

PRIVACY TECHNOLOGIES

Carmela Troncoso

2nd March 2018

<https://spring.epfl.ch/>



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

GOAL OF THIS LECTURE

Understanding **DIFFERENT CONCEPTIONS OF PRIVACY**
(beyond Data Protection legislation)

Understanding how appropriate **TECHNOLOGIES CAN SUPPORT PRIVACY**
(beyond trust)

Understanding how we **EVALUATE PRIVACY-PRESERVING SYSTEMS**
(beyond risk)

Understanding the **NEED TO PROTECT METADATA**
(beyond data)

THE CONTEXT: UNIQUENESS OF DATA

USERS



PHYSICAL
(BIOMETRICS)

fingerprints



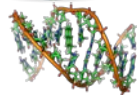
iris



face



DNA



BEHAVIORAL

typing



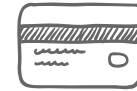
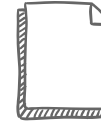
locations



social network



DEVICES

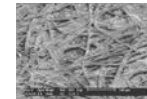


PHYSICAL ("BIOMETRICS")

radio fingerprinting



paper fiber patterns



magnetic behavior

PUFs (Physically Unclonable Functions)

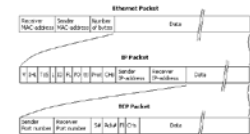
LOGICAL

IP, MAC addresses, IMSI

Certificates



Software, fonts, ...



THE CONTEXT: AVAILABILITY OF DATA

INTELLIGENT DATA-BASED APPLICATIONS

Road pricing

Health monitoring

Children/Elderly trackers

Smart metering

Intelligent buildings

Recommendation systems

Movies (Netflix)

Products (Amazon)

Friends (Social networks)

Music (Spotify, iTunes)

Location based services

Friend finders

Maps

Points of interest

INDIVIDUAL APPLICATIONS ARE LEGITIMATE



TOGETHER THEY BECOME A CHEAP
SURVEILLANCE INFRASTRUCTURE

THE CONTEXT: WE NEED A TRADEOFF SECURITY/PRIVACY!!

“Surveillance is good and privacy is bad for national security. A trade-off is needed!

(SURVEILLANCE == SECURITY) == TRUE ??

not **EFFECTIVE**: smart adversaries evade surveillance

criminals use Telegram, Threema, Signal,...

... but we do not!!

risk of **ABUSE**: lack of transparency and safeguards

Snowden revelations: NSA spying on Americans, companies, ...

Spanish Interior ministry spying independentist politicians

risk of **SUBVERSION** for crime / terrorism

Greek Vodafone scandal (2006): “someone” used the legal interception functionalities (backdoors) to monitor 106 key people: Greek PM, ministers, senior military, diplomats, journalists...

PRIVACY IS A SECURITY PROPERTY

INDIVIDUALS

freedom from intrusion, profiling and manipulation, protection against crime / identity theft, flexibility to access and use content and services, control over one's information

COMPANIES

protection of trade secrets, business strategy, internal operations, access to patents

GOVERNMENTS / MILITARY

protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations

ALL – SHARED INFRASTRUCTURE

telecommunications, operating systems, search engines, on-line shops, software, ...
denying security to some, means denying it to all

AND IT IS IMPORTANT FOR SOCIETY



Daniel Solove,
Prof. of Law

“Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. **A SOCIETY WITHOUT PRIVACY PROTECTION WOULD BE SUFFOCATION**”

Not so much Orwell’s “Big Brother” as Kafka’s “The Trial”:

“...a bureaucracy with inscrutable purposes that uses people’s information to make important decisions about them, yet **DENIES THE PEOPLE THE ABILITY TO PARTICIPATE IN HOW THEIR INFORMATION IS USED**”

“The problems captured by the Kafka metaphor are of a different sort than the problems caused by surveillance. They often do not result in inhibition or chilling. Instead, they are **PROBLEMS OF INFORMATION PROCESSING—THE STORAGE, USE, OR ANALYSIS OF DATA—RATHER THAN INFORMATION COLLECTION.**”

“...not only frustrate the individual by creating a sense of helplessness and powerlessness, but they also **AFFECT SOCIAL STRUCTURE BY ALTERING THE KIND OF RELATIONSHIPS PEOPLE HAVE WITH THE INSTITUTIONS THAT MAKE IMPORTANT DECISIONS ABOUT THEIR LIVES.**”



THE CHEAP SURVEILLANCE
INFRASTRUCTURE

MAY BECOME



ONE RING TO RULE THEM ALL

TAKEAWAYS

DIGITAL IDENTITIES ARE VERY POWERFUL

AND/BUT ENABLE CHEAP “SURVEILLANCE”

PRIVACY IS OF COURSE IS ABOUT SENSITIVE VALUES

BUT ALSO NEEDED FOR SAFEGUARD SOCIETAL AND DEMOCRATIC VALUES

PRIVACY **IS** A SECURITY PROPERTY

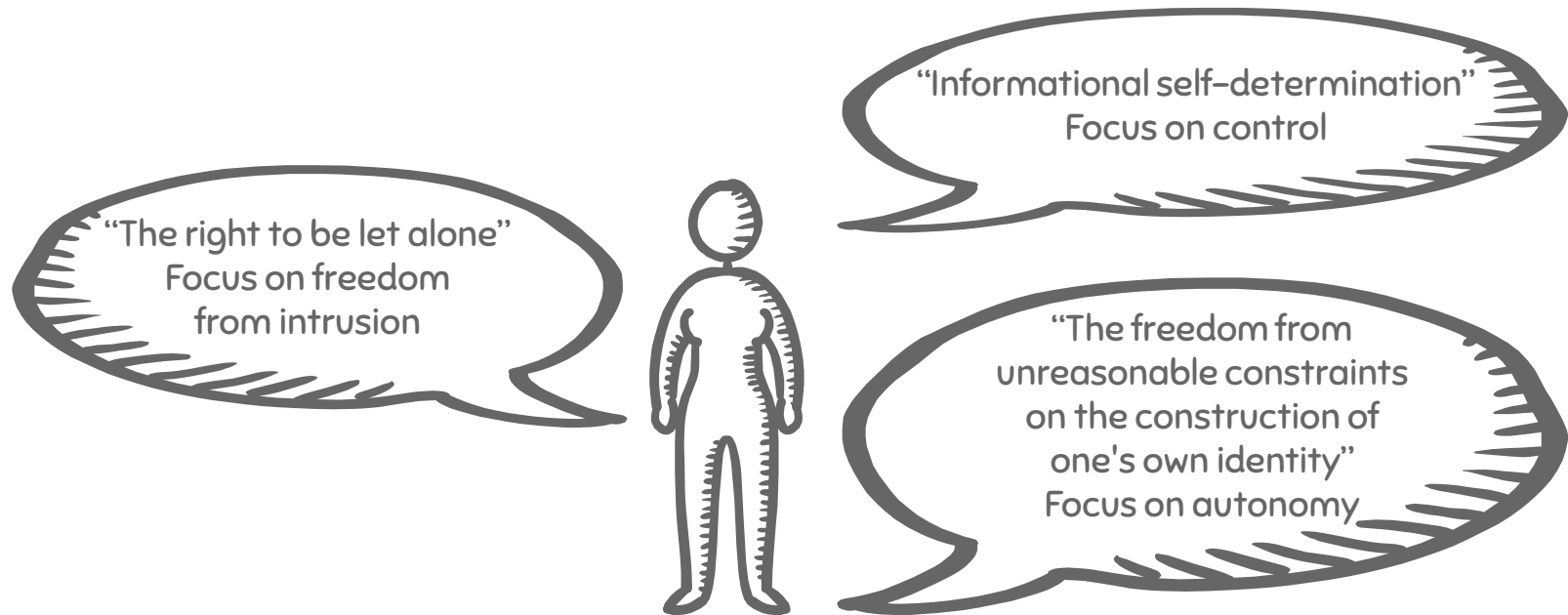
THE NEED FOR A TRADEOFF IS A FALLACY

WHAT IS PRIVACY

Abstract and subjective concept, hard to define

Dependent on cultural issues, study discipline, stakeholder, context

Popular definitions:



WHAT IS PRIVACY IN PRIVACY ENHANCING TECHNOLOGIES

3 different flavors depending on ...

the “privacy” concept they embed

their goals

their challenges and limitations

Gürses, Seda, and Claudia Diaz. "Two tales of privacy in online social networks." IEEE Security & Privacy 11.3 (2013): 29–37.

Diaz, Claudia, and Seda Gürses. "Understanding the landscape of privacy technologies." Information Security Summit (2012): 58–63.

Danezis, George, and Seda Gürses. "A critical review of 10 years of privacy technology." Surveillance cultures: a global surveillance society (2010): 1–16.

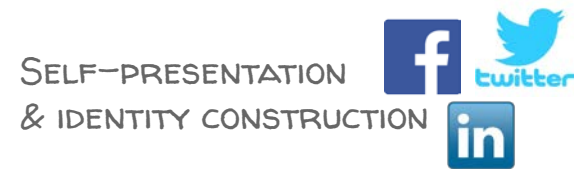
“SOCIAL PRIVACY”: CONCERNS

Technology brings problems for the user

“My parents discovered I'm gay”

“My boss knows I am looking for other job”

“My friends saw my naked pictures”



PRIVACY VS PUBLICITY TENSION

Decision making

Cognitive overload

Bounded rationality

Immediate gratification

WHO DEFINES THE PRIVACY PROBLEM: **USERS**

"SOCIAL PRIVACY": GOALS

Meet privacy expectations: "DON'T SURPRISE THE USER"

TWO MAIN APPROACHES

- Support decision making

 - Privacy controls visible and easy to use

 - Predict actions to avoid regret

Help users develop appropriate privacy practices

APPROPRIATE DEFAULTS: only friends

EASY CONFIGURATION: automated grouping

CONTEXTUAL FEEDBACK: "how X sees my profile"

PRIVACY NUDGES: force to reconsider
Audience, time, sentiment,...



“SOCIAL PRIVACY”: LIMITATIONS

Focus on concerns directly related to actions (and implicit?)

Front-end oriented

No info about the server, only privacy towards third parties



COMMON INDUSTRY APPROACH
MAKE USERS COMFORTABLE

Limited by user understanding

As much as policies can do...

Based on average consumer



Based on privacy expectations

What if expectations are null....

“INSTITUTIONAL PRIVACY”: CONCERNS

Data COLLECTED without users' awareness or *informed consent*
Data PROCESSED for illegitimate purposes

Data SECURITY

correctness, integrity, deletion
Information not becoming public
Safety (crime protection, stalking,...)

WHO DEFINES THE PRIVACY PROBLEM: LEGISLATION
GENERAL DATA PROTECTION REGULATION

“INSTITUTIONAL PRIVACY”: GOALS

Ensure compliance with data protection principles:

informed consent

purpose limitation

data minimization

subject access rights

APPROPRIATE DEFAULTS: towards organization!

EASY CONFIGURATION: policy negotiation with organization

Data SECURITY

Prevent (or mitigate) data breaches

ACCESS CONTROL: limit and log who accesses what

“PRIVATE” DATA PUBLISHING: anonymization

Auditability and accountability

“INSTITUTIONAL PRIVACY”: LIMITATIONS

Assumes:

- collection and processing by organizations is necessary
- organizations are (semi)–trusted and honest
 - Reliance on punishment
 - No technical protection of the data

Focuses on limiting misuse, **NOT** collection

- Easy to circumvent minimization to collect in bulk
- Auditing may require more data!
- The danger of *informed consent*: if compliant is ok!

COMMON INDUSTRY APPROACH
MAKE USERS COMFORTABLE
+ LEGAL COMPLIANCE!!



Limited

- Scope (personal data != all data)
- transparency (proprietary sw and algorithms)

“ANTI-SURVEILLANCE PRIVACY”: CONCERNS

Data disclosure **BY DEFAULT** through ICT infrastructure

Threat model **ANYBODY** that may see the data

ISP

Service provider

Government

Concerned about

Surveillance

Censorship

Other democratic values:

Freedom speech

Freedom association

Democracy itself!



WHO DEFINES THE PRIVACY PROBLEM: **SECURITY EXPERTS**

“ANTI-SURVEILLANCE PRIVACY”: GOALS

Prevent/minimize default disclosure of personal information anyone:

Only information explicitly disclosed is made available to intended recipients
(confidentiality)

Both user-generated and implicit!

Circumvent censorship



Minimize the need to trust others

Distribute trust by avoiding single points of failure



END-TO-END ENCRYPTION: PGP, OTR

ANONYMOUS COMMS: Tor

OBFUSCATION:

- dummy actions
- hiding
- generalization

ADVANCED CRYPTO:

- Private information retrieval
- Anonymous authentication
- Multiparty computation
- Blind signatures
- Cryptographic commitments

“ANTI-SURVEILLANCE PRIVACY”: LIMITATIONS

Making secure private designs is hard

- “Narrow” tools

- Difficult to combine

Usability problems

- For developers:

 - how the @\$%&#\$Ŷ& do I program this?

 - performance

- For users:

 - Unintuitive

Incentives are low

- For providers: they lose the data!

- For governments: national security, fraud detection, surveillance & control

TAKEAWAYS

PRIVACY CAN BE UNDERSTOOD IN MANY WAYS

WHO SETS THE PROBLEM?

WHO IS THE ADVERSARY?

TAKEAWAYS

PRIVACY CAN BE UNDERSTOOD IN MANY WAYS

WHO SETS THE PROBLEM?

WHO IS THE ADVERSARY?

ANTI SURVEILLANCE PETS

WHAT ARE THEY? WHAT DO THEY DO?

ANTI-SURVEILLANCE PETS



CRYPTOGRAPHY → CONFIDENTIALITY!

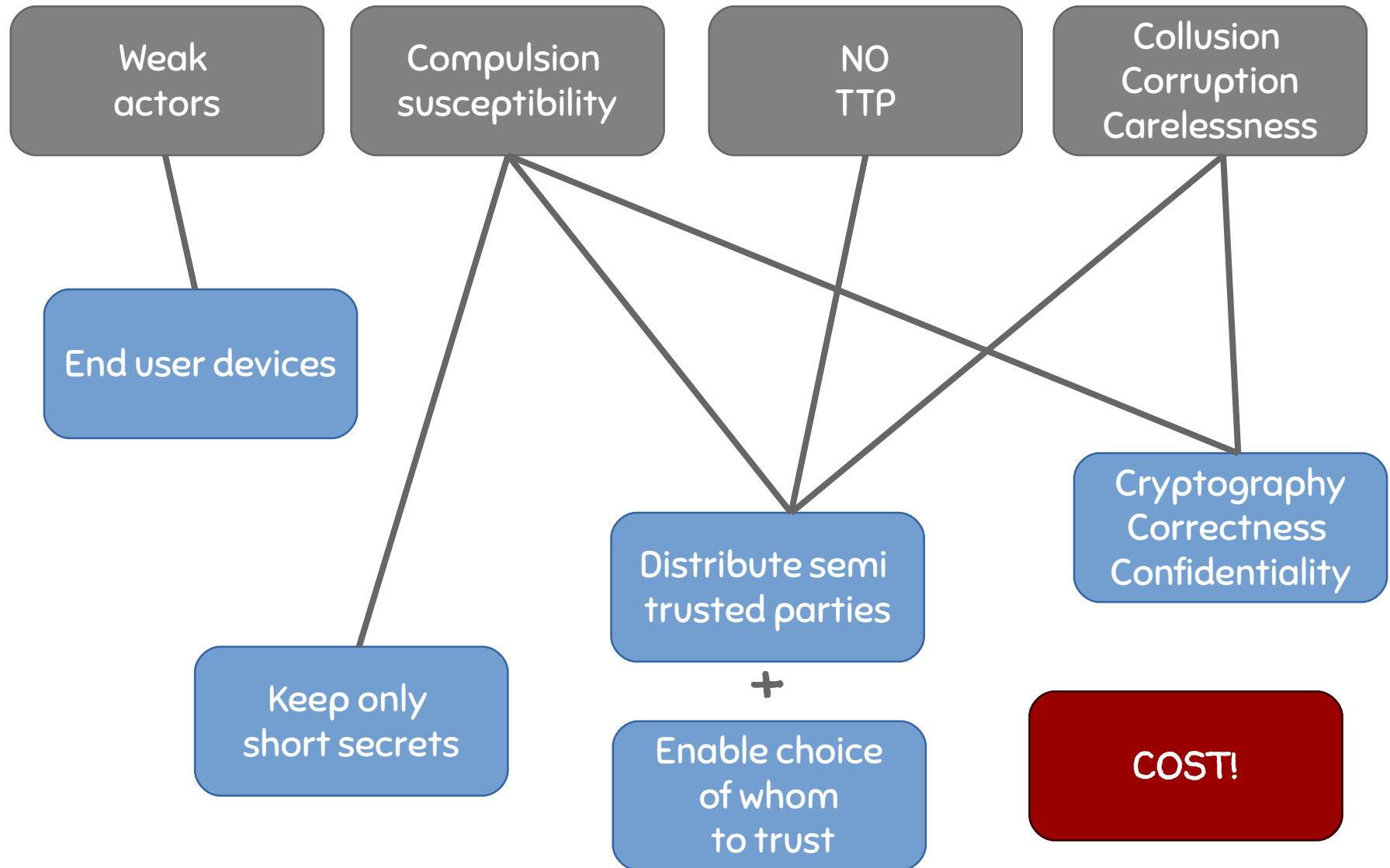
TRADITIONAL: computer security context

PRIVACY A BIT DIFFERENT THAN TRADITIONAL CONFIDENTIALITY.

WHAT MAKES PRIVACY ENHANCING TECHNOLOGIES (PETs) DIFFERENT:

- Threat model: WEAK actors, POWERFUL adversaries.
- Susceptibility to COMPULSION.
- Cannot assume the existence of TRUSTED THIRD PARTIES (TTP):
- Also worry about COST, COLLUSION, CORRUPTION, CARELESSNESS.

ANTI-SURVEILLANCE PETS – DESIGN PRINCIPLES

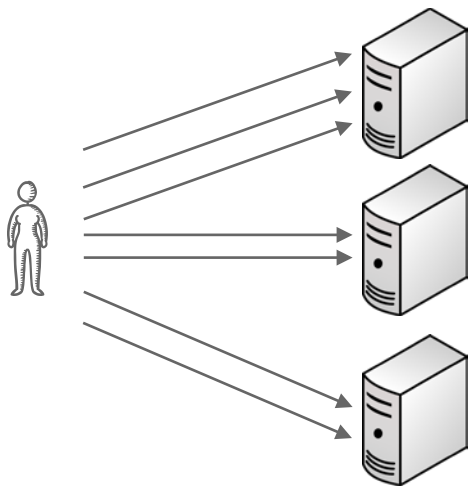


“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

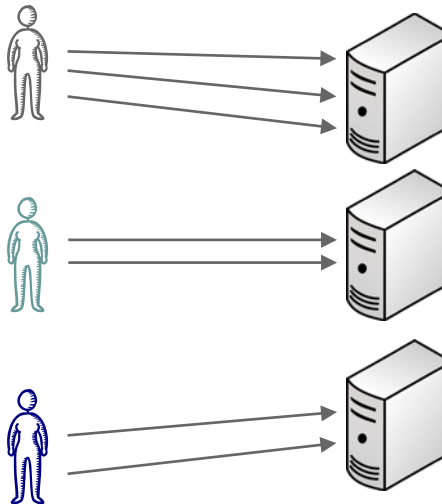
PRIVACY PROPERTIES: PSEUDONIMITY

–PFITZMANN–HANSEN: “the use of pseudonyms as IDs [...] A digital pseudonym is a bit string which is unique as ID and which can be used to authenticate the holder”

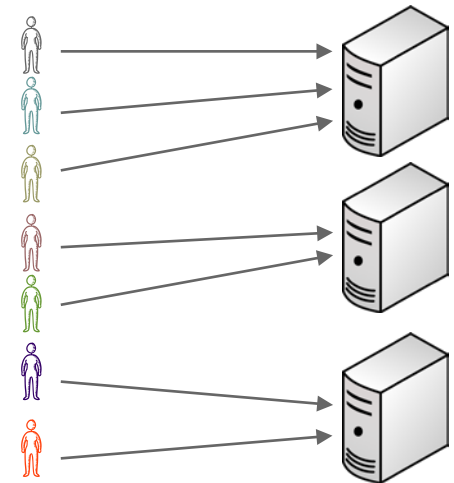
–ISO 15408: “a user may use a resource or service without disclosing its identity, but can still be accountable for that use.”



IDENTITY



PSEUDONYMITY



ANONYMITY

Pfitzmann, Andreas and Hansen, Marit. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. 2010.

“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: ANONYMITY

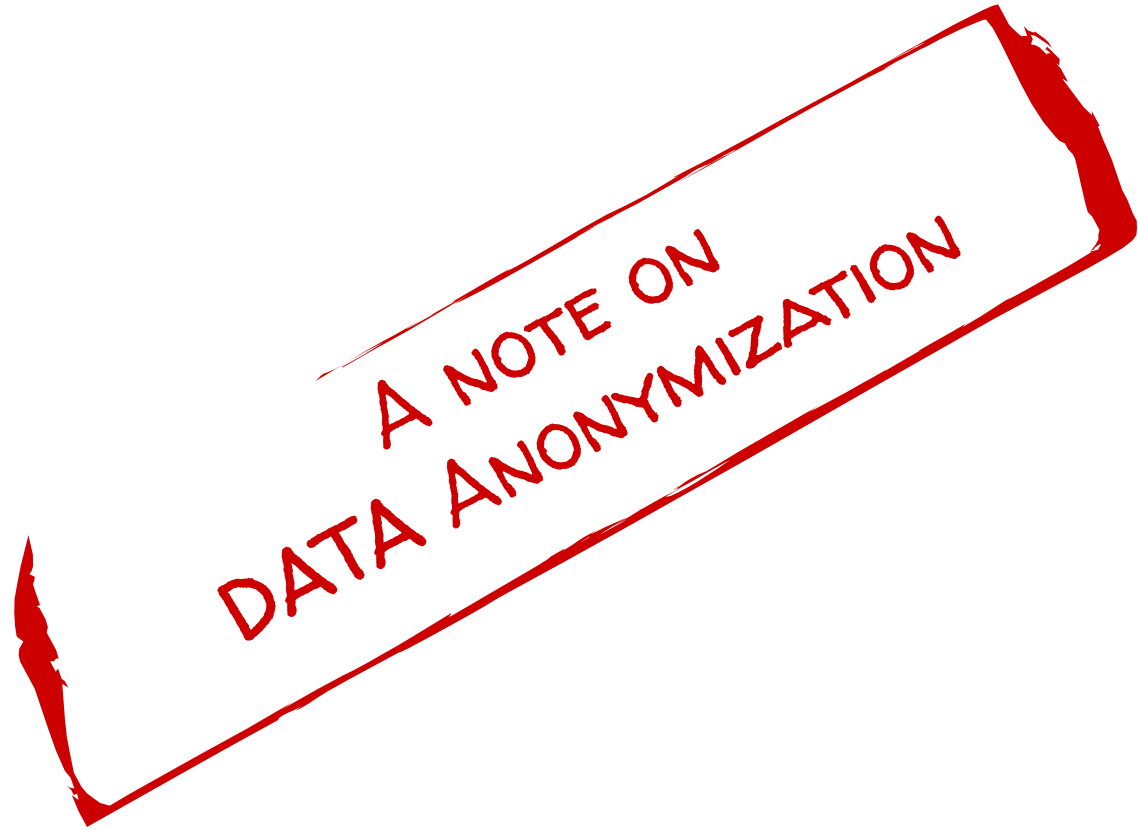
–PFITZMANN–HANSEN: “Anonymity is the state of being not identifiable within a set of subjects, the anonymity set [...] The anonymity set is the set of all possible subjects who might cause an action”

–ISO 29100: “a characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly”

Who is...

- ...the reader of a web page, the person accessing a service
- ...the sender of an email, the writer of a text
- ...the person to whom an entry in a database relates
- ...the person present in a physical location

DECOUPLING IDENTITY
AND ACTION!



“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: ANONYMITY



“Wouldn't it be nice if... you could take a dataset full of private data, and transform it into one with no private data – while keeping all the value of the data?”

(by decoupling data from identities)

“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: ANONYMITY



“Wouldn't it be nice if... you could take a dataset full of private data, and transform it into one with no private data – while keeping all the value of the data?”



MAGICAL THINKING!

THIS CANNOT HAPPEN IN GENERAL!

There are gazillion techniques for at data anonymization

- Remove identifiers (removing, hashing, encrypting)

- Add noise (values, graph)

- Generalise (k-anonymity, cloaking, ...)



“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: ANONYMITY

1) IS IT STILL POSSIBLE TO SINGLE OUT AN INDIVIDUAL

On the Anonymity of Home/Work Location Pairs

Philippe Golle and Kurt Partridge

Palo Alto Research Center
{pgolle, kurt}@parc.com

Unique in the Crowd: The privacy bounds of human mobility

Yves-Alexandre de Montjoye^{1,2}, César A. Hidalgo^{3,4}, Michal Verleyen² & Vincent D. Blondel^{1,5}

Abstract. Many applications benefit from user location data raises privacy concerns. Anonymizing

location

“the median size of the individual's anonymity set in the U.S. working population is 1, 21 and 34,980, for locations known at the granularity of a census block, census tract and county respectively”

“if the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals.” [15 monthsh, 1.5M people]

We study fifteen months of human mobility data for one and a half million individuals and find that human mobility traces are highly unique. In fact, in a dataset where the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals. We coarsen the data spatially and temporally to find a

L. Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh 2009.

Simple Demographics Often Identify People Uniquely

How Unique is Your Browser? *a report on the Panoptick experiment*



Peter Eckersley
Senior Staff Technologist
Electronic Frontier Foundation
pde@eff.org

83.6% had completely unique fingerprints
(entropy: 18.1 bits, or more)

94.2% of “typical desktop browsers” were unique
(entropy: 18.8 bits, or more)

web browser

“It was found that 87% (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on {5-digit ZIP, gender, date of birth}”

Latanya Sweeney
Carnegie Mellon University
latanya@andrew.cmu.edu

“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: ANONYMITY

2) LINK TWO RECORDS WITHIN A DATASET (OR DATASETS)

De-anonymizing Social Networks

Arvind Narayanan and Vitya Shmatikov
The University of Texas at Austin

Abstract

Operators of online social networks are increasingly sharing potentially sensitive information about users and their relationships with advertisers, application developers, and data-mining researchers. Privacy is typically protected by anonymization, i.e., removing names, addresses, etc.

We present a framework for analyzing privacy and anonymity in social networks and develop a new re-identification algorithm targeting anonymized social-network graphs. To demonstrate its effectiveness on real-

associated with individual nodes are suppressed. Such suppression is often misinterpreted as removal of “personally identifiable information” (PII), even though PII may include much more than names and identifiers (see the discussion in Appendix D). For example, the EU privacy directive defines “personal data” as “any information relating to an identified or identifiable natural person [...]”; an identifiable person is one who can be identified, directly or indirectly, in particular by one or more factors such as racial, ethnic, economic

take two graphs representing social networks and map the nodes to each other based on the *graph structure alone*—no usernames, no nothing
NETFLIX PRIZE, KAGGLE CONTEST

An Automated Social Graph De-anonymization Technique

Kumar Sharad
University of Cambridge, UK
kumar.sharad@cl.cam.ac.uk

George Danezis
University College London, UK
g.danezis@ucl.ac.uk

social graphs

ABSTRACT

We present a generic and automated approach to re-identifying nodes in anonymized social networks which enables novel anonymization techniques to be quickly evaluated. It uses machine learning to discover features which distinguish pairs of nodes in disparate anonymized sub-graphs. The technique involves inferring and in-

Social network graphs in particular are high dimensional and feature rich data sets, and it is extremely hard to preserve their anonymity. Thus, any anonymization scheme has to be evaluated in detail, including those with a sound theoretical basis [11]. Techniques have been proposed to resist de-anonymization [8, 17, 22], however, Dwork and Naor have shown [7] that preserving privacy of

Technique to automate graph de-anonymization based on machine learning.
Does not need to know the algorithm!

Authorship attribution also works across domains!!

DE GRUYTER OPEN

Proceedings on Privacy Enhancing Technologies · 2016 (3):155–171

Rebekah Overdori^{1*} and Rachel Greenstadt

Blogs, Twitter Feeds, and Reddit Comments: Cross-domain Authorship Attribution

Abstract: Stylometry is a form of authorship attribution that relies on the linguistic information to attribute

curity by serving as a verification or identification tool for digital text across the Internet.

As social media and micro-blogging sites increase in popularity, so does the need to identify the authors of these types of text. The accuracy with which stylometry can identify anonymous and pseudonymous authors has direct security implications. It can be used for verification of a person's claimed identity, or to identify the author of an anonymous threat should a threat occur.

Doppelgänger Finder: Taking Stylometry To The Underground

Sadia Afroz¹, Aylin Caliskan-Islam¹, Ariel Stolerman¹, Rachel Greenstadt¹ and Damon McCoy²
¹University of California, Berkeley ²Drexel University ³George Mason University

Link messages from same person with different pseudonyms

Abstract—Stylometry is a method for identifying anonymous authors of anonymous texts by analyzing their writing style. While stylometric methods have produced impressive results in previous experiments, we wanted to explore their performance on a challenging dataset of particular interest to the security research community. Analysis of underground forums can provide key information about who controls a given bot network or who is involved in the sale and use of the information

Other information gleaned from underground forums is providing security researchers, law enforcement, and policy makers valuable information on how the market is segmented and specialized, the social dynamics of the community, and potential bottlenecks that are vulnerable to interventions. These advances have been accomplished primarily through

stylometry

“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: ANONYMITY

3) INFER INFORMATION ABOUT AN INDIVIDUAL

Inference Attacks on Location Tracks

John Krumm

Microsoft Research
One Microsoft Way
Redmond, WA, USA
jckrumm@microsoft.com

Abstract. Although the privacy threats and countermeasures associated with location data are well known, there has not been a thorough experiment to assess the effectiveness of either. We examine location data gathered from volunteer subjects to quantify how well four different algorithms can identify

“Based on GPS tracks from, we identify the latitude and longitude of their homes. From these locations, we used a free Web service to do a reverse “white pages” lookup, which takes a latitude and longitude coordinate as input and gives an address and name. [172 individuals]”

“I Know What You Did Last Summer” — Query Logs and User Privacy

Rosie Jones Ravi Kumar Bo Pang Andrew Tomkins
Yahoo! Research, 701 First Ave, Sunnyvale, CA 94089.
{jonesr,ravikumar,bopang,atomkins}@yahoo-inc.com

“We investigate the subtle cues to user identity that may be exploited in attacks on the privacy of users in web search query logs. We study the application of simple classifiers to map a sequence of queries into the gender, age, and location of the user issuing the queries.”

ABSTRACT

We investigate the subtle cues to user identity that may be exploited in attacks on the privacy of users in web search query logs. We study the application of simple classifiers to map a sequence of queries into the gender, age, and location of the user issuing the queries. We then show how these classifiers may be carefully combined at multiple granularities to map a sequence of queries into a

bilities; this is the goal of this paper. We initiate the study of subtle cues to user identity that exist as vulnerabilities in web search query logs, which may be exploited in attacks on the privacy of users.

Privacy attack models. We begin with a characterization of two key forms of attack against which a query log privacy scheme must be resilient. The first is a *trace attack*, in which an attacker studies a privacy-enhanced version of a sequence of searches (*trace*) made

“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: ANONYMITY

MAGICAL THINKING!
THIS CANNOT HAPPEN IN GENERAL!



DATA ANONYMIZATION IS A WEAK PRIVACY MECHANISM

ONLY TO BE USED WHEN OTHER PROTECTIONS ARE ALSO APPLIED.

(CONTRACTUAL, ORGANIZATIONAL)

IMPOSSIBLE TO SANITISE WITHOUT SEVERELY DAMAGING USEFULNESS

REMOVING PII IS NOT ENOUGH! – ANY ASPECT COULD LEAD TO RE-IDENTIFICATION

RISK OF DE-ANONYMIZATION? PROBABILISTIC ANALYSIS
 $\Pr[\text{identity} \rightarrow \text{action} \mid \text{observation}]$

WHAT DO WE WANT THE DATA FOR...? STATISTICS!



“Wouldn't it be nice if I could send complex queries to a database to extract statistics, and it returned results that are informative, but leak very little information about any individual?”

QUERY-BASED PRIVACY
DIFFERENTIAL PRIVACY!



Why is that possible (while anonymization was impossible):

The final result DEPENDS ON MULTIPLE PERSONAL RECORDS

However it DOES NOT DEPEND MUCH ON ANY PARTICULAR ONE (sensitivity)

Therefore adding a little bit of noise to the result, suffices to hide any record contribution

For full anonymization.... one would need to add a lot of noise to all the entries



DIFFERENT ARCHITECTURE TO PROVIDE ROBUST PRIVACY!

A TTP HOLDS THE DATA!

ACTUALLY AFTER SOME USES... UTILITY DROPS

BETTER SUITED FOR ONE-TIME USE → DATA COLLECTION!

END -- A NOTE ON
DATA ANONYMIZATION

“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: UNLINKABILITY

-PFITZMANN-HANSEN: “two or more items within a system, are no more and no less related than they are related concerning the a-priori knowledge”

- ISO15408: “a user may make multiple uses of resources or services without others being able to link these uses together”

Two...

- ... anonymous letters written by the same person
- ... web page visits by the same user
- ... entries in a databases related to the same person
- ... two people related by a friendship link
- ... same person spotted in two locations

PROBABILISTIC ANALYSIS – $\Pr[\text{item A} \longleftrightarrow \text{item B} \mid \text{observation}]$

“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: UNOBSERVABILITY

– PFITZMANN–HANSEN: “an items of interest being indistinguishable from any item of interest at all [...] Sender unobservability then means that it is not noticeable whether any sender within the unobservability set sends.”

– ISO15408: “a user may use a resource or service without others, especially third parties, without being able to observe that the resource or service is being used.”

Hiding...

...whether someone is accessing a web page

...whether an entry in a database corresponds to a real person

...whether someone or no one is in a given location

PROBABILISTIC ANALYSIS – $\Pr[\text{real} \mid \text{fake, observation}]$

“DUMMY” ACTIONS



“ANTI-SURVEILLANCE PETS” TECHNICAL GOALS

PRIVACY PROPERTIES: PLAUSIBLE DENIABILITY

- Not possible to prove user knows, has done or has said something
- Resistance to coercion:
 - Not possible to prove that a person has hidden information in a computer
 - Not possible to know that someone has the combination of a safe

Not possible to prove ...

- ... that a person has hidden information in a computer
- ... that someone has the combination of a safe
- ... that a person has been in a place at a certain point in time
- ... that a database record belongs to a person

PROBABILISTIC ANALYSIS – $\Pr[\text{fake} \mid \text{real, observation}]$

PRIVACY EVALUATION IS A PROBABILISTIC ANALYSIS

SYSTEMATIC REASONING TO EVALUATE A MECHANISM

Anonymity – $\Pr[\text{identity} \rightarrow \text{action} \mid \text{observation}]$

Unlinkability – $\Pr[\text{action A} \leftrightarrow \text{action B} \mid \text{observation}]$

Obfuscation – $\Pr[\text{real action} \mid \text{observed noisy action}]$



1) MODEL THE PRIVACY-PRESERVING
MECHANISM AS A PROBABILISTIC
TRANSFORMATION

IF IT IS NOT PROBABILISTIC, IT IS NOT SECURE

2) DETERMINE WHAT THE ADVERSARY WILL SEE

3) “INVERT” THE MECHANISM AS THE ADVERSARY WOULD DO
THE ADVERSARY KNOWS!!!

4) COMPUTE PROBABILITY AFTER “INVERSION”

5) MEASURE... MEAN ERROR, ENTROPY (ANY FLAVOUR), DIFF. PRIVACY

“INVERSION”? WHAT DO YOU MEAN?

1) ANALYTICAL MECHANISM INVERSION

GIVEN THE DESCRIPTION OF THE SYSTEM, DEVELOP THE MATHEMATICAL EXPRESSIONS THAT EFFECTIVELY INVERT THE SYSTEM:

$$\text{Pr}[\text{OBS} \mid \text{REAL DATA}, \text{PET}] \rightarrow \text{Pr}[\text{REAL DATA} \mid \text{OBS}, \text{PET}]$$



NOT ALWAYS POSSIBLE – MAY REQUIRE APROX. OR SAMPLING

2) MACHINE LEARNING (DATA DRIVEN)

TRAIN A CLASSIFIER TO BREAK THE MECHANISMS!

ONLY POSSIBLE IF ENOUGH DATA (THOUGH DATA CAN BE CREATED)



MUST TAKE INVERSION INTO ACCOUNT!! SYSTEMATIC DESIGN!!!

TAKEAWAYS

PRIVACY CAN BE FORMALIZED IN DIFFERENT WAYS

IMPLEMENT DIFFERENT PROTECTIONS

ANONYMIZATION IS HARD

WEAK PROTECTION! USE CAREFULLY

PRIVACY IS A PROBABILISTIC CONCEPT

EXAMPLES OF PRIVACY ENHANCING TECHNOLOGIES

“ANTI-SURVEILLANCE PRIVACY”: GOALS

Prevent/minimize default disclosure of personal information anyone:

Only information explicitly disclosed is made available to intended recipients
(confidentiality)

Both user-generated and implicit!

Circumvent censorship



Minimize the need to trust others

Distribute trust by avoiding single points of failure



END-TO-END ENCRYPTION: PGP, OTR

ANONYMOUS COMMS: Tor

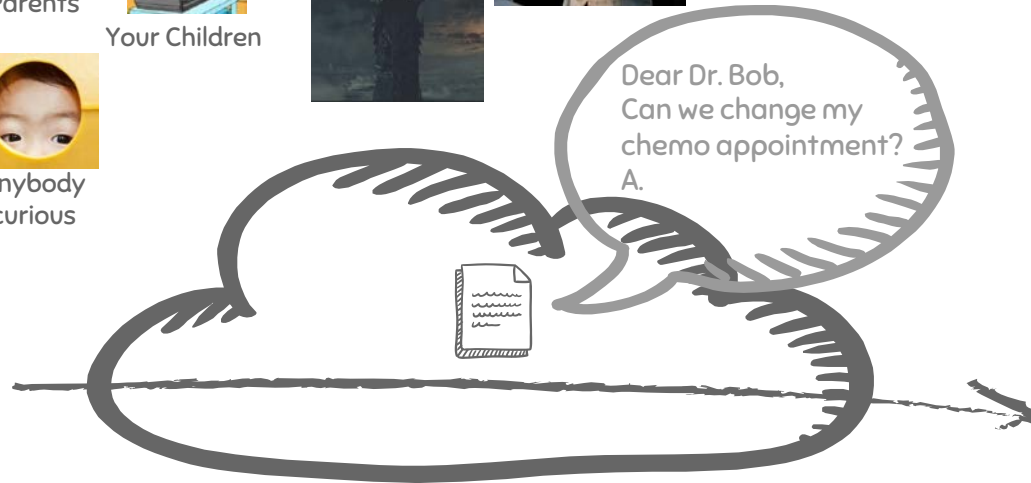
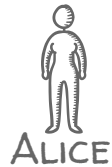
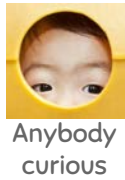
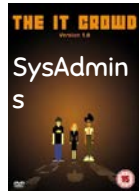
OBFUSCATION:

- dummy actions
- hiding
- generalization

ADVANCED CRYPTO:

- Private information retrieval
- Anonymous authentication
- Multiparty computation
- Blind signatures
- Cryptographic commitments

THE ADVERSARY IS ANYONE AND VERY POWERFUL

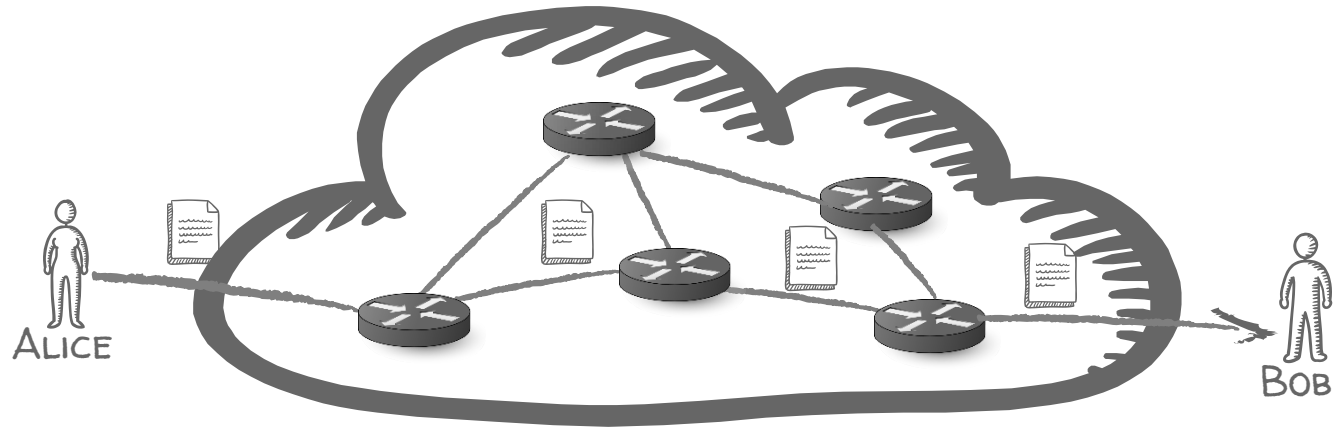


A NETWORK

END TO END ENCRYPTION

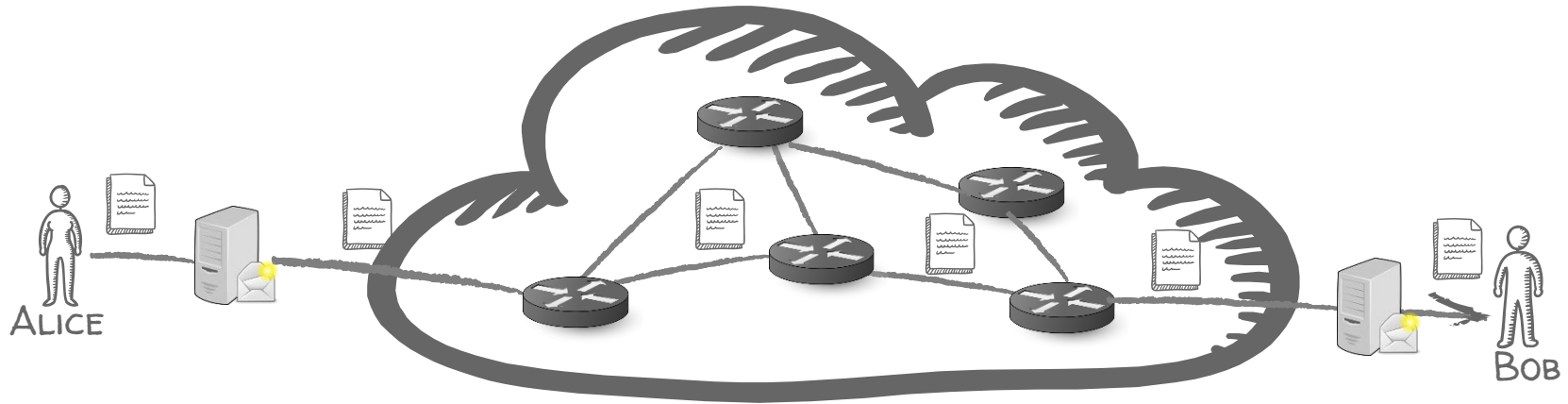


END TO END ENCRYPTION



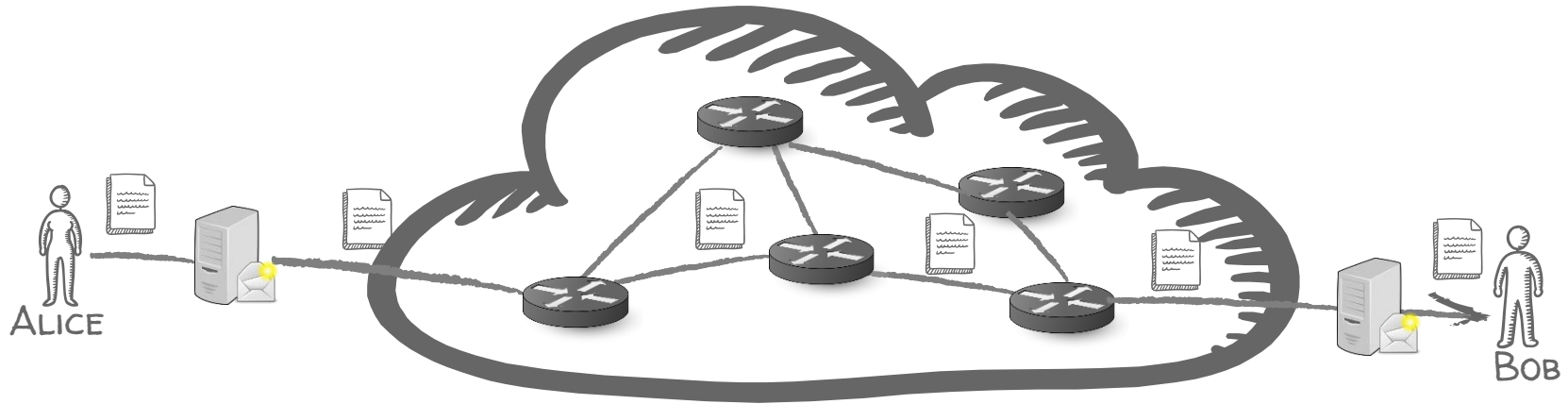
A NETWORK

END TO END ENCRYPTION



A NETWORK

END TO END ENCRYPTION



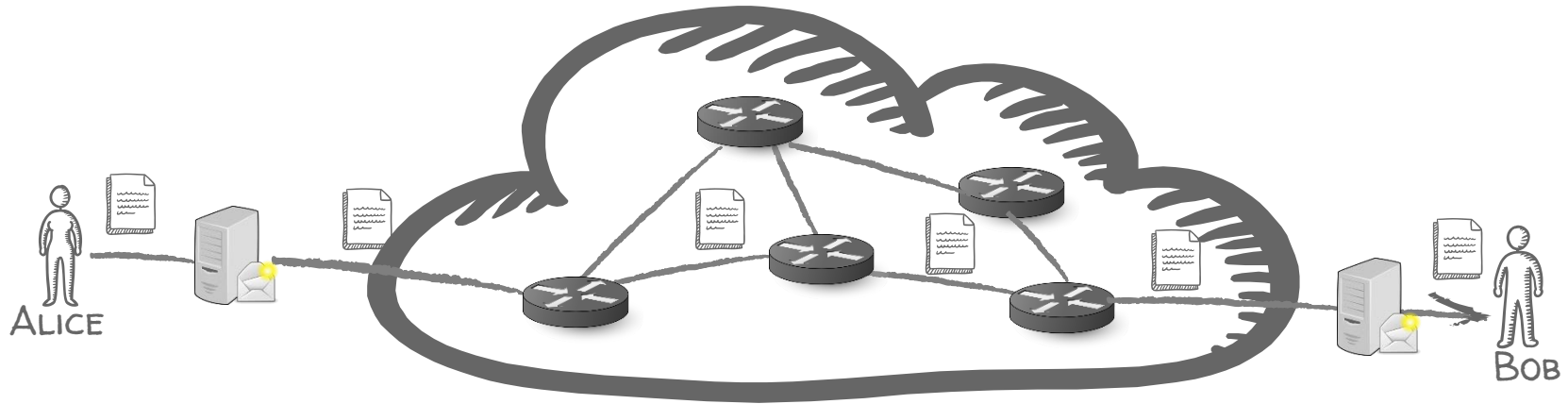
A NETWORK



CRYPTOGRAPHY → CONFIDENTIALITY!

END TO END ENCRYPTION

WHAT IS AN END?



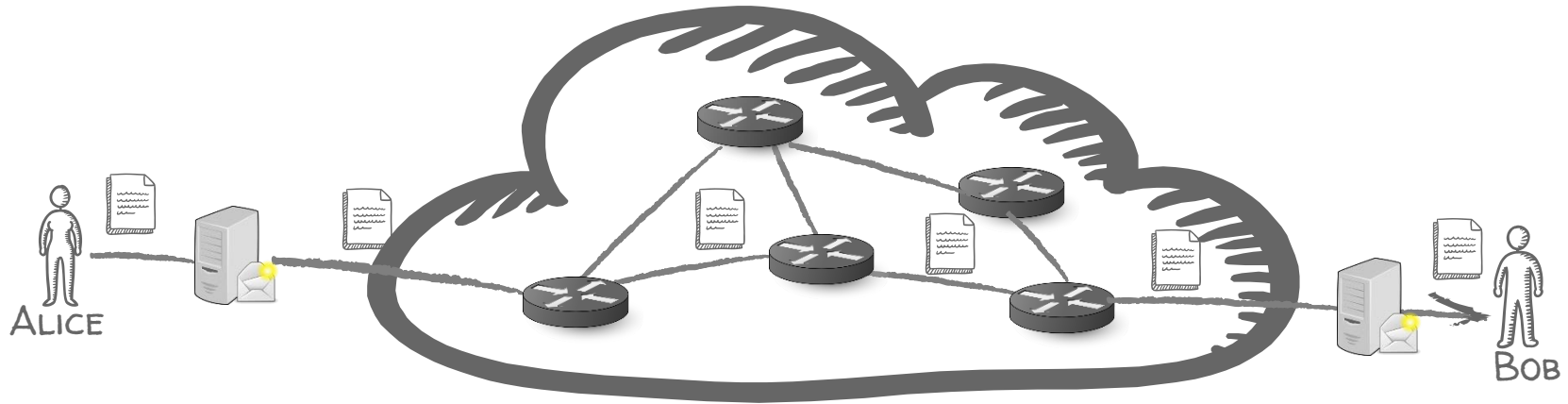
A NETWORK



CRYPTOGRAPHY → CONFIDENTIALITY!

END TO END ENCRYPTION

WHAT IS AN END?
(ePRIVACY REGULATION→?)



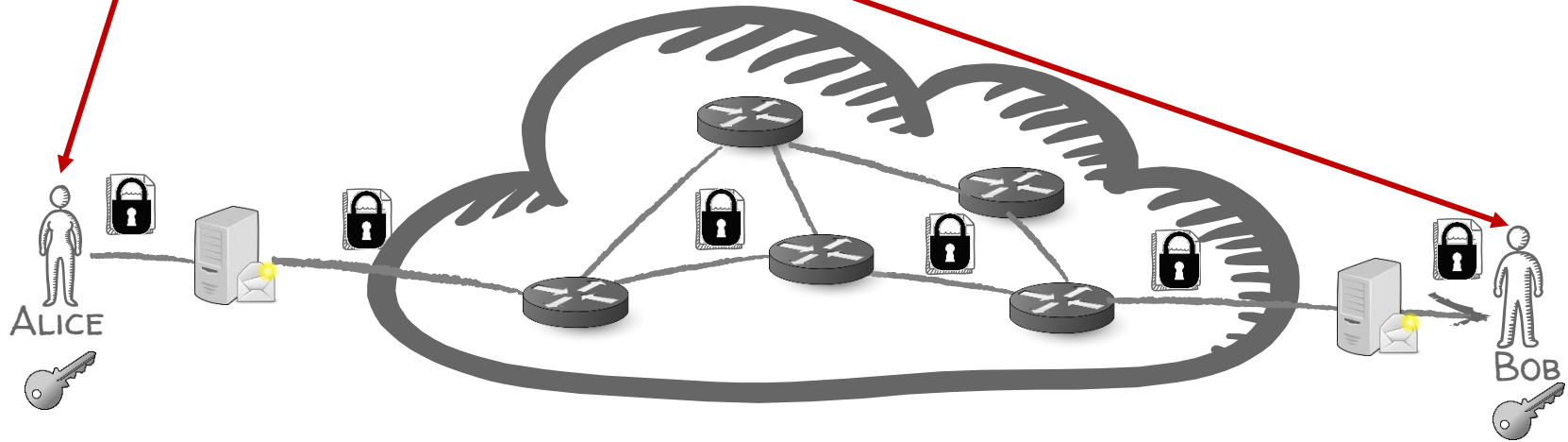
A NETWORK



CRYPTOGRAPHY → CONFIDENTIALITY!

END TO END ENCRYPTION

WHAT IS AN END?
(ePRIVACY REGULATION → ?)



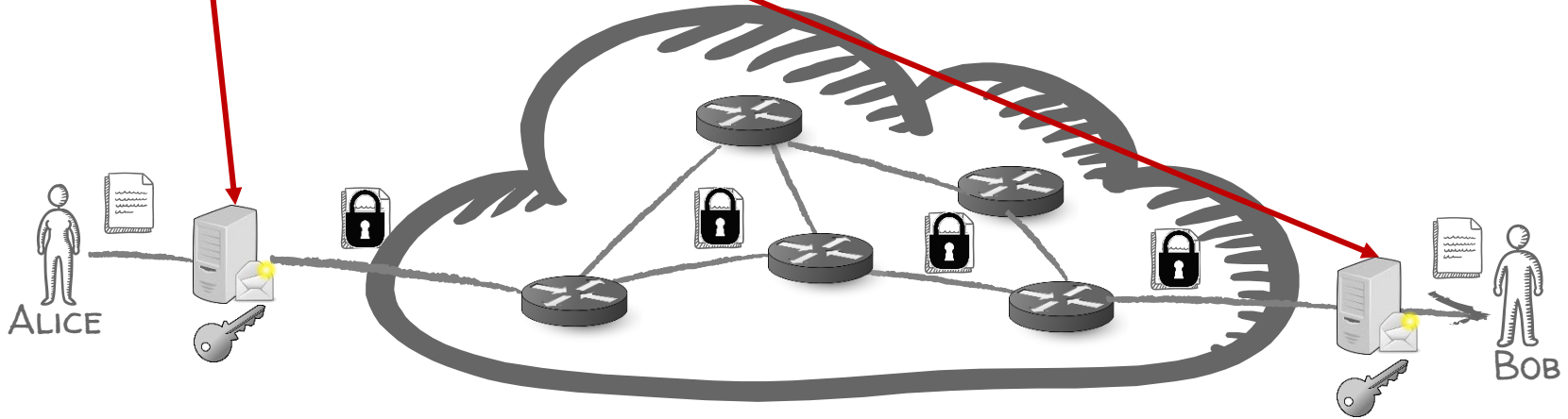
A NETWORK



CRYPTOGRAPHY → CONFIDENTIALITY!

END TO END ENCRYPTION

WHAT IS AN END?
(ePRIVACY REGULATION → ?)



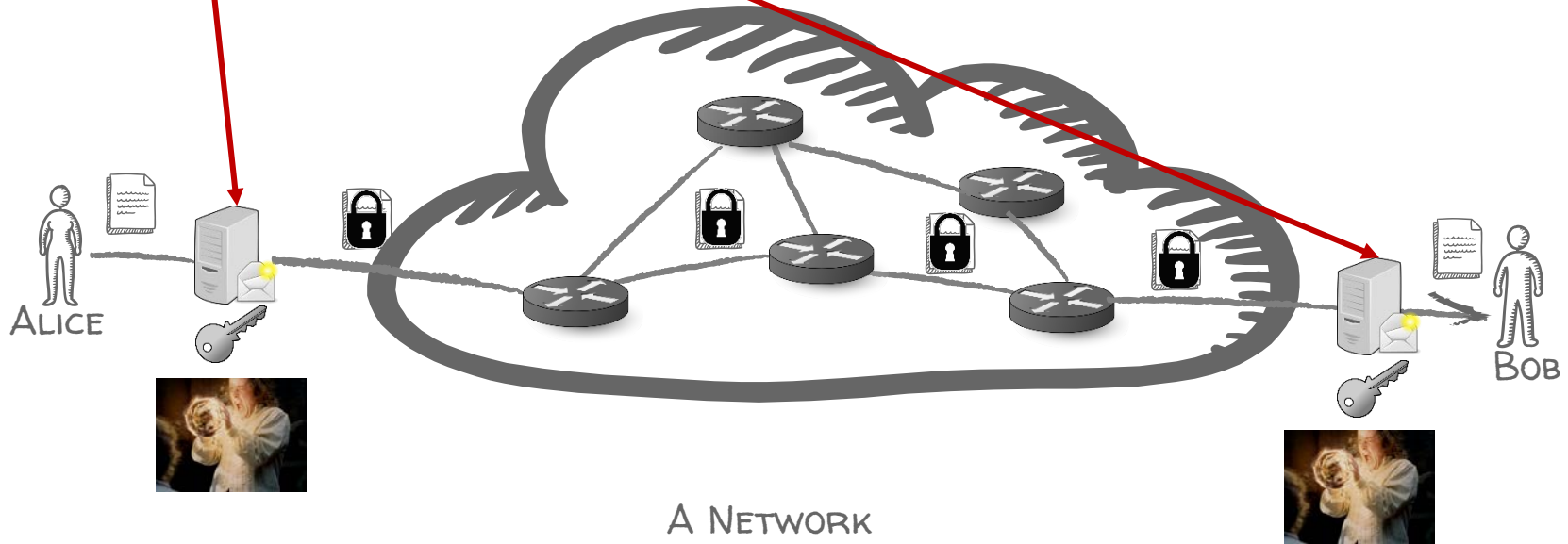
A NETWORK



CRYPTOGRAPHY → CONFIDENTIALITY!

END TO END ENCRYPTION

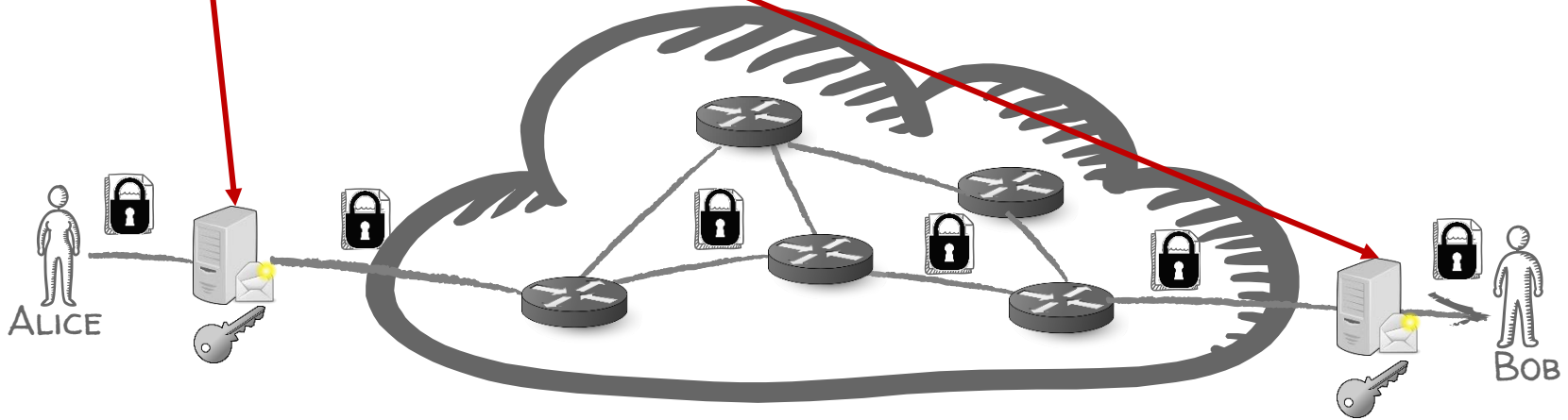
WHAT IS AN END?
(ePRIVACY REGULATION → ?)



CRYPTOGRAPHY → CONFIDENTIALITY!

END TO END ENCRYPTION

WHAT IS AN END?
(ePRIVACY REGULATION → ?)



A NETWORK



CRYPTOGRAPHY → CONFIDENTIALITY!



HOW TO KNOW WHICH END IS CONSIDERED?

PERFECT FORWARD SECRECY



CRYPTOGRAPHY → CONFIDENTIALITY!



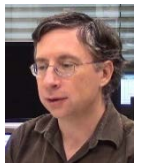
Compulsion
susceptibility

BUT WHAT IF SOMEONE FORCES YOU TO DISCLOSE THE KEY?

PERFECT FORWARD SECRECY (PFS)

- 1) Start with keys that allow Alice to authenticate Bob.
 - Public key encryption
- 2) Alice and Bob create fresh public keys and exchange them
- 3) They establish fresh shared keys, and talk secretly
 - Diffie Hellman
- 4) Once done, they delete the shared keys.

PERFECT FORWARD SECRECY



ONE-TIME USE KEYS: EPHEMERAL KEYS

AFTER A CONVERSATION IS OVER
NO-ONE CAN DECRYPT WHAT WAS SAID!!!

PLAUSIBLE
DENIABILITY

DESIGN
PRINCIPLES

End user devices

Keep only
short secrets

Cryptography
Correctness
Confidentiality



SECURE
COMMUNICATIONS

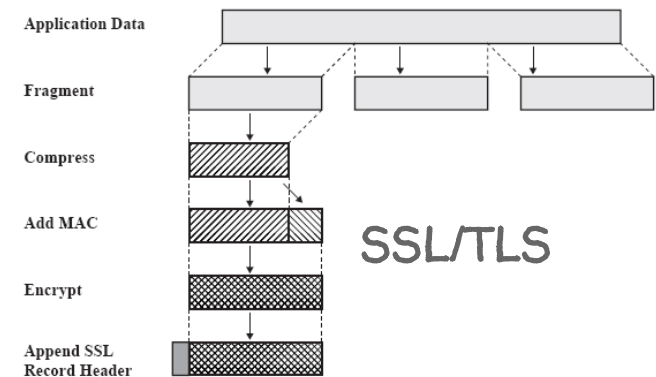
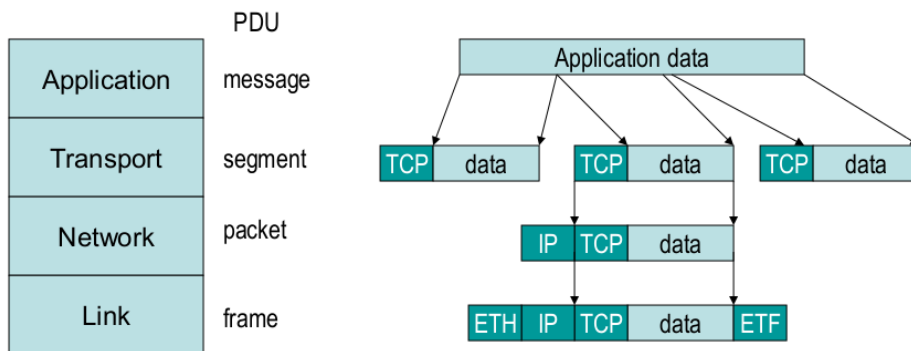
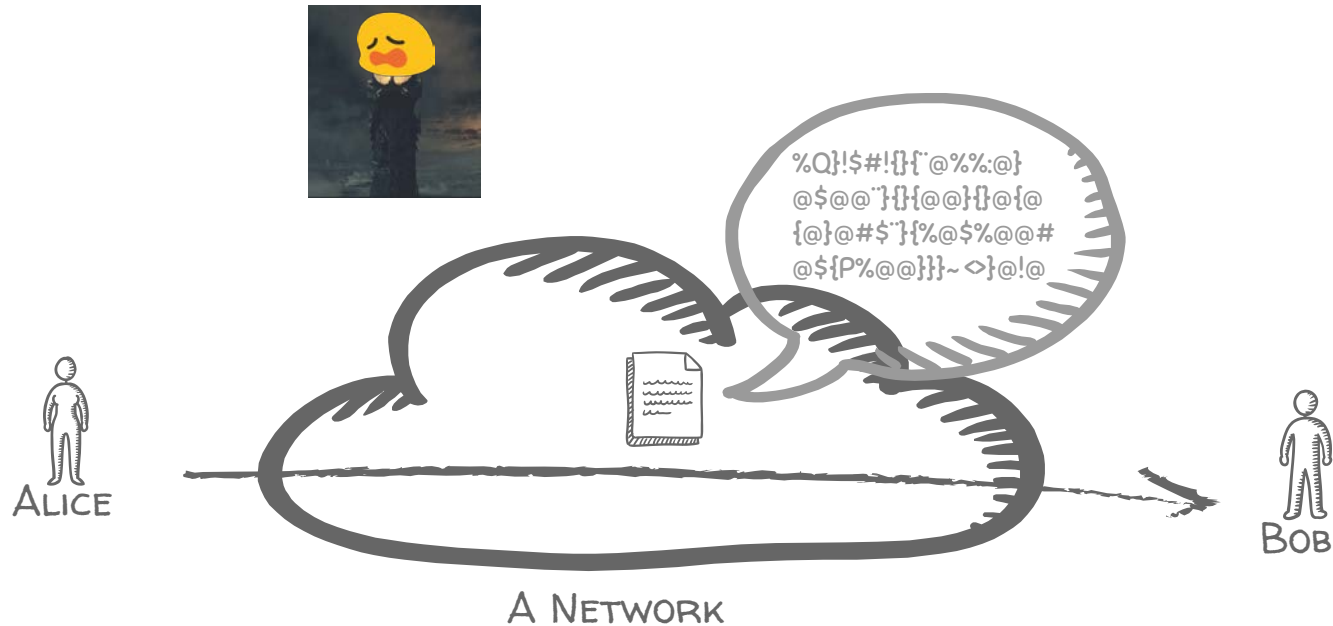
- Off-the-record (OTR)



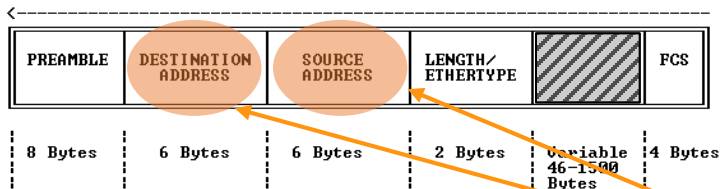
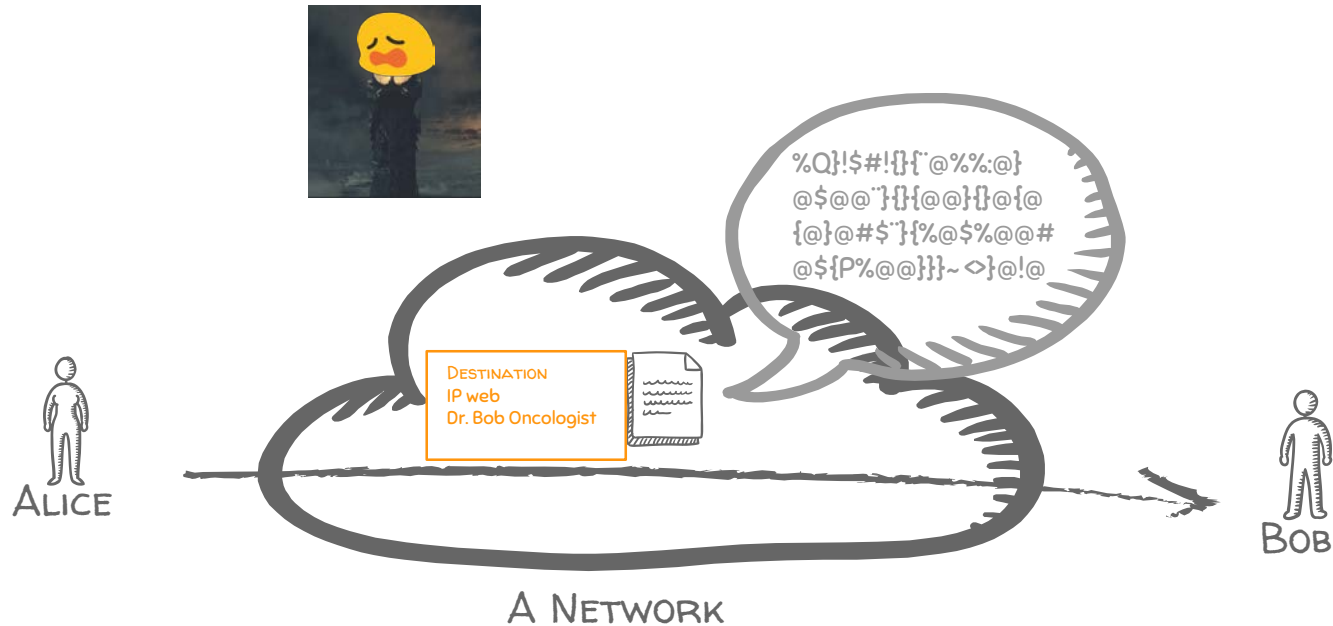
- Signal



BUT WE CAN ENCRYPT! WHAT IS THE PROBLEM?



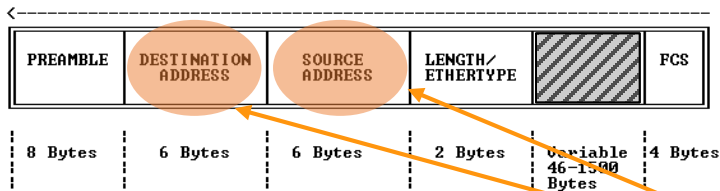
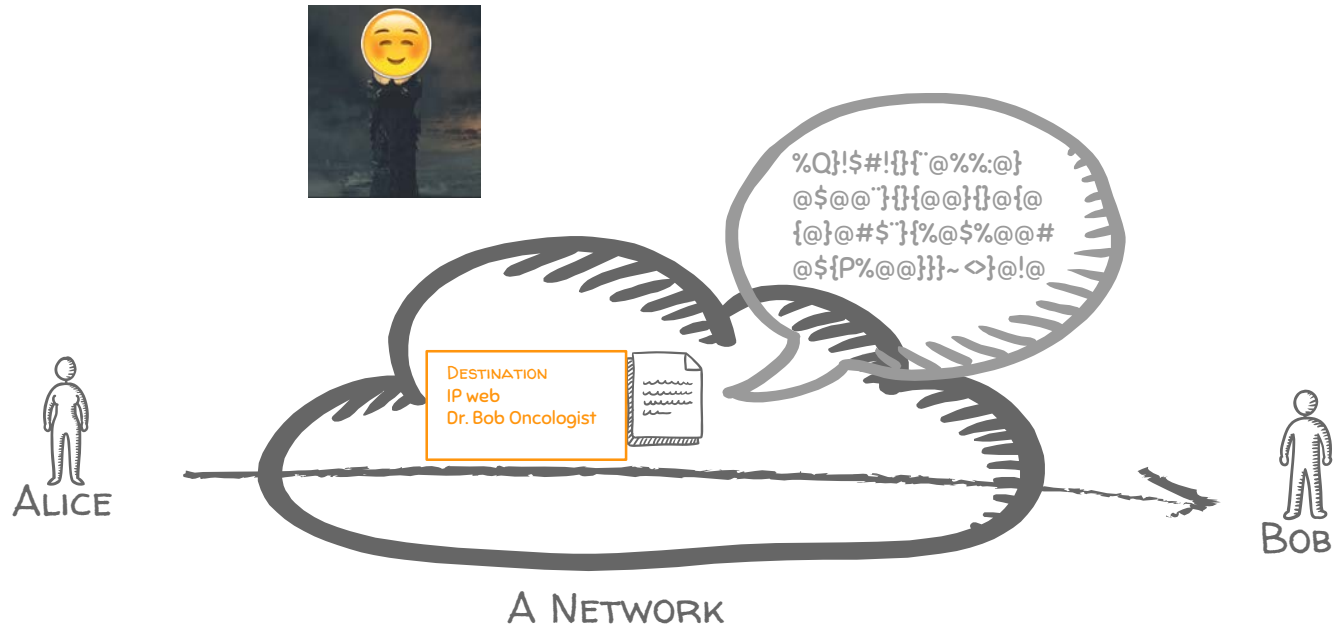
BUT WE CAN ENCRYPT! WHAT IS THE PROBLEM?



ETHERNET
(IEEE 802.3, 1997)

Same for IP, TCP, SMTP, IRC,
HTTP, ...

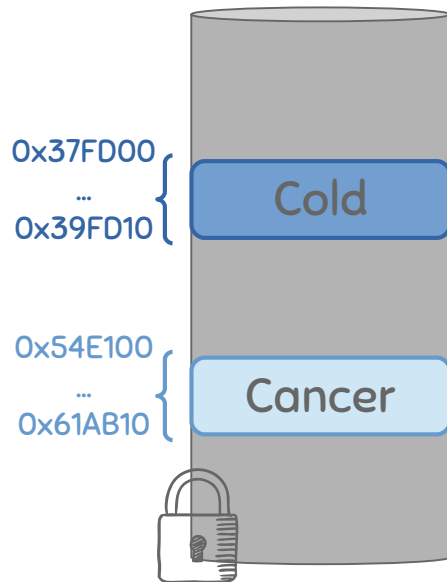
OMG!! META DATA IS ALSO SENSITIVE!!



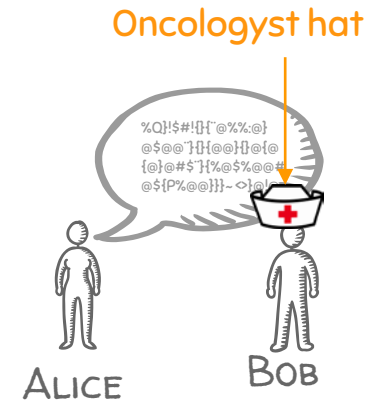
ETHERNET
(IEEE 802.3, 1997)

Same for IP, TCP, SMTP, IRC,
HTTP, ...

OMG!! META DATA IS ALSO SENSITIVE!!



ADDRESS
Dr. Bob Oncologist



TRAFFIC ANALYSIS: META DATA ANALYSIS

WIKIPEDIA: traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication

MAKING USE OF "JUST" TRAFFIC DATA OF A COMMUNICATION (AKA METADATA) TO EXTRACT INFORMATION (AS OPPOSED TO ANALYZING CONTENT OR PERFORM CRYPTANALYSIS)



Identities of
communicating parties



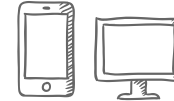
Timing, frequency,
duration



Location



Volume



Device

MILITARY ROOTS

- M. Herman: "These non-textual techniques can establish **TARGETS'** **LOCATIONS**, order-of-battle and **MOVEMENT**. Even when messages are not being deciphered, traffic analysis of the target's Command, Control, Communications and intelligence system and its patterns of behavior provides indications of his **INTENTIONS** and **STATES OF MIND**"
- **WWI**: British troops finding German boats.
- **WWII**: assessing size of German Air Force, fingerprinting of transmitters or operators (localization of troops).



NOWADAYS

- Diffie&Landau: "Traffic analysis, not cryptanalysis, is the backbone of communications intelligence"
- Stewart Baker (NSA): "metadata **ABSOLUTELY TELLS YOU EVERYTHING ABOUT SOMEBODY'S LIFE**. If you have enough metadata, you don't really need content."
- Tempora, MUSCULAR → XkeyScore, PRISM
- Also "good" uses: recommendations, location-based services,

Herman, Michael. Intelligence power in peace and war. Cambridge University Press, 1996.

Diffie, Whitfield, and Susan Landau. Privacy on the line: The politics of wiretapping and encryption. MIT press, 2010.

<http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>

PROTECTING THE COMMUNICATION LAYER

ANONYMOUS COMMUNICATIONS

➤ GENERAL APPLICATIONS

- Freedom of speech
- Profiling / price discrimination
- Spam avoidance
- Investigation / market research
- Censorship resistance

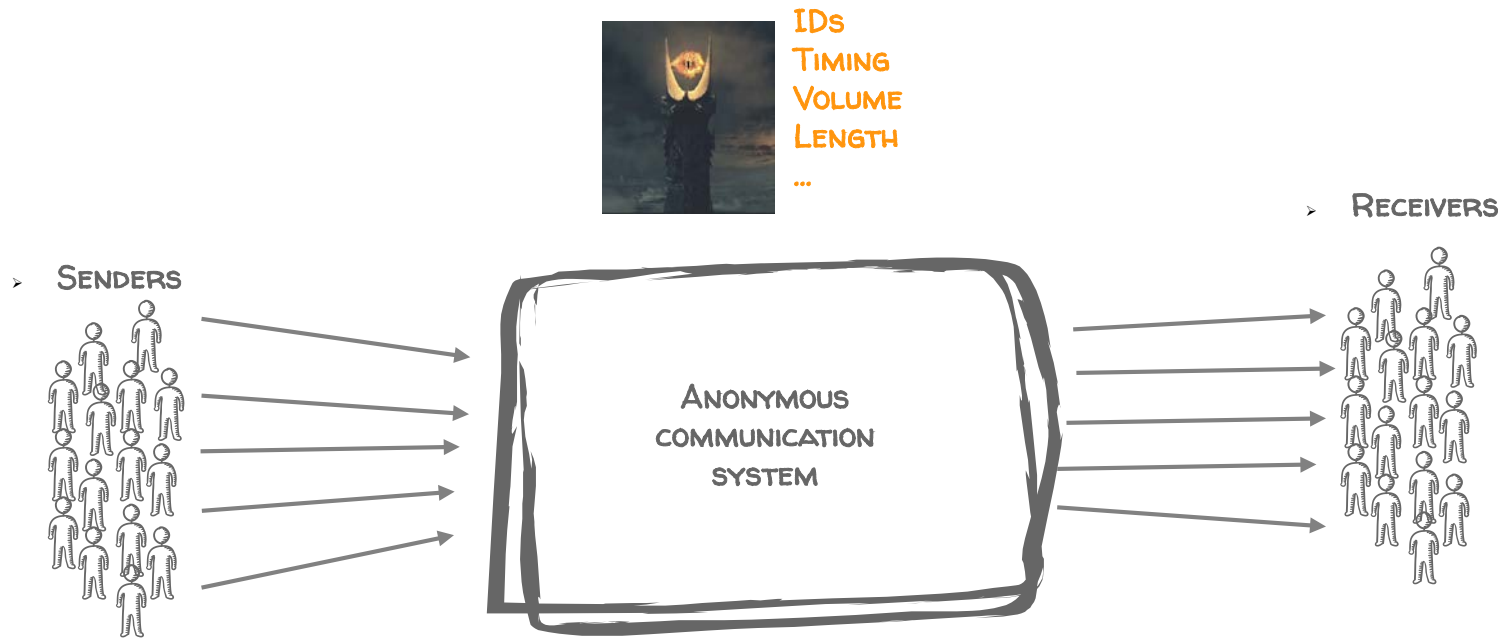
➤ SPECIALIZED APPLICATIONS

- Electronic voting
- Auctions / bidding / stock market
- Incident reporting
- Witness protection / whistle blowing
- Showing anonymous credentials!

Anonymity is important to:

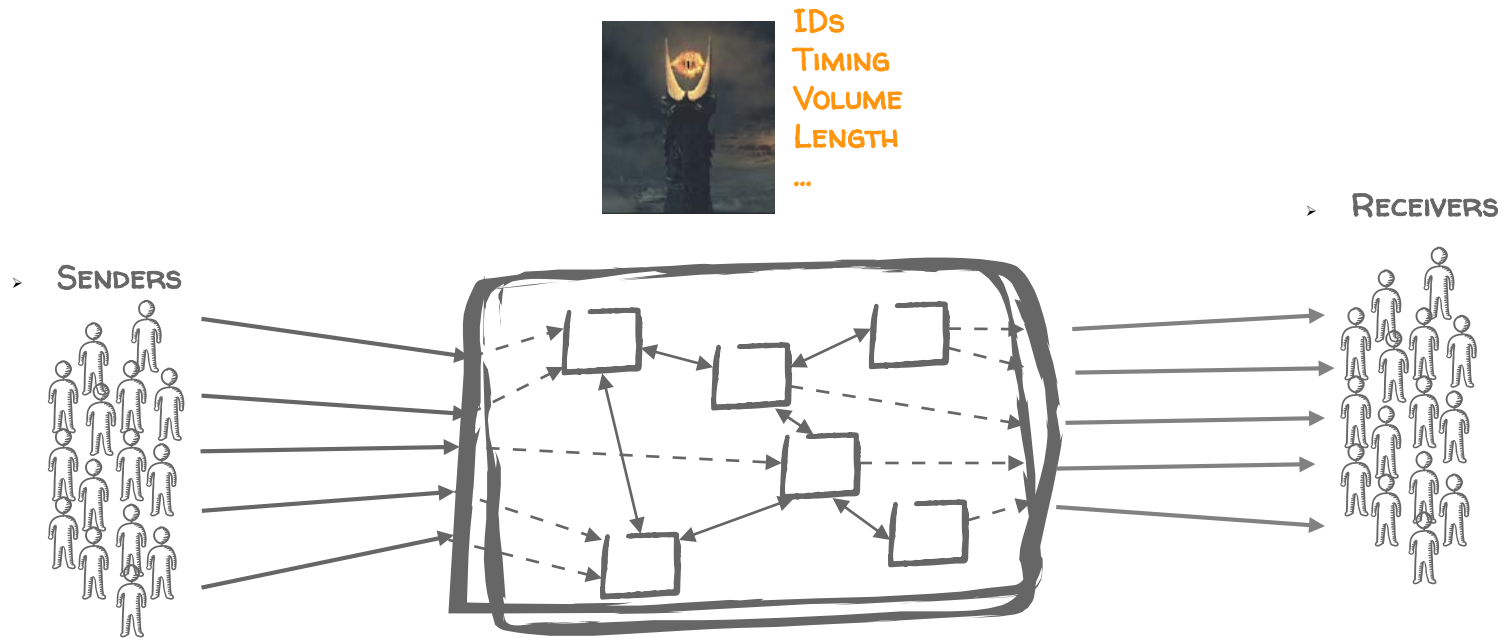
- the people who run some of the funniest parody Twitter accounts, such as [@FeministHulk](#) (SMASH THE PATRIARCHY!) or [@BPGlobalPr](#) during the Deepwater Horizon aftermath. San Francisco would not be better off if we knew who was behind [@KarltheFog](#), the most charming personification of a major city's climate phenomenon.
- the young LGBTQ youth seeking advice online about coming out to their parents.
- the marijuana grower who needs to ask questions on an online message board about lamps and fertilizer or complying with state law, without publicly admitting to committing a federal offense.
- the medical patient seeking advice from other patients in coping with a chronic disease, whether it's alopecia, irritable bowel syndrome, cancer or a sexually transmitted infection.
- the online dater, who wants to meet new people but only reveal her identities after she's determined that potential dates are not creeps.
- the business that wants no-pulled-punches feedback from its customers.
- the World of Warcraft player, or any other MMOG gamer, who only wants to engage with other players in character.
- artists. Anonymity is integral to the work of The Yes Men, Banksy and Keizer.
- the low-income neighborhood resident who wants to comment on an article about gang violence in her community, without incurring retribution in the form of spray paint and broken windows.
- the boyfriend who doesn't want his girlfriend to know he's posing questions on a forum about how to pick out a wedding ring and propose. On the other end: Anonymity is important to anyone seeking advice about divorce attorneys online.
- the youth from an orthodox religion who secretly posts reviews on hip hop albums or R-rated movies.
- the young, pregnant woman who is seeking out advice on reproductive health services.
- the person seeking mental health support from an online community. There's a reason that support groups so often end their names with "Anonymous."
- the job seeker, in pursuit of cover letter and resume advice in a business blogger's comments, who doesn't want his current employer to know he is looking for work.
- many people's sexual lives, whether they're discussing online erotica or arranging kink meet-ups.
- Political Gabfest listeners. Each week, the hosts encourage listeners to post comments. Of the 262 largely positive customer reviews on iTunes, only a handful see value in using their real names.

THE SOLUTION: ANONYMOUS COMMUNICATIONS



- BITWISE UNLINKABILITY
 - Crypto to make inputs and outputs bit patterns different
- (RE)PACKETIZING + (RE)SCHEDULE
 - Destroy patterns (traffic analysis resistance)

THE SOLUTION: ANONYMOUS COMMUNICATIONS



- BITWISE UNLINKABILITY
 - Crypto to make inputs and outputs bit patterns different
- (RE)PACKETIZING + (RE)SCHEDULE + (RE)ROUTING,
 - Destroy patterns (traffic analysis resistance)
 - Load balancing
 - Distribute trust

End user
devices

Distribute semi
trusted parties

Enable choice
of whom
to trust

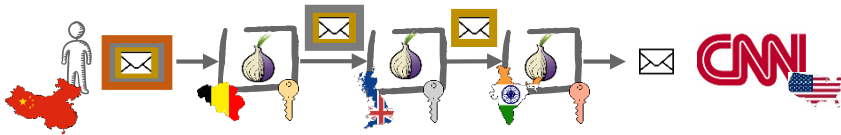
Cryptography
Correctness
Confidentiality

Keep only
short secrets

ANONYMOUS COMMUNICATIONS OUT THERE

LOW LATENCY 

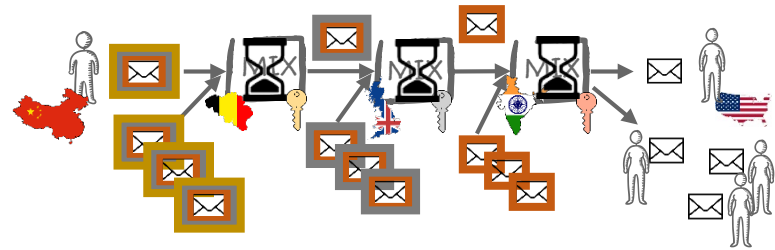
  



Web browsing, Instant Messaging, streaming

HIGH LATENCY 

MIXMASTER / MIXMINION

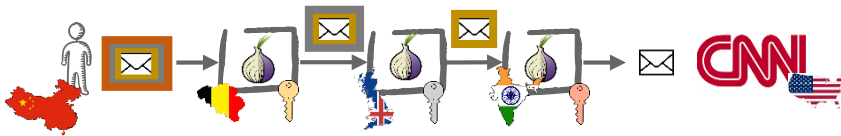


Email, Voting


ANONYMOUS COMMUNICATIONS OUT THERE

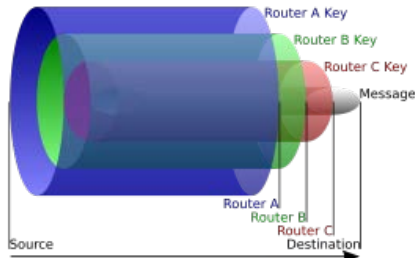
LOW LATENCY 



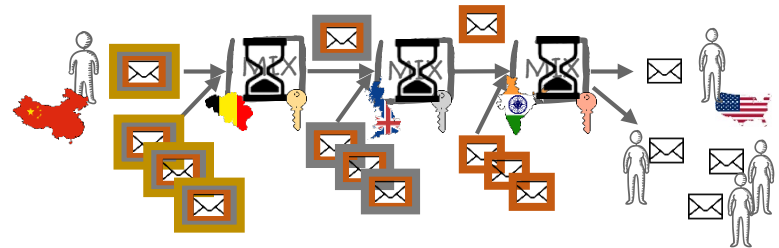
Web browsing, Instant Messaging, streaming

STREAM-based:  fixed



HIGH LATENCY 

MIXMASTER / MIXMINION



Email, Voting

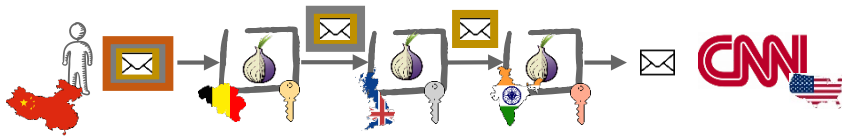
ANONYMOUS COMMUNICATIONS OUT THERE

LOW LATENCY 




Tor
TorProject.org

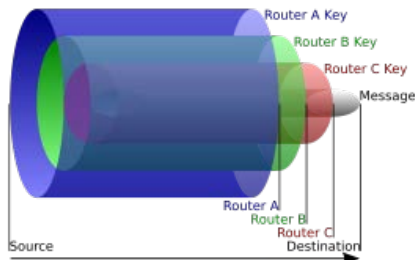
I2P

JONONYM



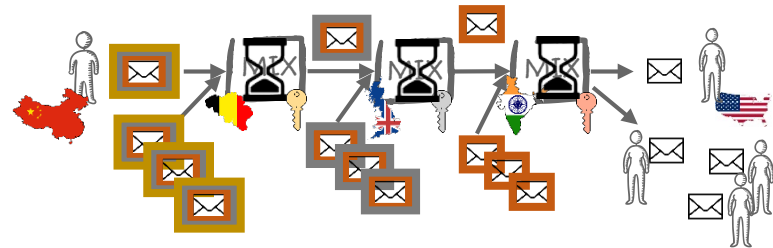
Web browsing, Instant Messaging, streaming

STREAM-based:    fixed



HIGH LATENCY 

MIXMASTER / MIXMINION



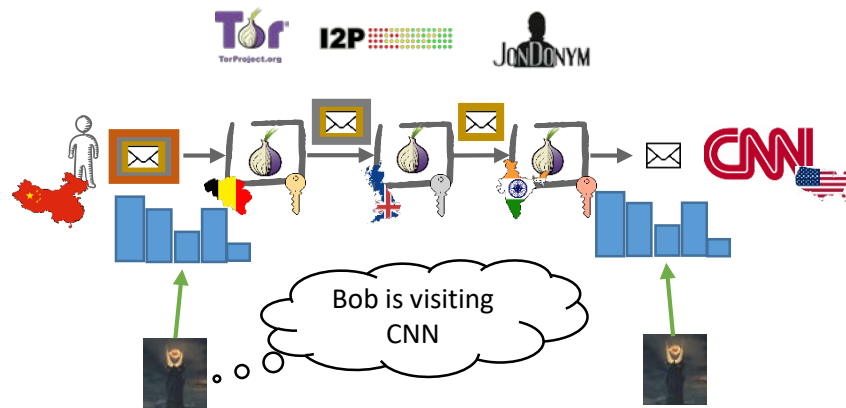
Email, Voting

MSG-based:    change

One message = one route
(slower)

ANONYMOUS COMMUNICATIONS OUT THERE

LOW LATENCY

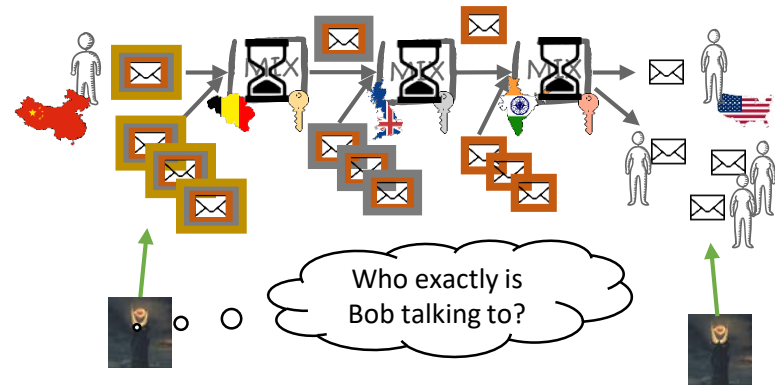


Cannot resist Global Adversary
(assumes adversary cannot see
both edges)

Web browsing, Instant Messaging, streaming

HIGH LATENCY

MIXMASTER / MIXMINION

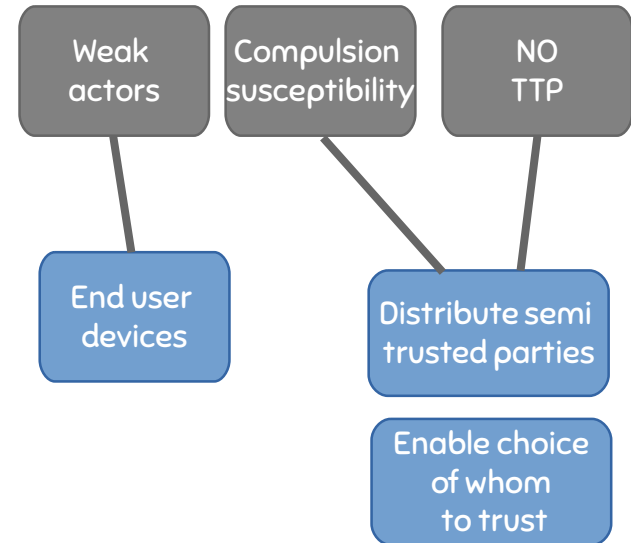
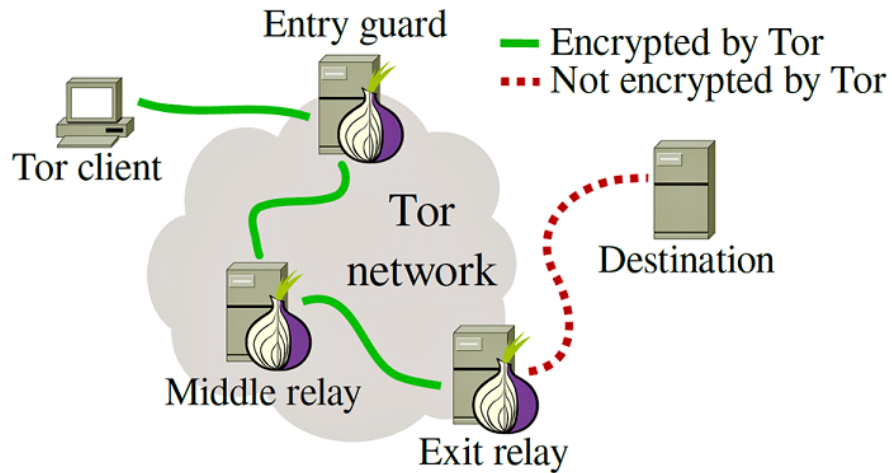


Global Adversary resistance **at**
the cost of latency
(and long term patterns
revealed)

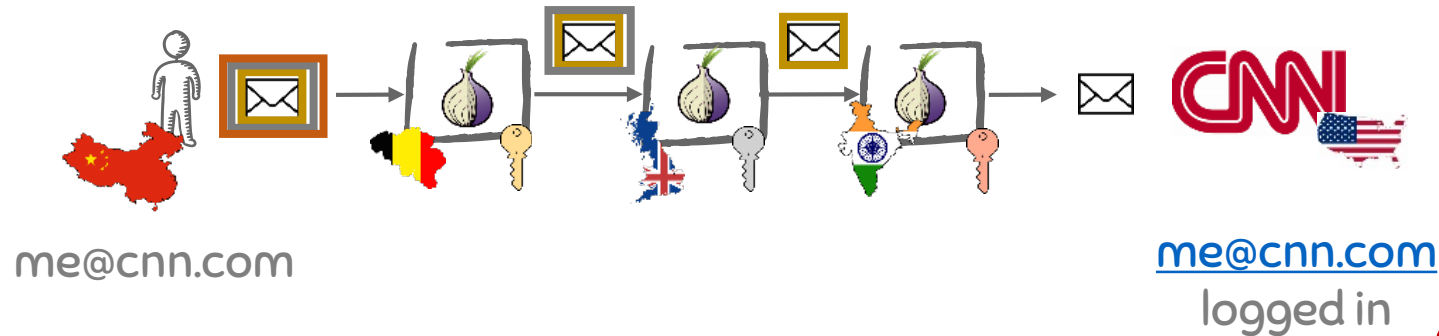
Email, Voting

MORE (ACADEMIC BUT GETTING THERE): DC-Nets, Loopix

ANONYMOUS COMMUNICATIONS VS. VPN



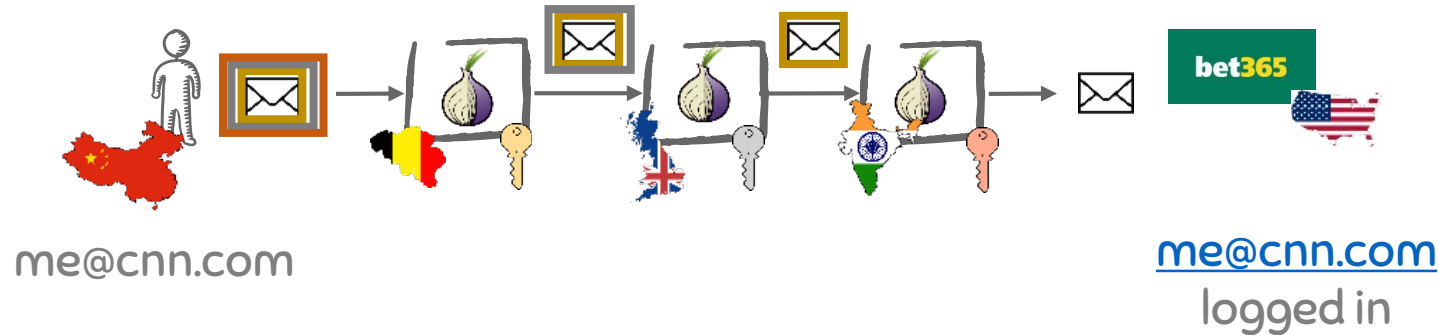
ANONYMOUS COMMUNICATIONS AT NETWORK LAYER WHAT ABOUT THE APPLICATION LAYER?



DEANONYMIZATION!!!

ANONYMOUS COMMUNICATIONS AT NETWORK LAYER

WHAT ABOUT THE APPLICATION LAYER?



Signature

DEANONYMIZATION
+ EXTRA INFORMATION

Name
ID#
Address
DoB
...

COMPROBACIÓN DEL CERTIFICADO DE AUTENTICACIÓN DE SU DNI ELECTRÓNICO

Estimado Sr/Sra. #####

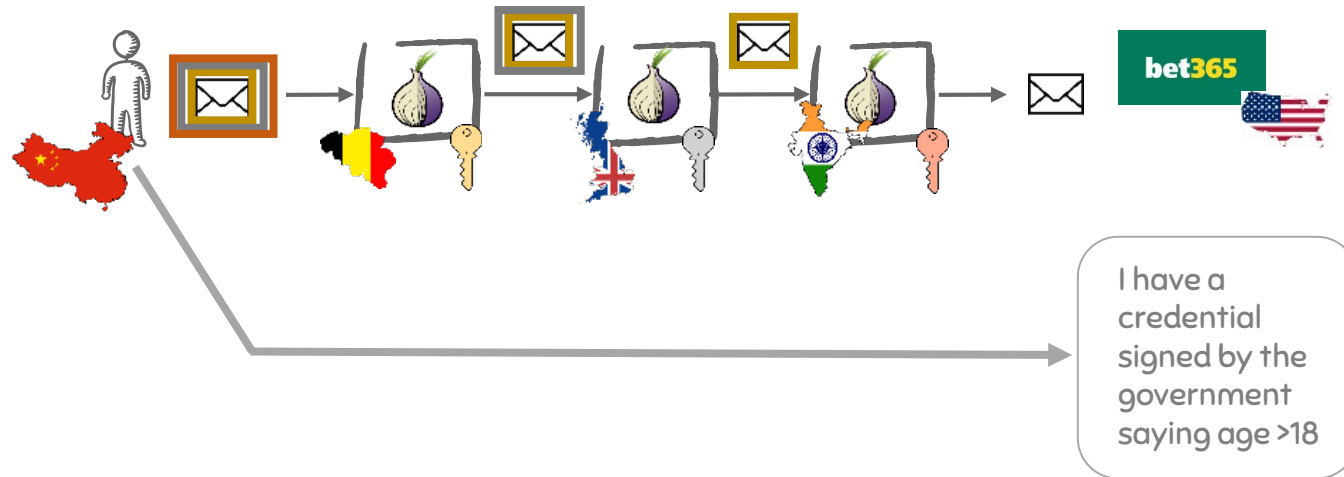
Su DNIe acaba de ser verificado. Esta usted en disposición de un Certificado de Autenticación Activo.



Identificador	Valor
INFORMACIÓN SOBRE LA IDENTIDAD	(Valores Personales)
Nombre	##### (AUTENTICACIÓN)
Apellidos	#####
NIF	#####
Número de Serie del Certificado de Autenticación	#####
Autoridad Emisora	AC DNIE 002
Propietario	#####
Comienzo de la Validez del Certificado	#####
Fin de la Validez del Certificado	25 de septiembre de 2010
Estado del Certificado de Autenticación	Activo

ANONYMOUS COMMUNICATIONS AT NETWORK LAYER

WHAT ABOUT THE APPLICATION LAYER?

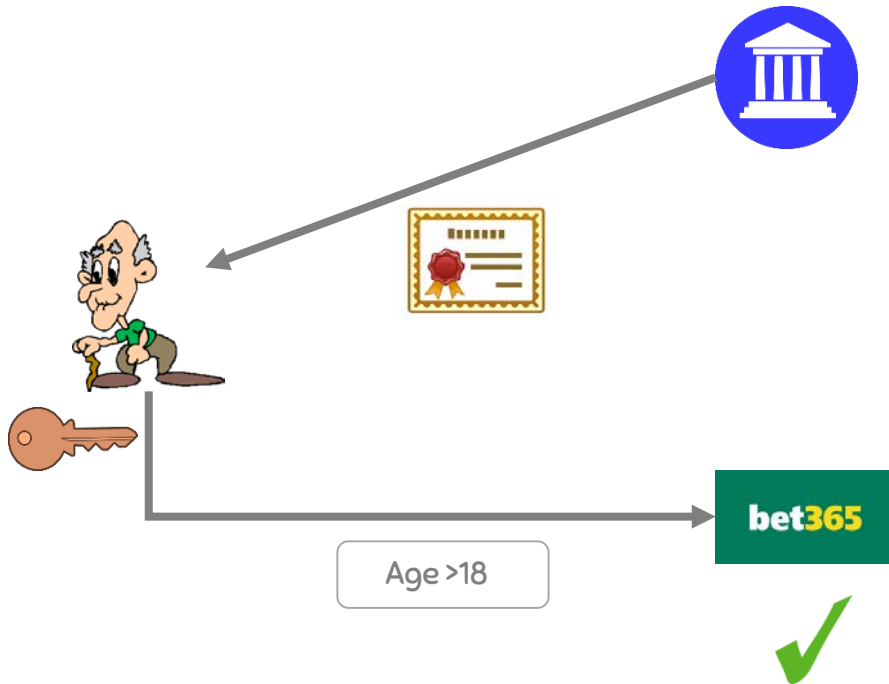


CANNOT

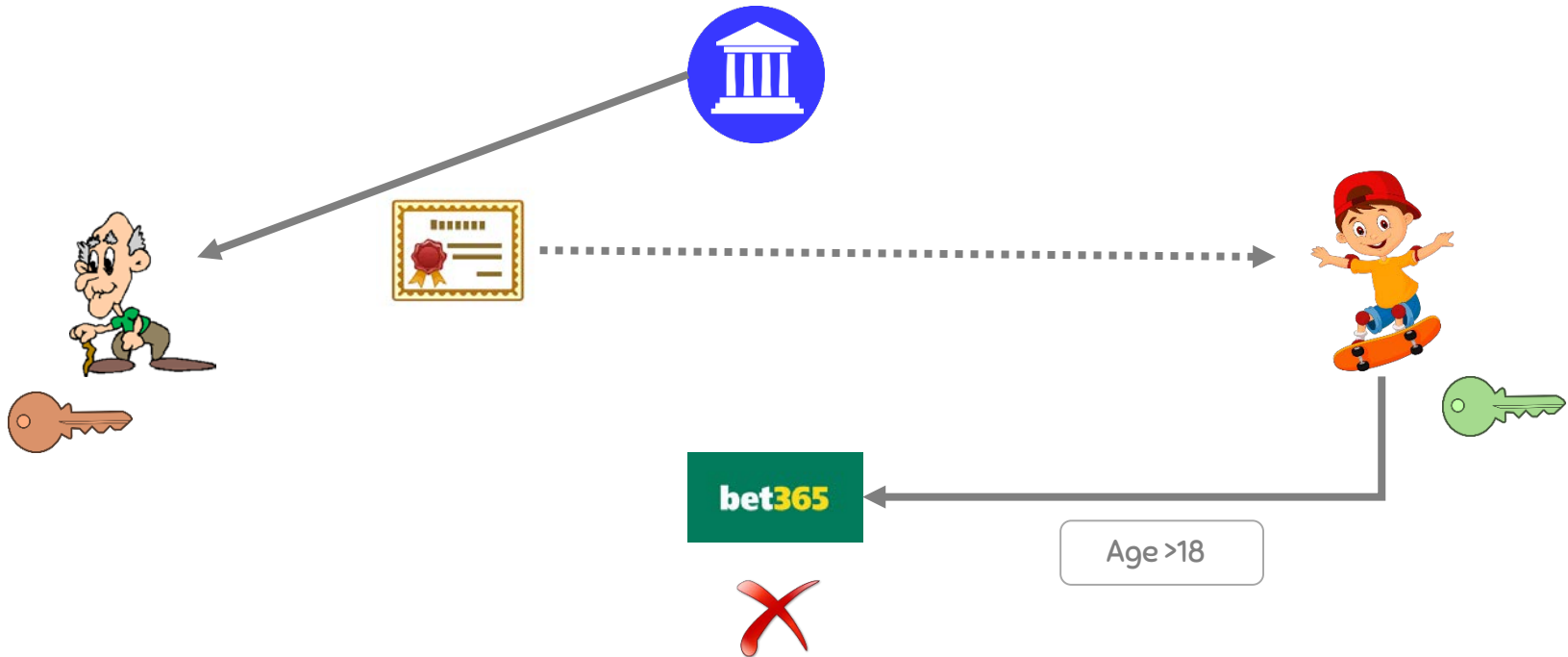
- Identify Alice (if her name is not provided)
- Learn anything beyond the info she gives (and what can be inferred)
- Distinguish two users with the same attributes
- Link multiple uses of the same credentials

ANONYMOUS CREDENTIALS / ATTRIBUTE-BASED CREDENTIALS

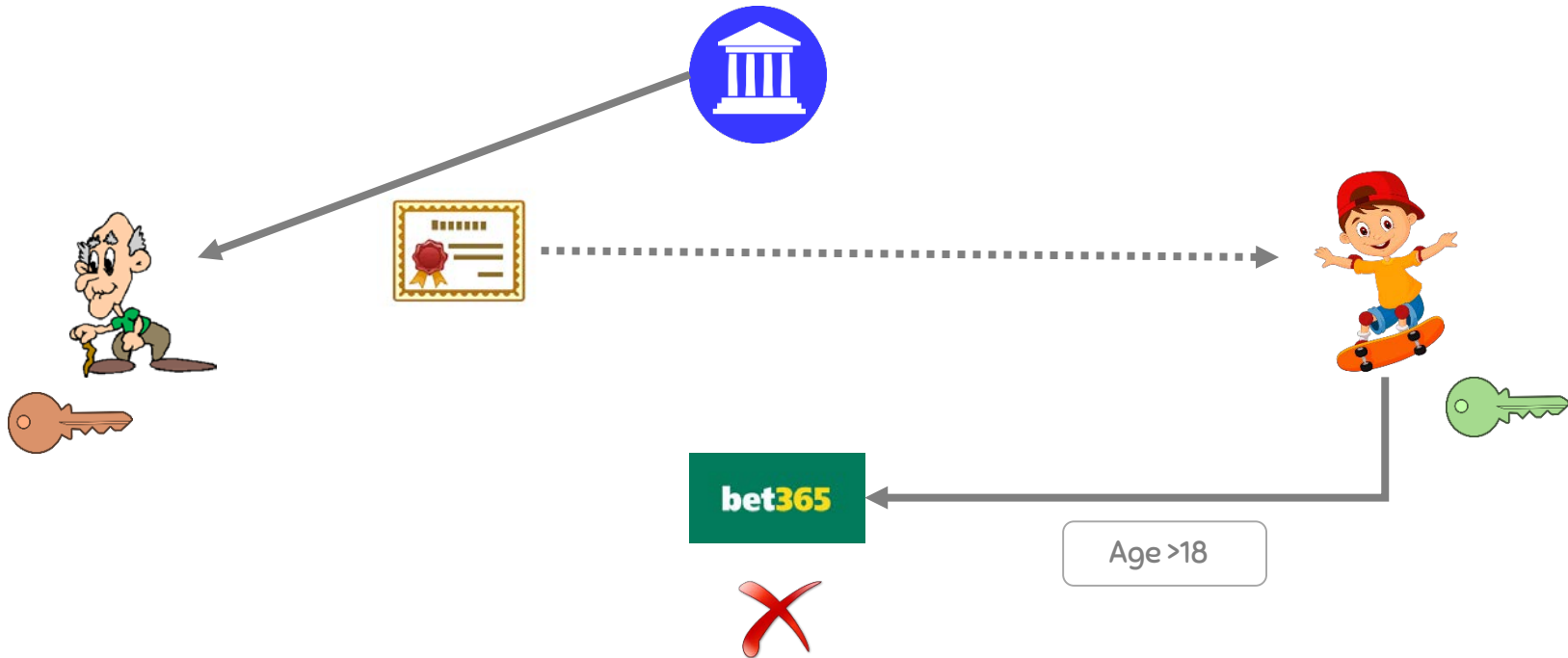
ATTRIBUTE BASED CREDENTIALS



ATTRIBUTE BASED CREDENTIALS



ATTRIBUTE BASED CREDENTIALS



COMPLETENESS: if the statement is true, the verifier will be convinced

ZERO-KNOWLEDGE: if the statement is true no cheating verifier learns anything other than this fact

SOUNDNESS: no cheating prover can convince the honest verifier

UNLINKABILITY: two requests cannot be linked to the same user

HOLDS EVEN IF VERIFIER AND PROVER COLLIDE

PKI VS. ATTRIBUTE BASED CREDENTIALS

Signed by a trusted issuer
Certification of attributes
Authentication (secret key)
Double-signing detection

No data minimization
Users are identifiable
Users can be tracked
(Signature linkable to other contexts
where PK is used)

Signed by a trusted issuer
Certification of attributes
Authentication (secret key)
Double-signing detection

Data minimization
Users are anonymous
Users are unlinkable across contexts

ZERO KNOWLEDGE PROOFS

“A zero knowledge proof is a protocol between two parties, a prover and a verifier, where the prover, who makes some claim, can convince the verifier that their claim is valid, whilst revealing nothing more than the validity of their claim.”



The finding Waldo example

ZERO KNOWLEDGE PROOFS

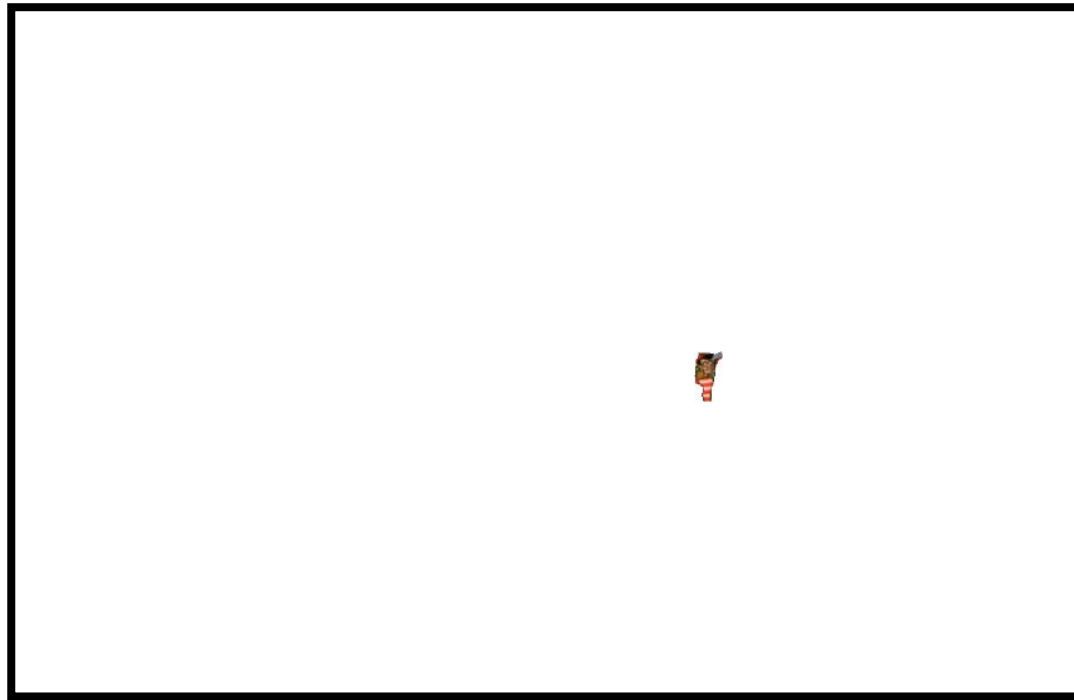
“A zero knowledge proof is a protocol between two parties, a prover and a verifier, where the prover, who makes some claim, can convince the verifier that their claim is valid, whilst revealing nothing more than the validity of their claim.”



The finding Waldo example

ZERO KNOWLEDGE PROOFS

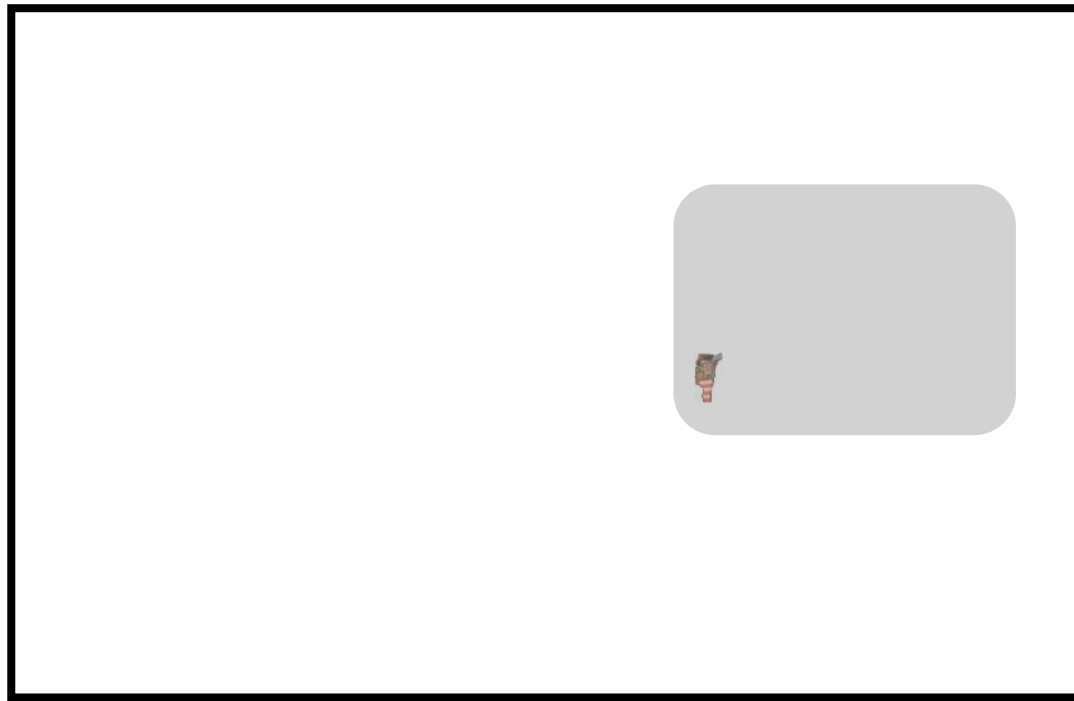
“A zero knowledge proof is a protocol between two parties, a prover and a verifier, where the prover, who makes some claim, can convince the verifier that their claim is valid, whilst revealing nothing more than the validity of their claim.”



The finding Waldo example

ZERO KNOWLEDGE PROOFS

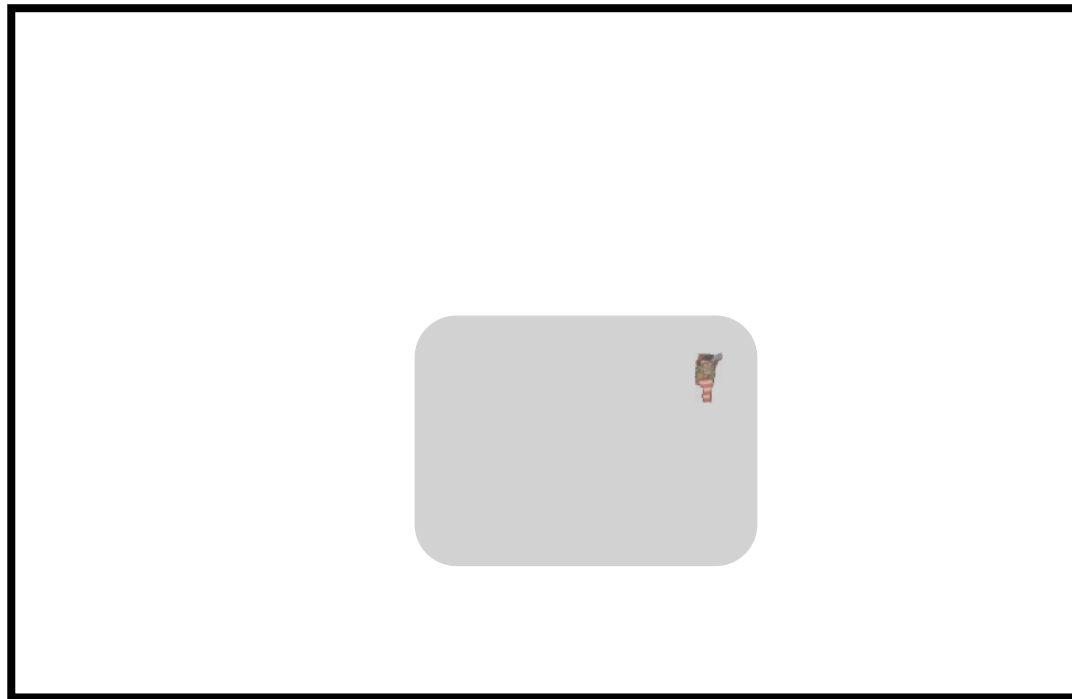
“A zero knowledge proof is a protocol between two parties, a prover and a verifier, where the prover, who makes some claim, can convince the verifier that their claim is valid, whilst revealing nothing more than the validity of their claim.”



The finding Waldo example

ZERO KNOWLEDGE PROOFS

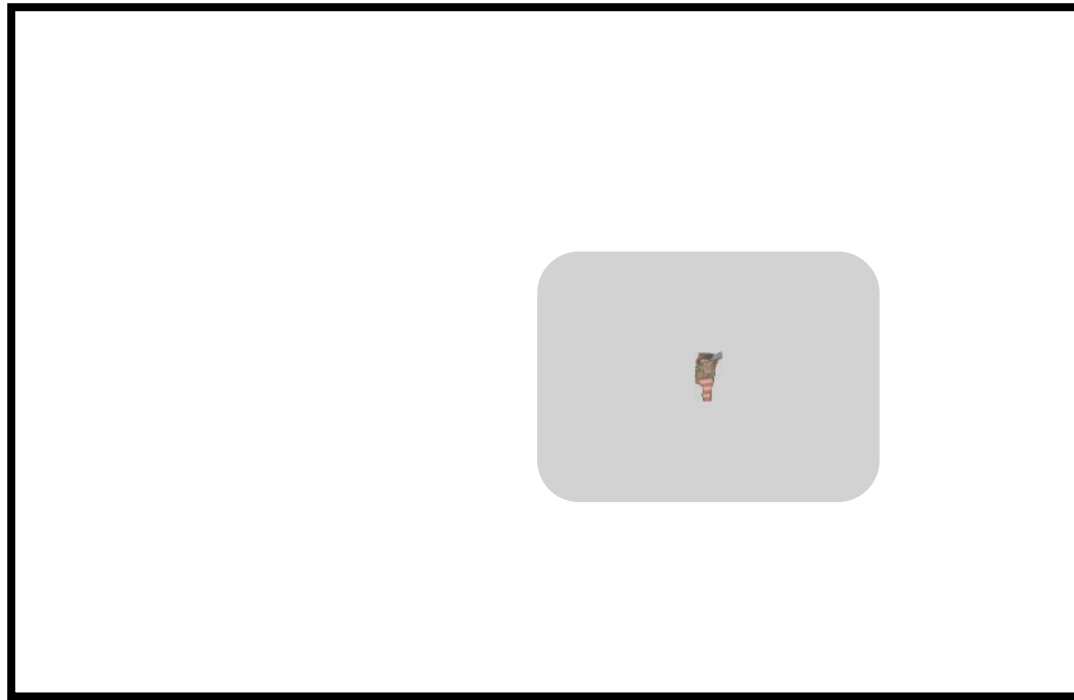
“A zero knowledge proof is a protocol between two parties, a prover and a verifier, where the prover, who makes some claim, can convince the verifier that their claim is valid, whilst revealing nothing more than the validity of their claim.”



The finding Waldo example

ZERO KNOWLEDGE PROOFS

“A zero knowledge proof is a protocol between two parties, a prover and a verifier, where the prover, who makes some claim, can convince the verifier that their claim is valid, whilst revealing nothing more than the validity of their claim.”



The finding Waldo example

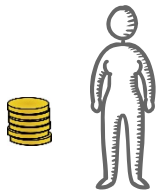
CRYPTOGRAPHIC COMMITMENTS

“a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later”



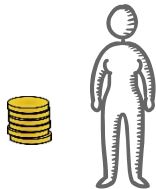
CRYPTOGRAPHIC COMMITMENTS

“a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later”



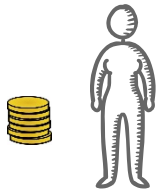
CRYPTOGRAPHIC COMMITMENTS

“a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later”



CRYPTOGRAPHIC COMMITMENTS

“a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later”



CRYPTOGRAPHIC COMMITMENTS

“a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later”



CRYPTOGRAPHIC COMMITMENTS

“a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later”



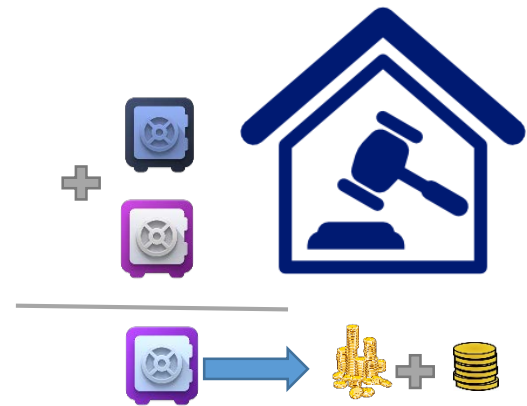
HIDING – given a commitment, no information about the value can be gained

BINDING – once committed, the content cannot be changed



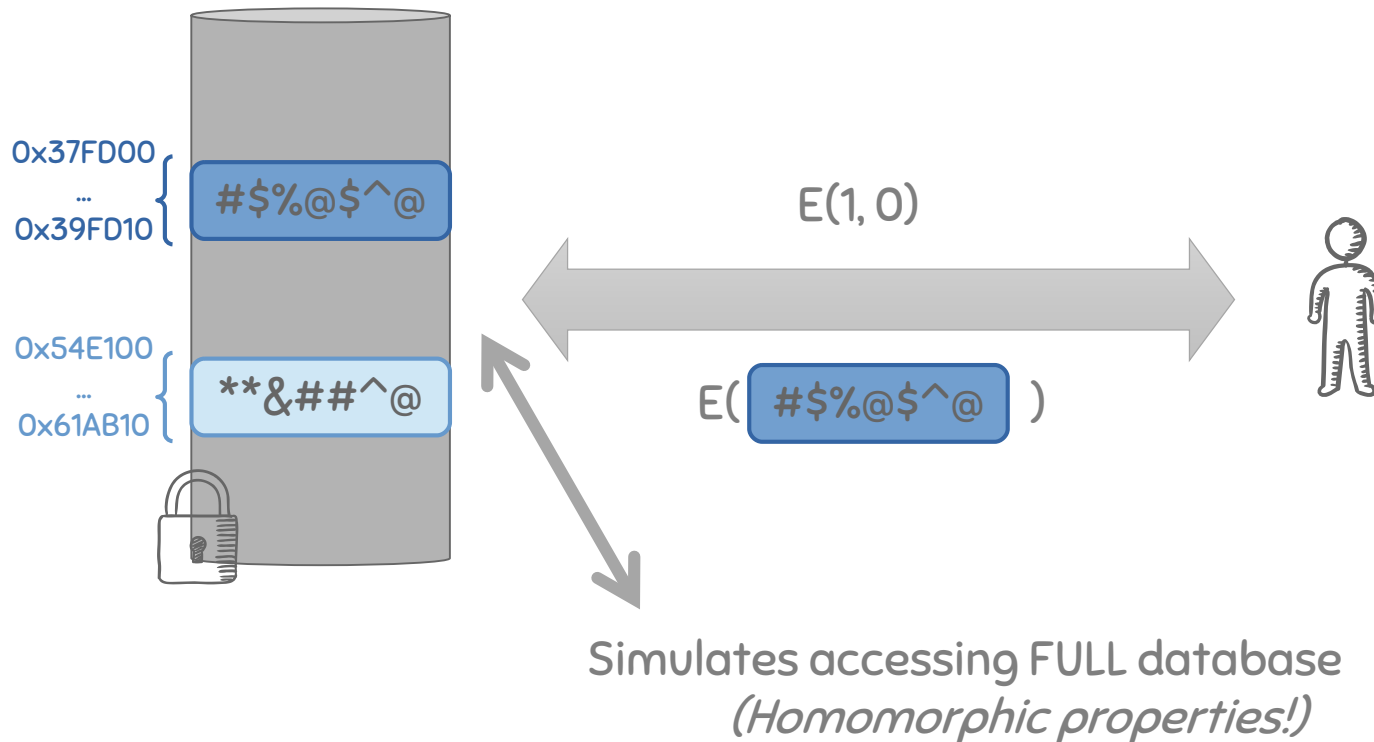
HOMOMORPHIC CRYPTOGRAPHIC COMMITMENTS

“a cryptographic primitive that allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later”



PRIVATE INFORMATION RETRIEVAL

"is a protocol that allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved."



MANY MORE...

PRIVATE SET INTERSECTION

a client and a server jointly compute the intersection of their private input sets in a manner that at the end the client learns the intersection and the server learns nothing (one-way PSI) or both learn the intersection (mutual PSI) -- private search

BLIND SIGNATURES

a server signs a message produced by a client without learning the content of the message -- eCash

MULTIPARTY COMPUTATION

parties to jointly compute a function over their inputs while keeping those inputs private -- compute total computations (statistics)

WE DEFINED PRIVACY GOALS

WE DEFINED TECHNICAL PROPERTIES EMBODIED IN PETS

WE KNOW SOME PETS

HOW DO WE BUILD PRIVACY-PRESERVING SYSTEMS?



ENGINEERING PRIVACY BY DESIGN 1.0

Two case studies:

- anonymous e-petitions: no identity attached to petitions
- privacy-preserving road tolling: no fine grained data sent to server

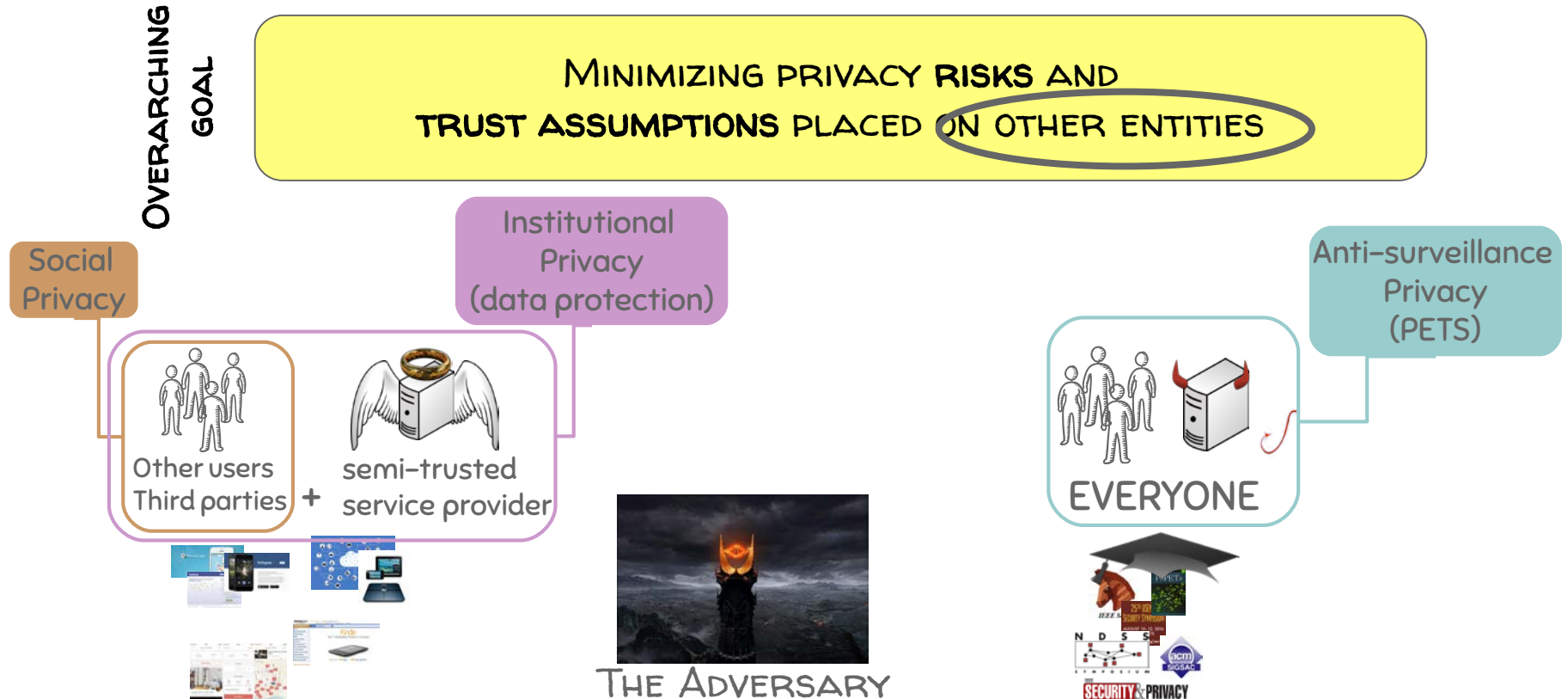
THE KEY IS “*DATA MINIMIZATION*”

BUT, it's not “data” that is minimized (in the system as a *whole*)

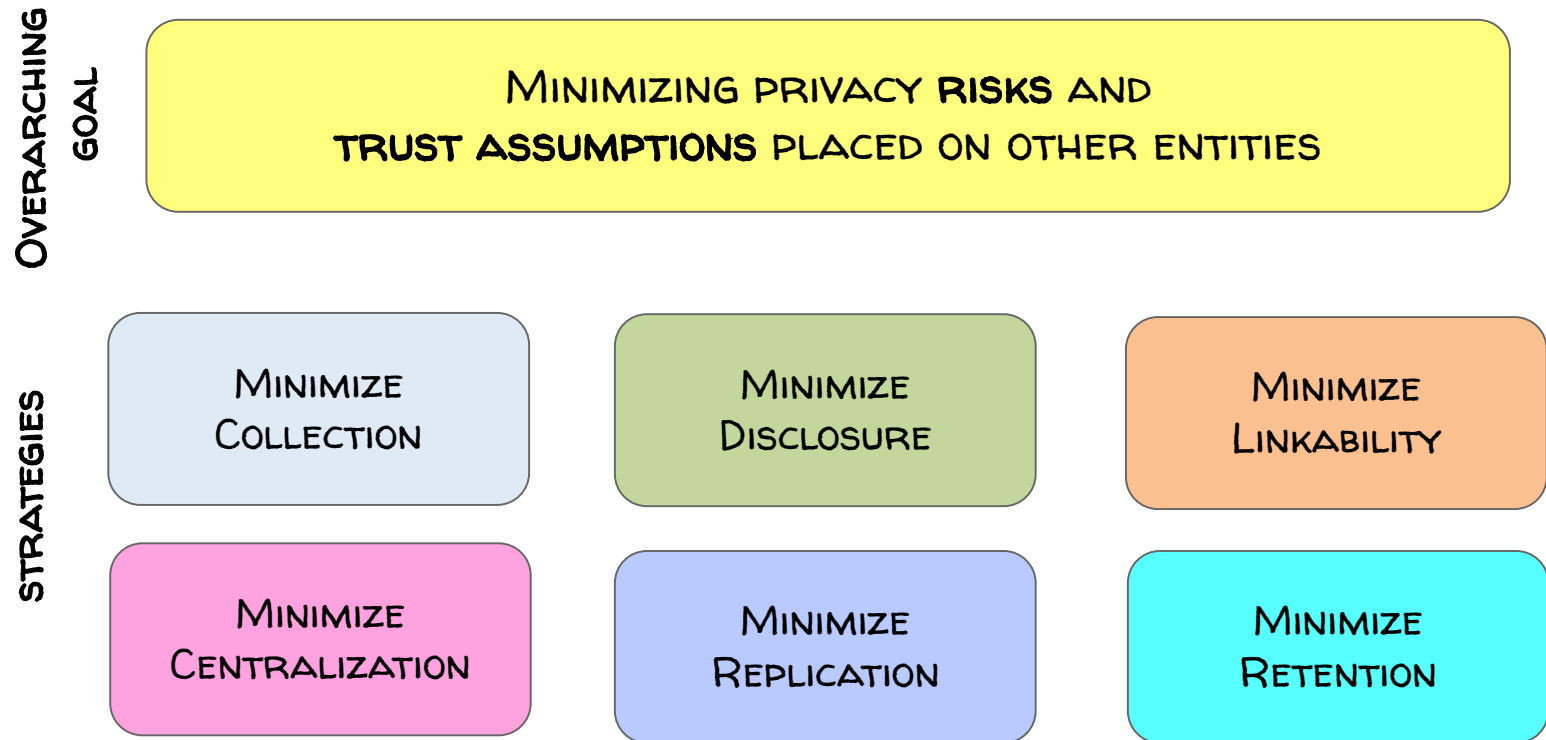
- kept in user devices
- sent encrypted to a server (only client has the key)
- distributed over multiple servers: only the user, or colluding servers, can recover the data

“*DATA MINIMIZATION*” IS A **BAD** METAPHORE

UNPACKING "DATA MINIMIZATION": PRIVACY BY DESIGN STRATEGIES



UNPACKING “DATA MINIMIZATION”: PRIVACY BY DESIGN STRATEGIES



GREAT! BUT... HOW DO WE USE THESE STRATEGIES?

We make explicit the activities and reasoning in **PRIVACY ENGINEERING DESIGN** process

CNIL-INRIA PRIZE ON PRIVACY PROTECTION 2017

CASE STUDY: ELECTRONIC TOLL PRICING

MOTIVATION: EUROPEAN ELECTRONIC TOLL SERVICE (EETS)

Toll collection on European Roads through On Board Equipment

Two approaches: Satellite Technology / DSRC

STARTING ASSUMPTIONS

1) Well defined functionality

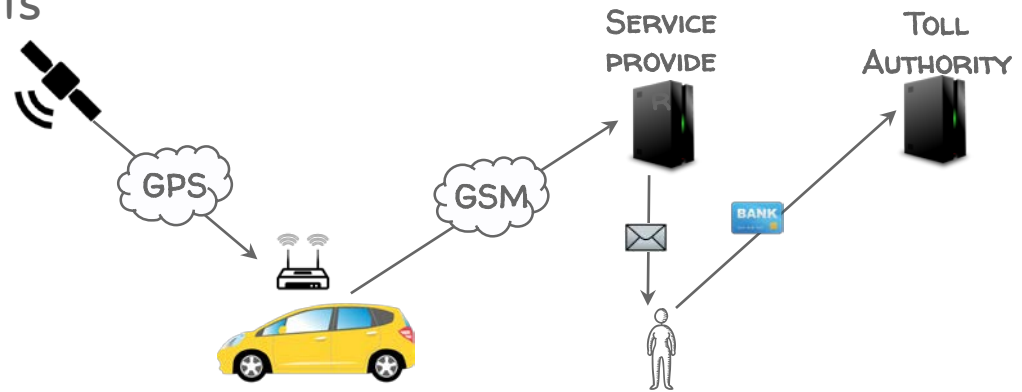
Charge depending on driving

2) Security, privacy & service integrity requirements

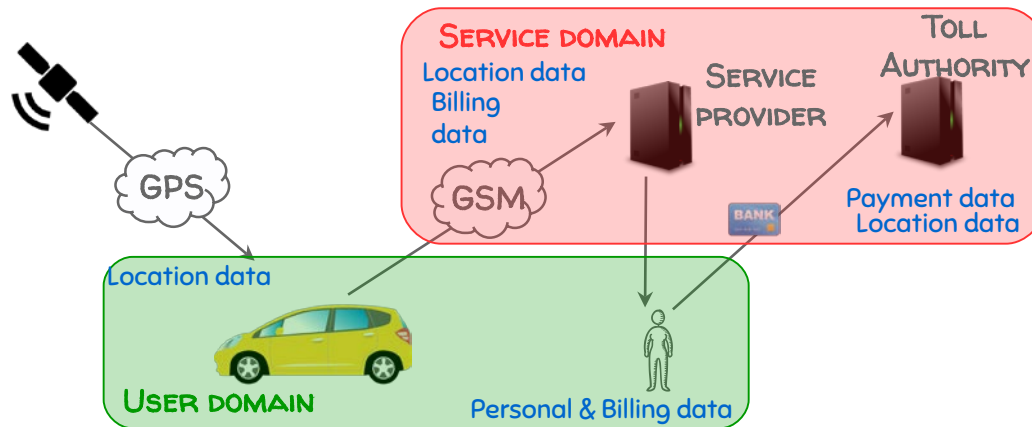
Users location should be private

No cheating clients

3) Initial reference system



CASE STUDY: ELECTRONIC TOLL PRICING



ACTIVITY 1: CLASSIFY ENTITIES IN DOMAINS

USER DOMAIN: components under the control of the user, eg, user devices

SERVICE DOMAIN: components outside the control of the user, eg, backend system at provider

ACTIVITY 2: IDENTIFY NECESSARY DATA FOR PROVIDING THE SERVICE

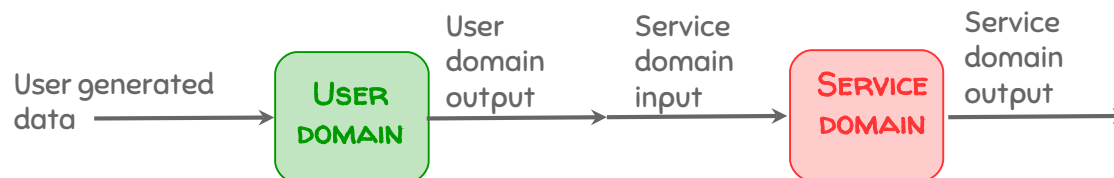
Location data – compute bill

Billing data – charge user

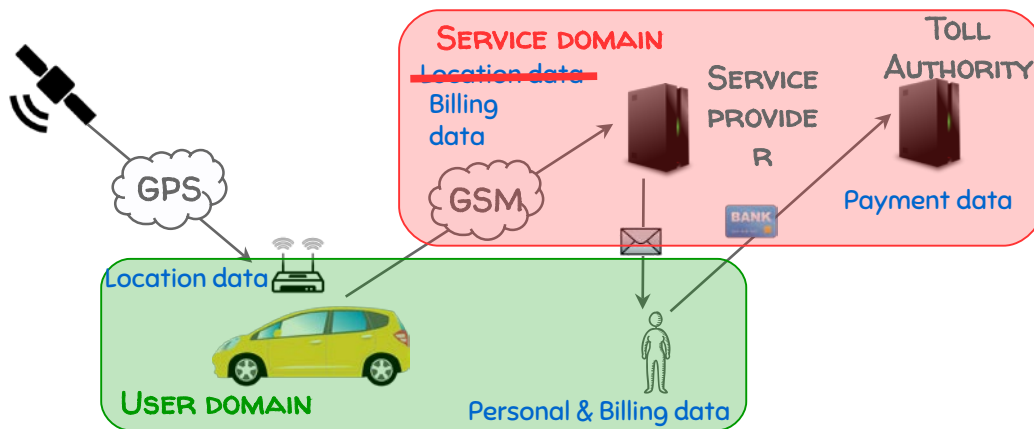
Personal data – send bill

Payment data – perform payment

ACTIVITY 3: DISTRIBUTE DATA IN ARCHITECTURE



CASE STUDY: ELECTRONIC TOLL PRICING



Location is not needed,
only the amount to bill!

Service integrity?

ACTIVITY 4: SELECT TECHNOLOGICAL SOLUTIONS FOLLOWING →

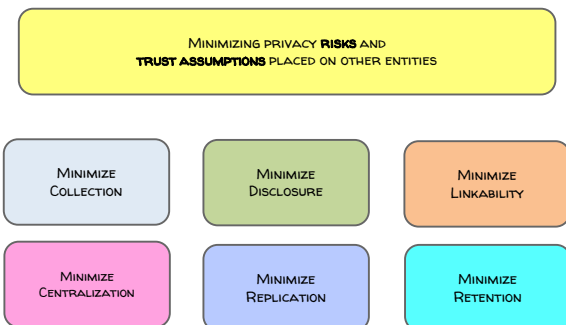
not sending the data (local computations)

encrypting the data

advanced privacy-preserving protocols

obfuscate the data

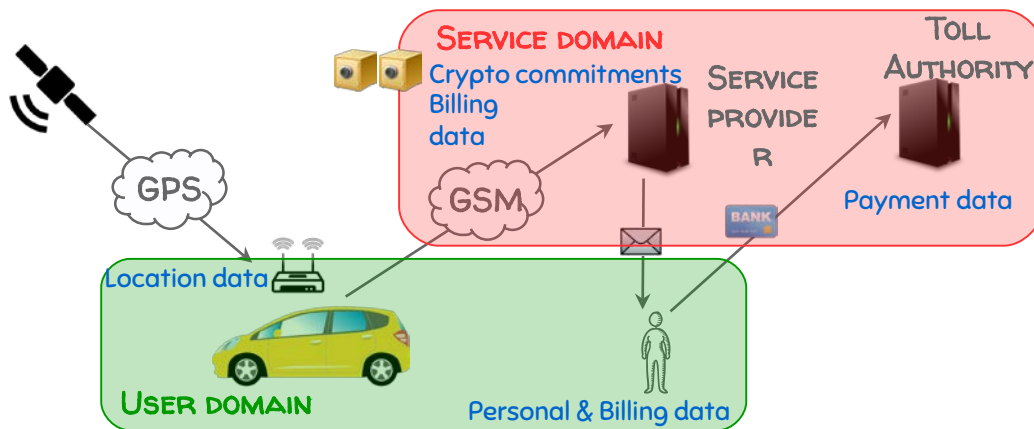
anonymize the data



J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, C. Geuens. PrETP "Privacy-Preserving Electronic Toll Pricing" USENIX Security Symposium 2010

C. Troncoso, G. Danezis, E. Kosta, J. Balasch, B. Preneel. "PriPAYD. Privacy-Friendly Pay-As-You-Drive Insurance" IEEE TDSC 2011

CASE STUDY: ELECTRONIC TOLL PRICING



Location is not needed,
only the amount to bill!

Service integrity?

ACTIVITY 4: SELECT TECHNOLOGICAL SOLUTIONS FOLLOWING →

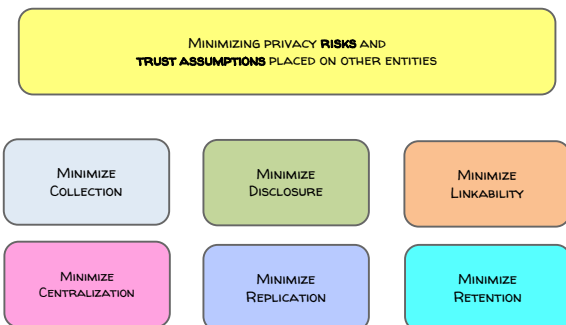
not sending the data (local computations)

encrypting the data

advanced privacy-preserving protocols

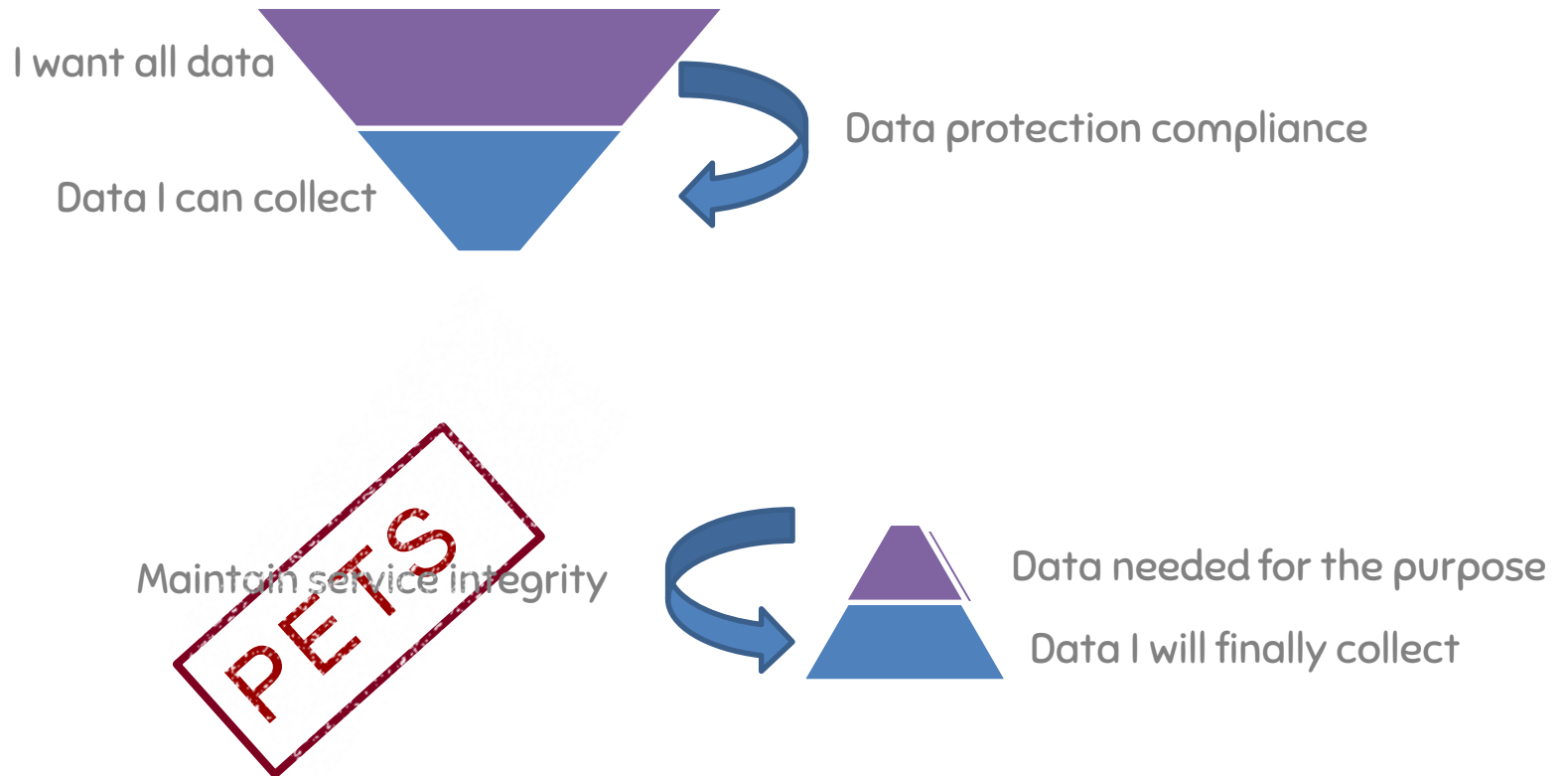
obfuscate the data

anonymize the data



A CHANGE IN OUR WAY OF THINKING....

THE USUAL APPROACH



TAKEAWAYS

WHO IS THE ADVERSARY MATTERS FOR DESIGNING

EMBED PRIVACY IN DESIGNS

REQUIRES “DIFFERENT” THINKING

6 STRATEGIES TO HELP DESIGN PROCESS

ULTIMATE GOAL REDUCE TRUST / RISK

GOAL OF THIS LECTURE

Understanding **DIFFERENT CONCEPTIONS OF PRIVACY**
(beyond Data Protection legislation)

Understanding how appropriate **TECHNOLOGIES CAN SUPPORT PRIVACY**
(beyond trust)

Understanding how we **EVALUATE PRIVACY-PRESERVING SYSTEMS**
(beyond risk)

Understanding the **NEED TO PROTECT METADATA**
(beyond data)