AI (e.g. NetFlix)

Pervasive Computing (2)

Pervasive computing gives rise to many privacy threats and challenges:

1. Interaction and interconnection => proliferation of attack vectors
2. “Background” data collection (lack of interaction)
3. Lifecycle management (e.g. stolen or second-hand devices)
4. (re-)identification (e.g. CCTV surveillance, facial recognition, fingerprinting, speech recognition).
5. Profiling and discrimination (based on intimate data)
6. Observable interaction (e.g. screen or voice) => shoulder surfing
7. Invetory attacks (e.g. shodan.io)
8. Linkage of systems => loss of context, de-anonymization

Privacy Enhancing Tools and technologies

Privacy by design
Cryptography
Encrypted communication technologies
Anonymous communication technologies

Privacy by design

"Design, in its broadest sense, is the enabler of the digital era - it's a process that creates order out of chaos, that renders technology usable to business. **Design means being good, not just looking good.**"

Clement Mok

The status quo

Most modern IT systems:

- make the user largely responsible for their privacy:
  - E.g. App permissions and Facebook privacy settings
- but give the user little choice and information
  - E.g. either accept lengthy Terms of Service (ToS) or don't use the software/website

Lately, experts and regulators have been promoting *usable privacy and security:*

- Built-in protection with strong defaults.
- Understandable and easy to configure.

Privacy by design

Privacy by Design (PbD) = taking privacy into account from the start of the engineering process.

- i.e. Think of privacy risks and protections *before* starting development, *during* development, and even *after* development.

- PbD shifts the burden from users towards developers;
- PbD is becoming the new best-practice standard;
- PbD is being integrated into law (e.g. the new European GDPR);
- But PbD is hard (more on this later).

PbD Principles for software

Cavoukian's high-level principles for privacy-aware *software*:

1. **Proactive not reactive:** anticipate and prevent privacy risks.
2. **Privacy as default:** default settings are the most secure.
3. **Embedded privacy:** privacy is "built-in".
4. **Full functionality:** no trade-off between privacy and functionality.
5. **End-to-end security:** encrypt all data and destroy it after use.
6. **Visibility and transparency:** be able check the above.
7. **Respect for User privacy:** Notice, consent, anonymity, access, etc.

PbD Principles for ubiquitous systems

Langheinrich's* data collection principles for privacy-aware *ubiquitous systems*:

- **Notice:** Let the subject know which data is being collected.
- **Choice and consent:** Subject must agree and can opt out.
- **Anonymity:** When possible, data should be anonymized.
- **Proximity and locality:** When possible, store and process data locally.
- **Adequate security:** Be hacker-proof.
- **Access and recourse:** Detect and punish privacy violations.

Privacy impact assessment

In order to design privacy-aware applications, developers need to first understand the privacy concerns of their users.

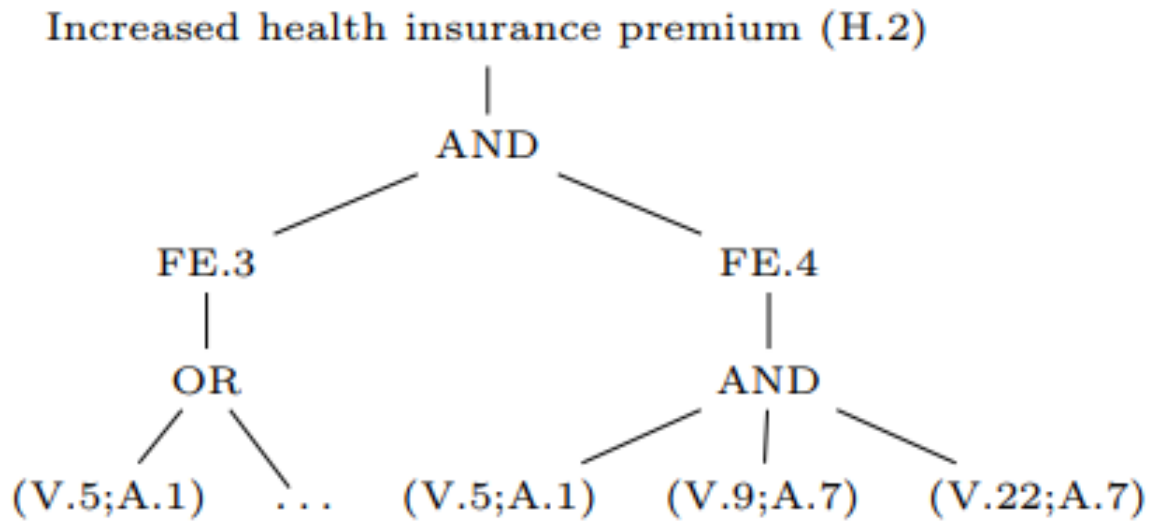
Privacy Impact Assessment (PIA) = an analysis of how an individual's or groups of individuals' personally identifiable information is collected, used, shared and maintained and how this might compromise their privacy.

Goals of PIA:

- Identify privacy risks and analyze their effects;
- Implement protections in order to meet expectations of privacy;
- Comply with data protection regulation;

PIA example: PRIAM

HAL's Privacy RIsk Analysis Methodology (PRIAM) suggest constructing harm trees which show how *privacy weakness (V)* make possible certain *feared events (FE)*, which in turn give rise to *harms (H).*



PIA obstacles

- To do a PIA you need to:
  1. Fully understand the system
  2. Know who the users are
  3. Know what kind of data you are collecting
  4. Be aware of cyber-risks
  5. Identify vulnerable data
  6. Think of possible privacy-breaches
  7. Quantify user's privacy concerns

- *Example: PRIAM*
  1. *Define the system*
  2. *Define stakeholders*
  3. *Define data*
  4. *Define risk sources*
  5. *Define privacy weaknesses*
  6. *Define feared events*
  7. *Define privacy harms*

Introduction to Cryptography

"One must acknowledge with cryptography no amount of violence will ever solve a math problem."

Jacob Appelbaum

Introduction to Cryptography

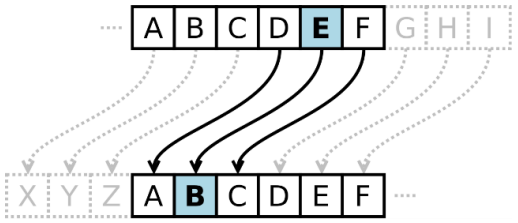
Cryptography = krypto (hidden, secret) + graphein (writing)

= the study of hiding and verifying information.

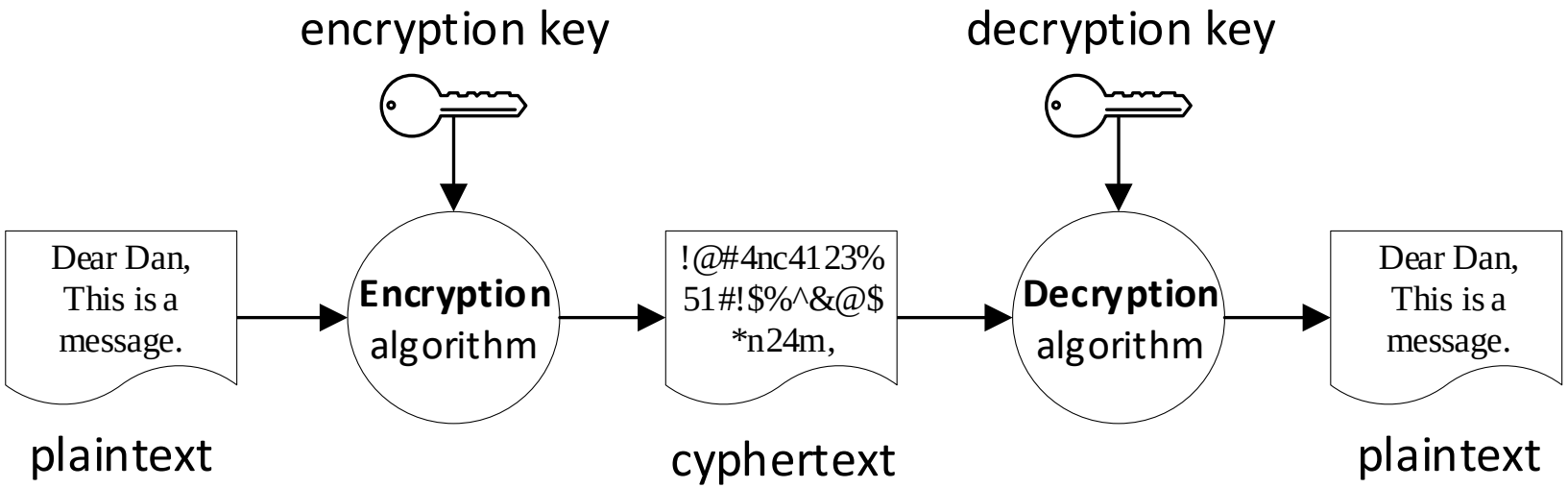
Example: *Ceaser's cypher.*

- Replace every letter with the letter `3` positions down in the alphabet.

- `Hello` **becomes** `Khoor`



Encryption and decryption

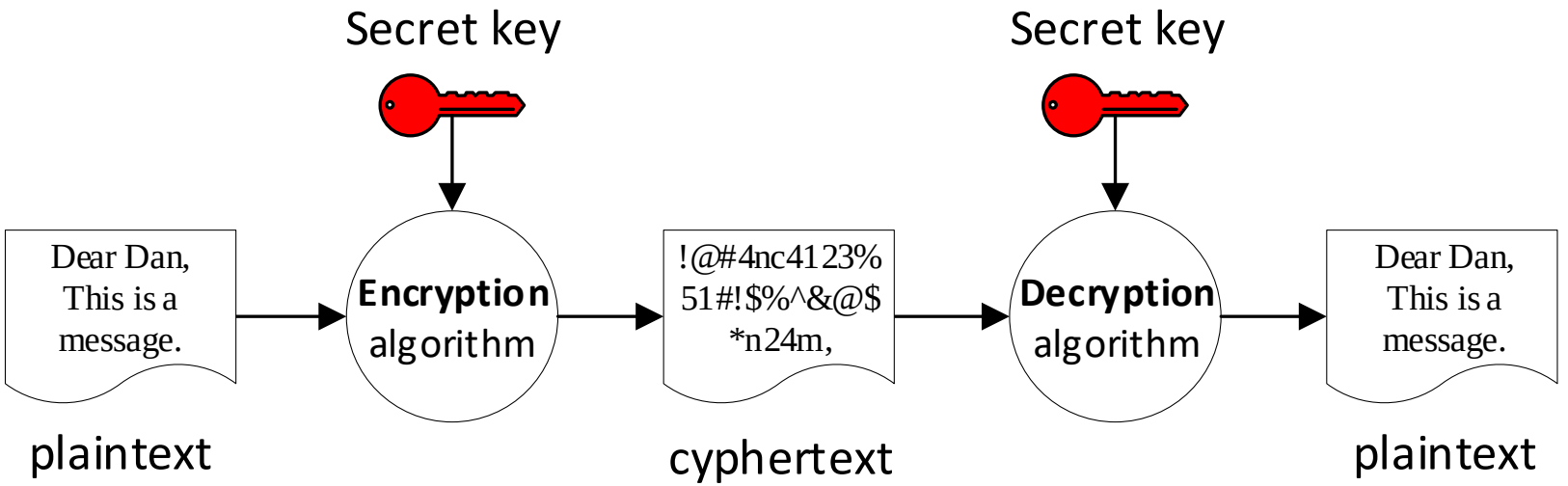


Encryption uses a *key* to encode *plaintext* into *cyphertext.*

Goal: very hard to decrypt cyphertext without key.

- E.g. via a brute-force attack.

Symmetric key

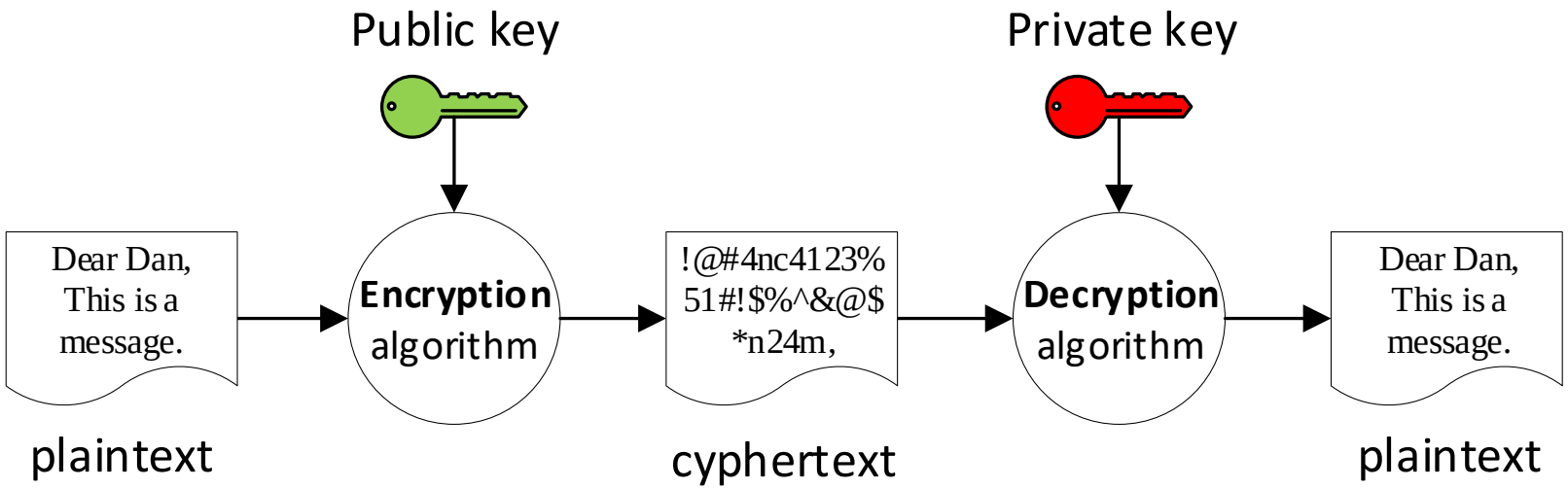


Symmetric key encryption uses the same key for both encryption and decryption.

- This key must be kept **secret.**

- Examples: Ceasar's cypher, DES, RC4, AES.

Asymmetric key



Asymmetric key encryption uses different keys for encryption and decryption:

- One of the keys muse be kept **private**, the other can made **public.**
- The public key cannot be used to for decryption.

- Examples: Diffie-Hellman, RSA

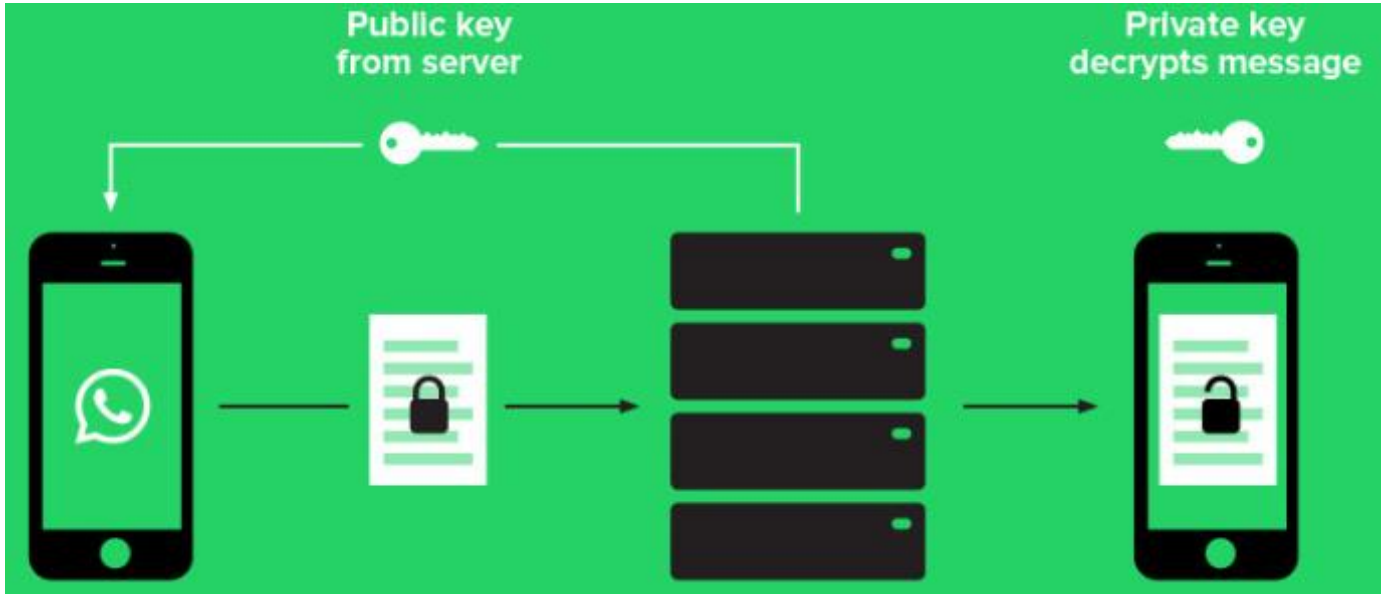
Encrypted communication technologies

"It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public."

Clay Shirky, Internet scholar and professor at N.Y.U.

End-to-end encryption

- **End-to-end encryption** = The sender and receiver do the encryption and decryption themselves.
- No one else has the encryption and decryption keys;
- So, in principle, no one else can read or modify the message.



Source: WhatsApp

PGP

- **PGP (Pretty Good Privacy)** = the most common method to encrypt e-mail.
- Uses *asymmetric keys* to provide *confidential* communication;
- Also allows *authenticating* the sender of a message using *digital signatures*;
- Free, works with any e-mail program, client or provider;
- But requires that the receiver has the public key of the sender.
  - Either by exchanging keys manually;
  - Or by publishing the public key on a key-server.

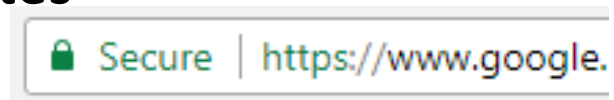
HTTPS

HTTP (Hypertext Transfer Protocol) is the backbone of the World Wide Web

- Anything sent via HTTP can be read by anyone on your network!
- Or your employer, school, ISP, etc.

HTTPS is the secure version of HTTP

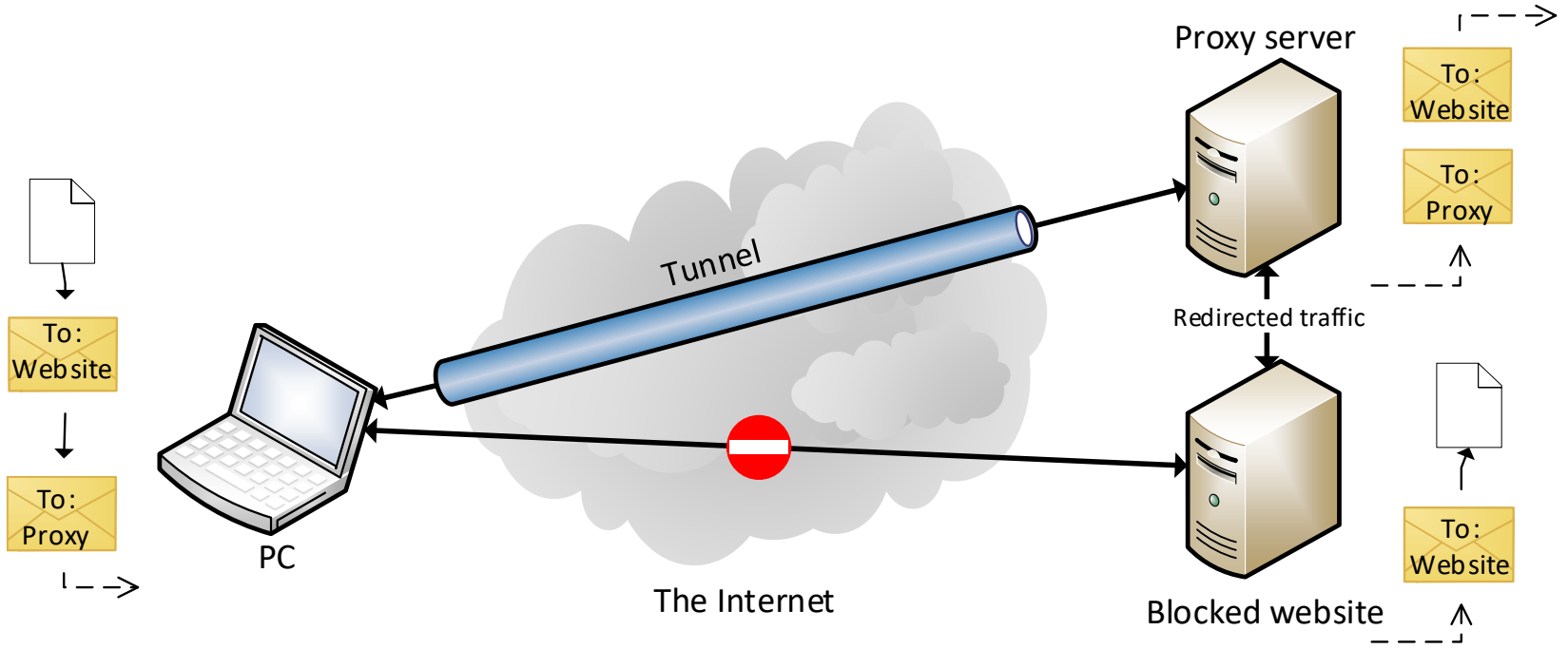
- It uses *asymmetric keys* to encrypt web traffic
- It relies on certificate authorities to vouch for websites
- Information entered on HTTPS webpages is **private.**



Tunnels

Tunneling protocols disguise internet traffic by *encapsulating packets.*

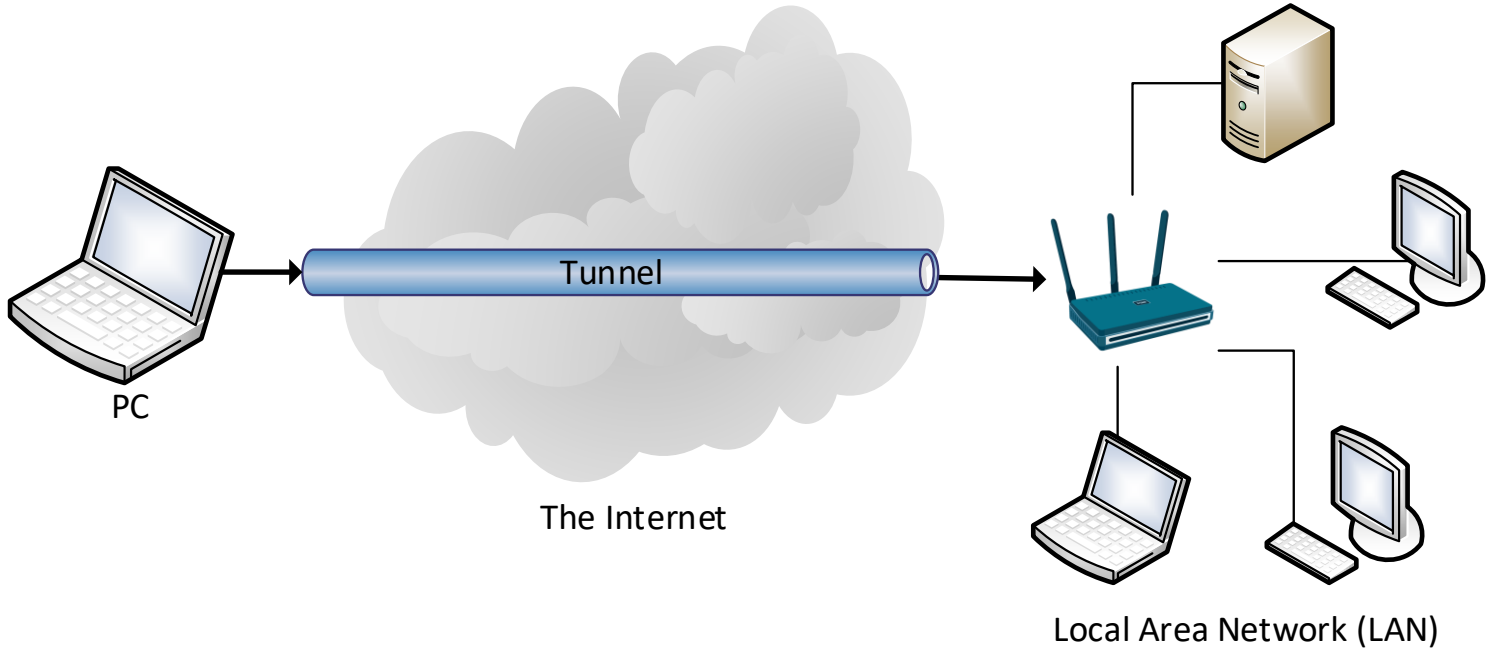
- In order to access websites or services not normally available
  - e.g. tunneling traffic through a proxy server



VPNs

Virtual Private Network = an extension of a private Local Area Network (LAN) over a public network, such as the Internet.

- Uses *tunneling* to provide "virtual" access to an internal network remotely.

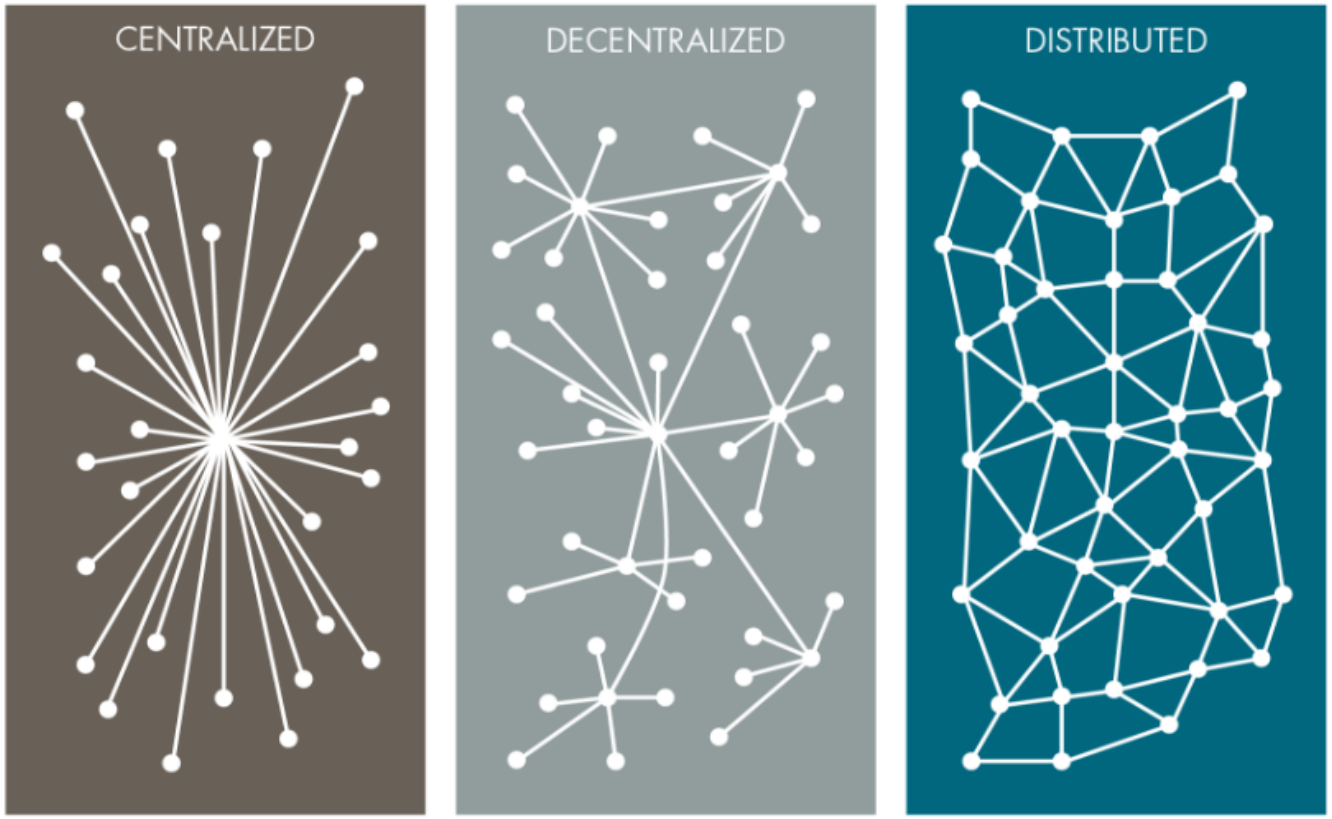


Anonymous communication technologies

“Give him a mask, and he will tell you the truth.”

Oscar Wilde

Decentralized and distributed networks



Reproduction of an original figure in "On Distributed Communication Networks" by Paul Baran

Center for Global Development

Visiting a regular website with TOR

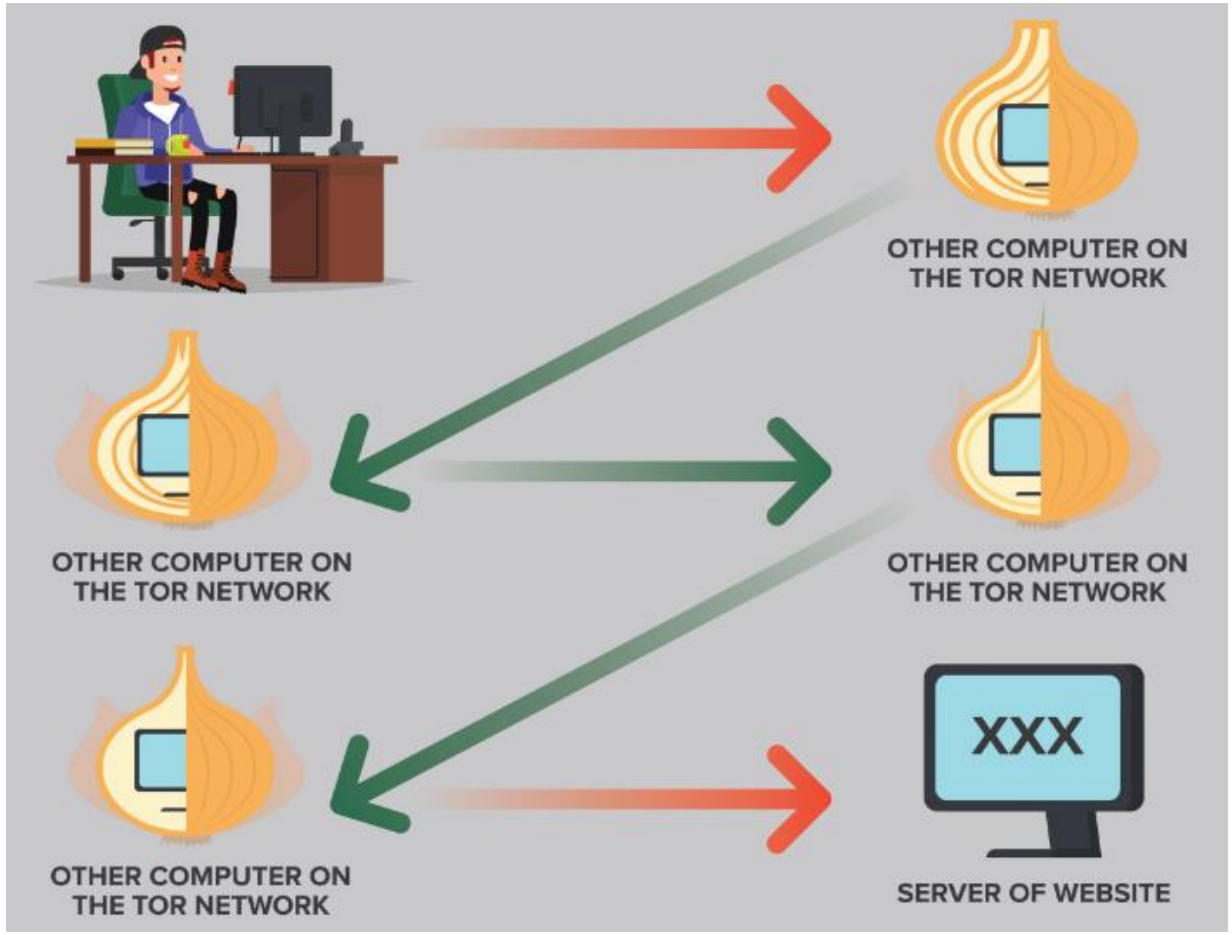


Image credit: http://mccann-cyber.com

Visiting a .onion website with TOR

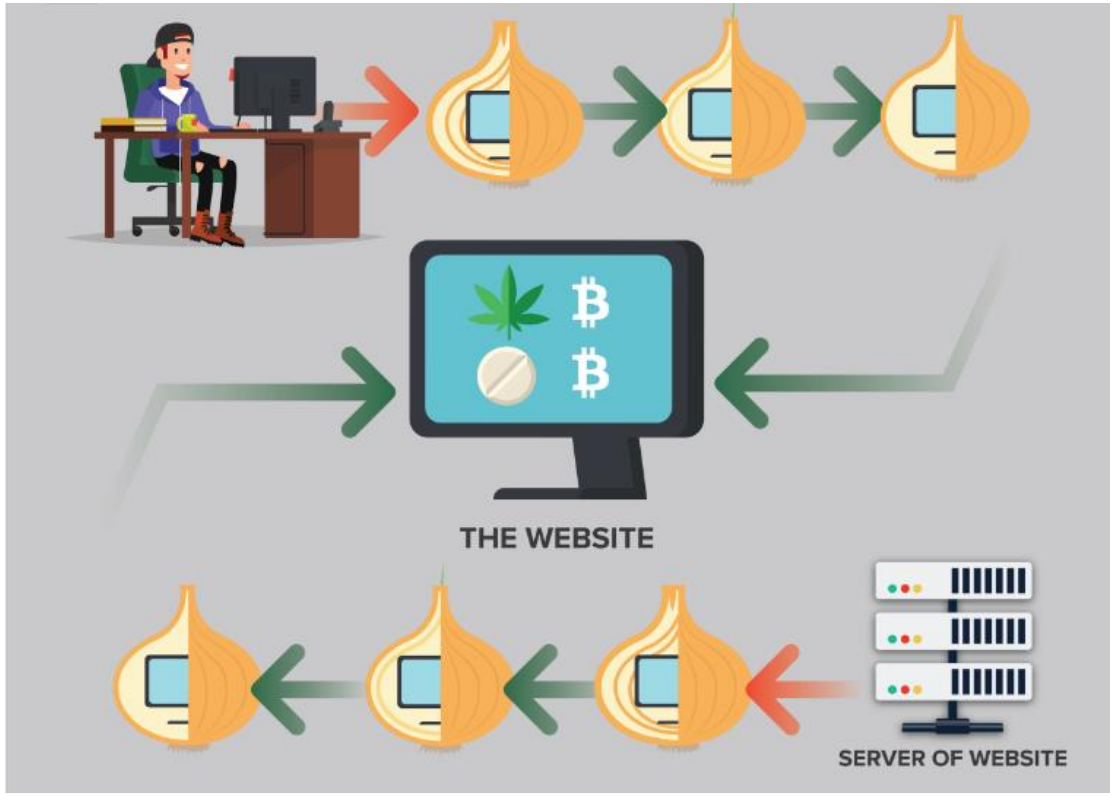


Image credit: http://mccann-cyber.com

Cryptocurrencies

Cryptocurrency = Virtual “money” which uses cryptography instead of a central bank to validate transactions and create additional units.

- E.g. Bitcoin.
- Cryptocurrencies are *decentralized* systems*:*
- There are no bank servers (e.g. ING) and no payment servers (e.g. VISA);
- Instead, each participant runs a node (i.e. a part of the IT infrastructure);
- Every new transaction has to be approved by many nodes;
- All approved transactions are saved on a *blockchain* (a tamper-proof, encrypted, transparent ledger)*;*
- Every participant has a copy of the blockchain.

Cryptocurrencies

- Cryptocurrencies have several advantages:
  - No single point of failure (as long as there are nodes, it works);
  - No intermediaries;
  - Nodes are anonymous (just a series of letters and numbers);
  - Cannot be controlled by governments or banks.

- But cryptocurrencies also have disadvantages (mostly because of anonymity):
- Often used to buy illegal products;
- Not widely accepted;
- Not backed.

How much data does **your** phone generate?

- Do you know which apps are installed on your phone?
- Do you know what data they collect?
- Do you know who has access to your data?

Download our app to find out!

(and anonymously contribute to science)

Visit **vm-thijs.ewi.utwente.nl**

or scan the QR code: