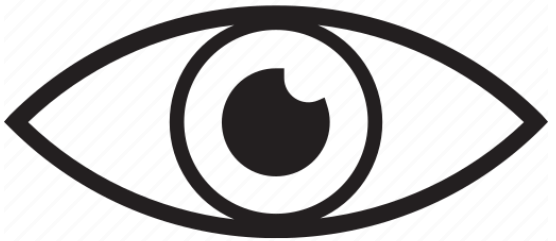
Privacy Preserving Technologies

Dr. Balázs Pejó

www.crysys.hu

1: Lecture Info



Goal

- Rather than going into the details, this class aims to raise awareness about many privacy issues and their current state-of-the-art solutions.
- Motivation to acquire systematic understanding of Privacy-Enhancing Technologies (PETs).
  - The class consist of ten lectures
- If you have any questions, please use the designated Teams channel; my ID is pejo.balazs@vik.bme.hu.
- References & Control Questions
  - Will be provided at the end of each class.
  - All material will be published on Moodle.
- **If any subject raise your interest, it is possible to do Project Laboratory / Thesis with us at CrySyS.**
  - https://crysys.hu/education/projects/
    - » https://crysys.hu/member/pejo & https://www.crysys.hu/~pejo/

PET Highlights

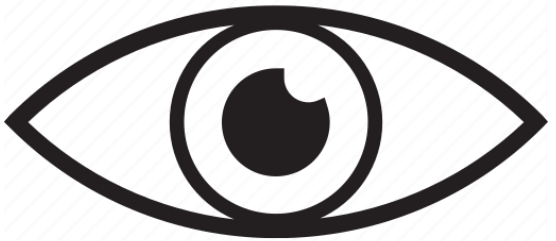
- Dark Patterns (x1)
  - Types / Legal & Technical Countermeasures / Cognitive Biases
- Tracking (x1)
  - Profiling / Online Data / Storage & Cache Tracking / Fingerprinting / Defense
- Law (x1)
  - GDPR: Rights / Data Types / Principles / Consent / Privacy Rights / Other Laws
- Deidentification (x2)
  - Attacks on (Un)Structured Data / Attacks on Aggregated Data: Entropy & Query Auditing & Reconstruction Attack & Attack on Location Data
- Machine Learning (x1)
  - Evasion & Poisoning & Backdoor / Inversion & Extraction & Inference & Reconstruction / Defense / Fairness & Explainability
- Anonymization (x2)
  - Primitives / K-Anonymity & More / Synthetic Data & Generative Models / Differential Privacy: Mechanisms & Models & Sensitivity & Dimensions
- Cryptography (x2)
  - CC & HE & SMPC & OT & SS & PSI & PIR & ZKP / Secure Messaging / Anonymous Communication & Mix Nets & TOR & Dark Web / E-Voting / Steganography / Cryptocurrencies

Schedule & Exam

- https://crysys.hu/education/VIHIAV35
- Moodle Exam
  - 23th May, 14 - 16
- 30 Multiple Choice
  - 3 from each topic
  - 1 Point Each
  - 45 min
- Grade
  - 2 : [15 - 18]
  - 3 : [19 - 22]
  - 4 : [23 - 26]
  - 5 : [27 - 30]
- Spare Exam
  - Oral / 4 Essay Q&A

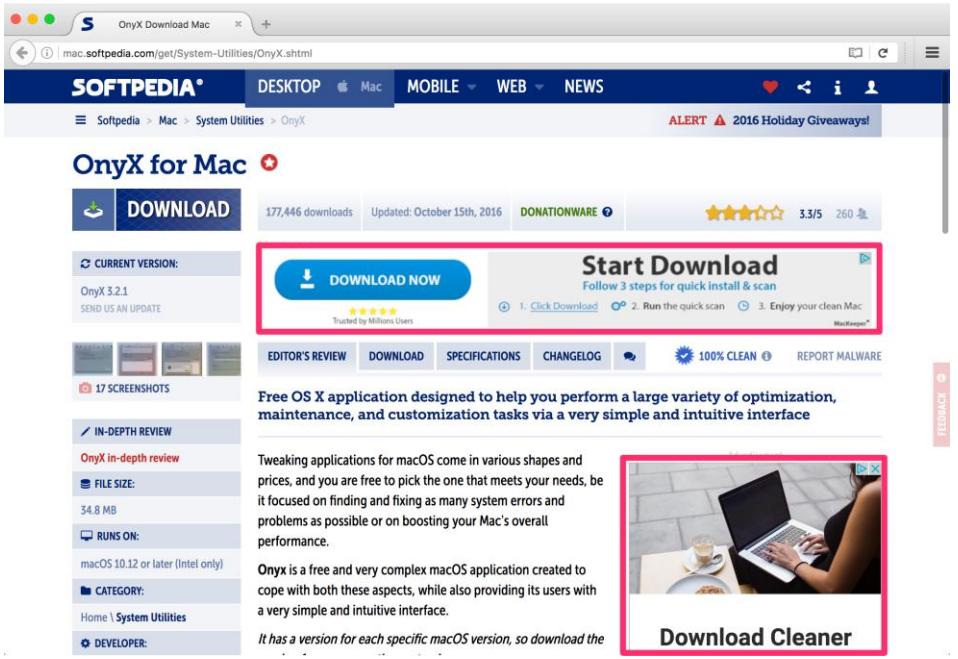
Date	Topic	Lecturer
Febr 13	Cancelled	-
Febr 20	Introduction and Motivation	Pejó B.
Febr 27	Dark Patterns: Types, Countermeasures, and Cognitive Biases	Pejó B.
Marc 6	Tracking: Profiling, Data Brokers, and Web Tracking	Pejó B.
Marc 13	Legal background of Data Protection: GDPR	Pejó B.
Marc 20	De-anonymization: Structured & Unstructured Data	Pejó B.
Marc 27	Re-identification: Entropy, Database Reconstruction, Query Auditing	Pejó B.
Apr 3	Machine Learning Privacy: Model Extraction & Inversion, Membership & Property Inferencene	Pejó B.
Apr 10	Anonymization Primitives, K-Anonymity, Synthetic Data	Pejó B.
Apr 17	Holiday	-
Apr 24	Holiday	-
May 1	Holiday	-
May 8	Differential Privacy: Properties, Mechanisms, Sensitivity, Dimensions	Pejó B.
May 15	Cryptography: Theory (HE/SMPC/OT/SS/PSI/PIR/ZKP)	Pejó B.
May 22	Cryptography: Applications (Secure Messaging / Steganography / Cryptocurrencies / E-Voting)	Pejó B.

01: Dark Pattern



Example: Disguised Ad

- A disguised ads are blending in the page or app, as if they were a part of the regular content or navigation.
  - For instance, the ad replicates a call-to-action button.
  - Every third click on an ad is by mistake, often by tricking the user.
  - Softpedia often run advertisements that look like a download button, tricking users into clicking on the ads rather than getting the thing they wanted.



Definition

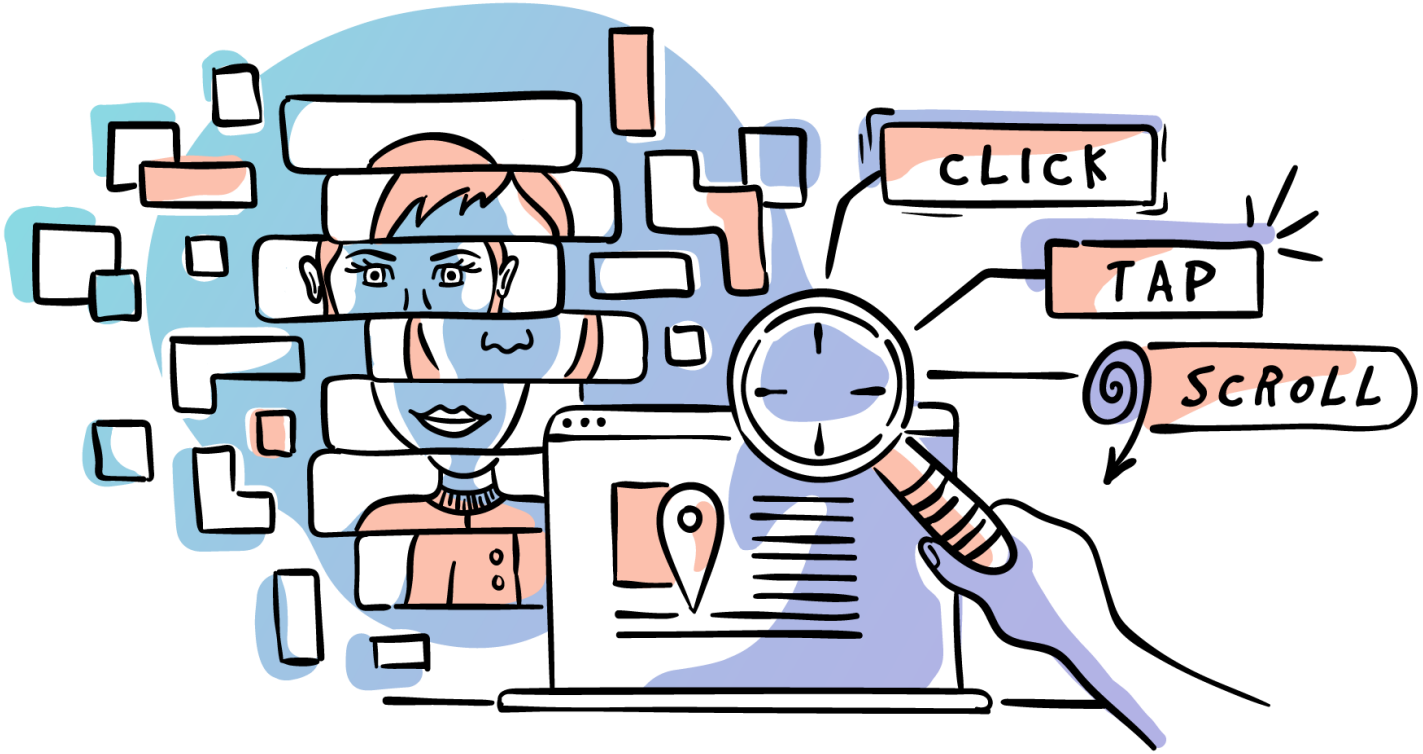
- Dark Patterns are carefully crafted interfaces that trick people into making decisions or performing actions that they otherwise would not.
  - Coined by Harry Brignull UX designer in 2010.
- Dark Patterns exploit human psychology for the sole purpose of encouraging people to act against their best interests.
  - We are not as in control of our actions as we like to think we are.
- Now called Deceptive Design.

Reason: Cognitive Bias

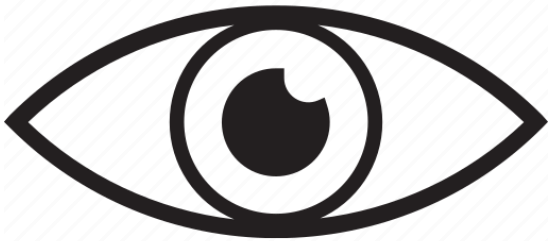
- The world is complex and fast, yet people must process and interpret information, for instance for decision making.
  - We receive roughly 11 million bits of information per second, but we can only process about 40 bits of information per second.
- Cognitive biases arise from our brain's efforts to simplify / make sense of the world to reach decisions (often as rules of thumb).
  - While the mechanism is effective, its limitations can cause subconscious (unintentional) errors.
- *I've studied cognitive biases my whole life and I'm no better at avoiding them.*
  - Daniel Kahneman

Loss Aversion

- The disutility of giving up an object is greater than the utility associated with acquiring it.
- It can be observed in the context of ‘free trials’, in which you allow the person to have access to a product or service for a certain, limited period and then, to allow continuity, one or more payments are requested.



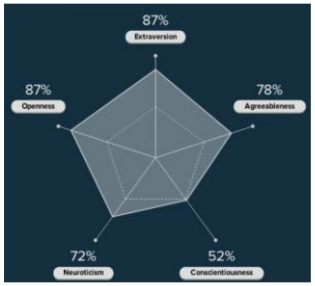
02: Tracking



Personalization

- People are different, with different level of susceptibility of different kind of Cognitive Biases.
- The effect of manipulations such as Dark Patterns could be increased with personalization.

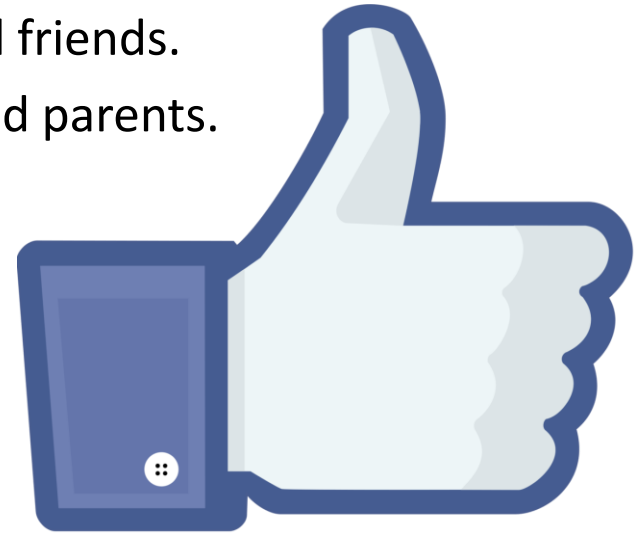
- The Big Five (OCEAN)
  - Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism.



- Ads that were matched to people's extraversion resulted in up to 40% more clicks and up to 50% more purchases.
  - Introvert:
    "Stay safe and secure with the new Iphone".
  - Extrovert:
    "Be where excitement is with the new Iphone".

Attack: Personality from Likes

- In 2015 86,220 volunteers shared their Facebook Likes and completed a 100-question personality survey that determined where they stood on the Big Five traits.
- Researchers trained a Machine Learning model to predict the personality based on Likes.
  - After 10 Likes the ML model outperformed colleagues.
  - After 70 Likes the ML model outperformed friends.
  - After 150 Likes the ML model outperformed parents.
  - After 300 Likes the ML model outperformed partners.
- (That time) on average, people on Facebook had 227 Likes.



Problem

- People cannot anticipate the future misuse of their data.
  - Tomorrow, one can develop a new ML model to infer sensitive details from seemingly harmless data that you share today.
  - Innocent details from different sources could be combined which might reveal undesired secrets.
- You can be stigmatized based on your religion, political affiliation, sexual orientation, etcetera.
- When you open a website and agree to give permission to share your consumer data with third-party partners, chances are that your personal data will end up being sold to a data broker.

No Free Lunch

- The entire economy of the internet is basically built on advertisement.
  - All the free stuff online is free, because you are the product.
- Companies know more about you than you would like, and they know more than you would think.
  - They know what you have done better than you do!

- Defense against data brokers:

Privacy Rights Clearinghouse

BrandYourself

Privacy Duck

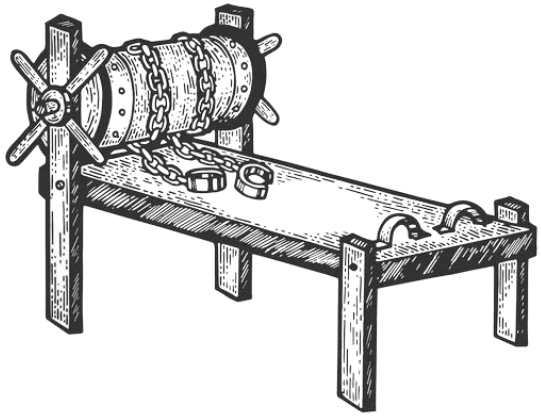
DeleteMe

03: Laws

General Rights

- Data protection is a right to protect any information relating to you as an identified or identifiable natural (living) person.
- Privacy is the right to private and family life, home and communications, to be autonomous, to be let alone.

- Fundamental rights are inherent to all humans, whatever our nationality, residence, sex, ethnicity, color, religion, language, etc.
  - Fundamental rights can be restricted, e.g., one can go to jail.
- Absolute rights cannot be restricted.
  - Not to be enslaved, not to be tortured, etc.



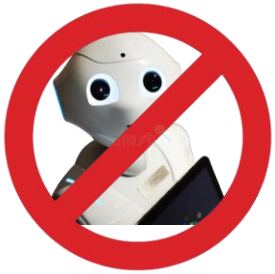
- Protection of private life and the protection of personal data are fundamental rights in EU.

Coverage

- Applies to all organizations processing the personal data of data subjects who reside in EU or the controller/processor has establishment in EU.
  - Focus on geography rather than citizenship.
- It does not apply to
  - Processing covered by the Law Enforcement Directive.
  - Processing for national security purposes.
  - Processing carried out by individuals purely for personal/household activities.
- It harmonizes data privacy laws across Europe.
  - Directly binding and applicable in all member states.

Privacy Rights

- Right to access
- Right to recitification
- Right to erasure (right to be forgotten)
- Right to object
- Right to restrict processing
- Right to data portability
- Right to be informed (transparency)
- Rights related to automated decisions and profiling

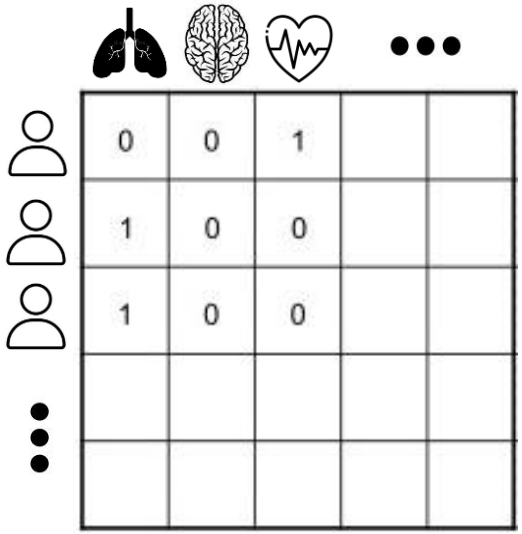


04 & 05: Deidentification

Dimensionality

- Refers to how many attributes a dataset has.
  - In an ideal world, data could be represented in a spreadsheet, with one column representing each dimension.
  - The actual dimensions can be unknown, as some columns could be correlated (e.g., duplicates), some are useless, etc.

- High (>1000) dimension is bad for privacy!
  - Healthcare has vast amounts of variables (e.g., blood pressure, weight, cholesterol level).

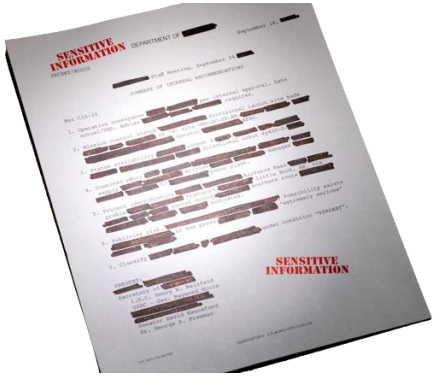


- Low (<100) dimensions bad for utility!

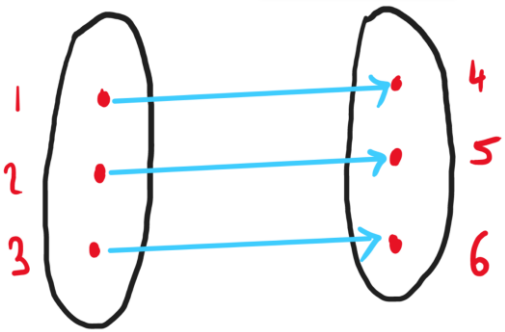
Column 1	Column 2
Peter	Human
John	Human
Kate	Human

Anonymized Data

- A simply anonymized dataset does not contain personally identifiable information (PII) such as name, address, phone number, etc.
- If individual patterns are unique enough, outside information can be used to link the data back to an individual.

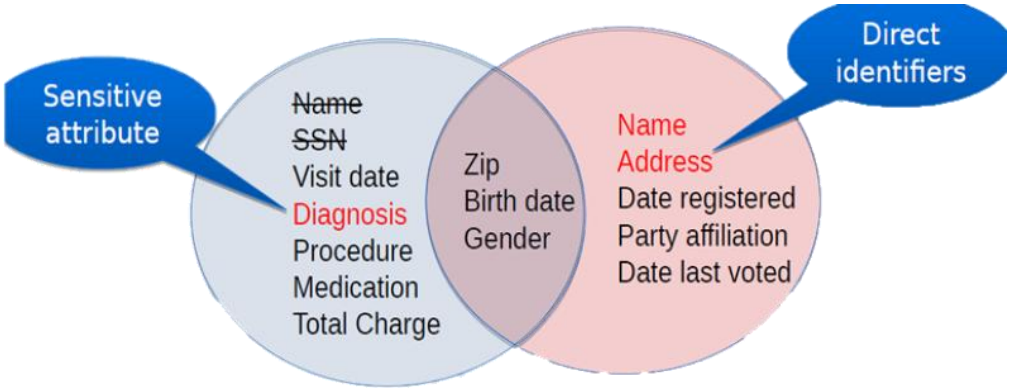


- Adversary has some prior (background) knowledge about its target.
- The attacker's task is to match pieces of information from the first source to pieces of information from the second source that correspond to the same underlying user.



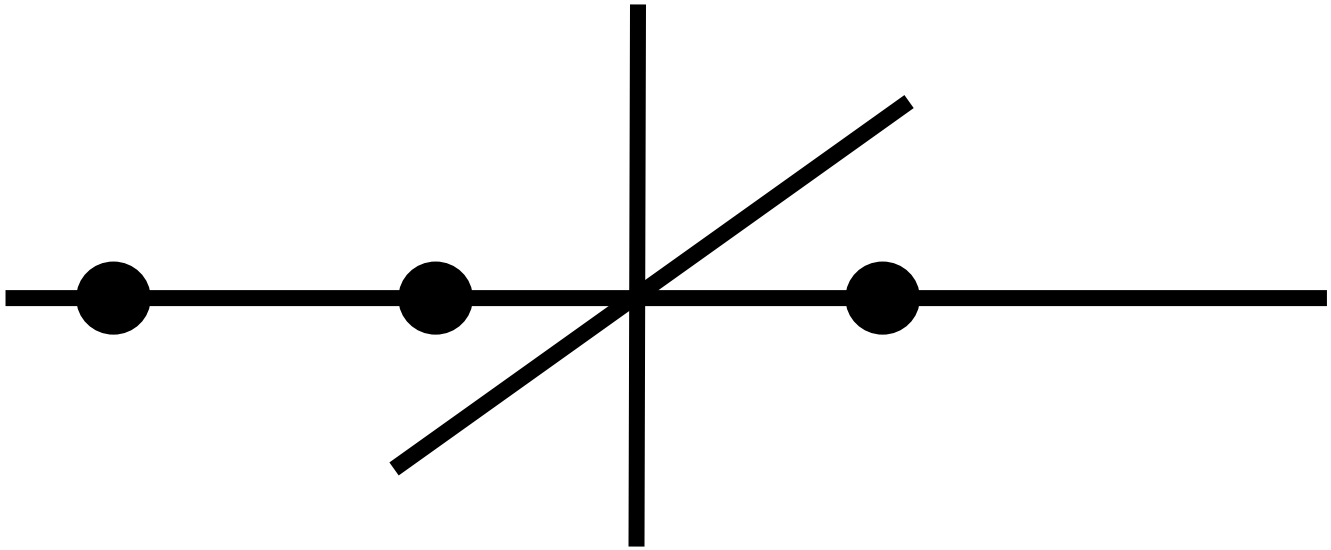
Targeted Attack on Medical Data

- In 1997 the Governor of Massachusetts strongly advocated for pseudo anonymized datasets.
- Latanya Sweeney de-identified him amongst the anonymized records by a Matching Attack.
  - She bought voter registration records for $10.
- She showed that data protection techniques used by American public administrations are at stake.
- In 2000 she concluded that 87% of the US population could potentially be identified by their ZIP code combined with gender and date of birth.



Curse of Dimensionality

- When the dimensionality increases, the volume of the space increases so fast that the available data become sparse.
- In high dimension, all records appear to be dissimilar in many ways, which assist re-identification.
  - If there are many attributes in a dataset, it is more likely that the adversary knows some of them that are enough to re-identify someone.

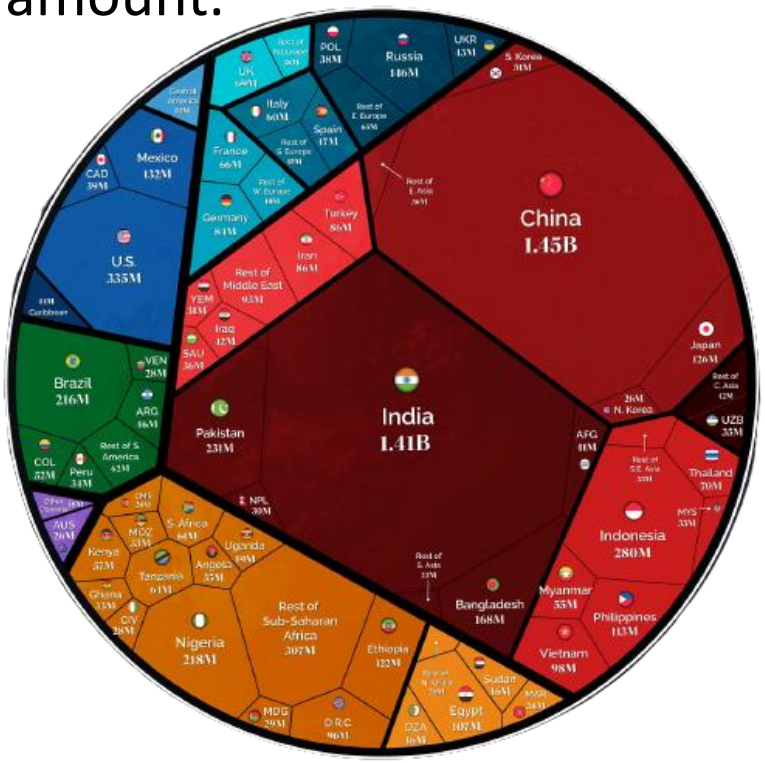


Reason: Entropy

- There are around 8 billion humans on the plane.
- The identity of a random, unknown person contains just under 33 bits of entropy ($2^{33} \approx 8$ billion).
- When we learn a new fact about a person, that fact reduces the entropy of their identity by a certain amount.

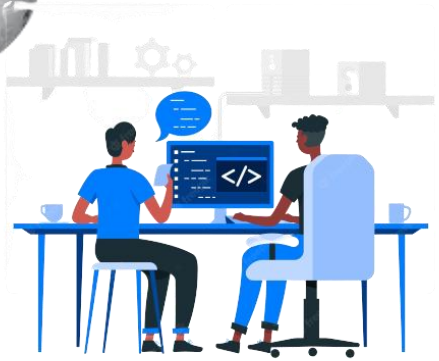
- $\Delta S = - \log_2 \Pr(X=x)$

- ΔS is the reduction in entropy, measured in bits.
- $\Pr(X=x)$ is simply the probability that the fact would be true of a random person.

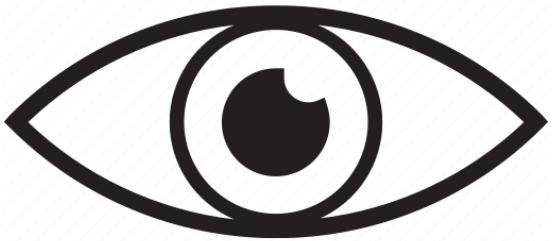


Example

- Western / Chinese Zodiac Sign: Ram & Goat
  - $\Delta S = -\log_2 Pr(\text{Starsigns=capricorn}) = -\log_2[1/(12x12)] = 7.2$
- City: Szolnok
  - $\Delta S = -\log_2 Pr(\text{ZIP=500*}) = -\log_2[70 \text{ thousand} / 8 \text{ billion}] = 16.8$
- Job: Software Engineer
  - $\Delta S = -\log_2 Pr(\text{Job=SE}) = -\log_2 (30 \text{ million} / 8 \text{ billion}) = 8.0$
- Starsigns & City & Job
  (assuming they are independent)
  - 7.2 + 16.8 + 8.0 = 33 bits
- Knowing all three pieces of information,
  we can probably say exactly who the person is!
  - By combining several facts, you might learn nothing, e.g., a starsign does not reduce the entropy if the birthday is already know.

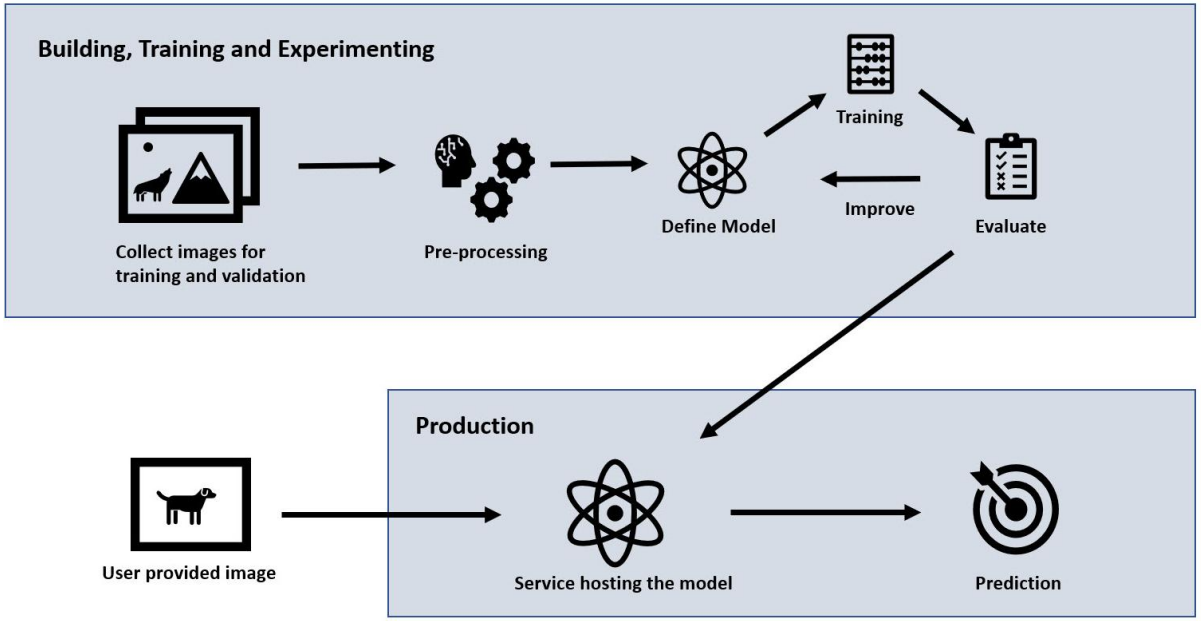


06: Machine Learning



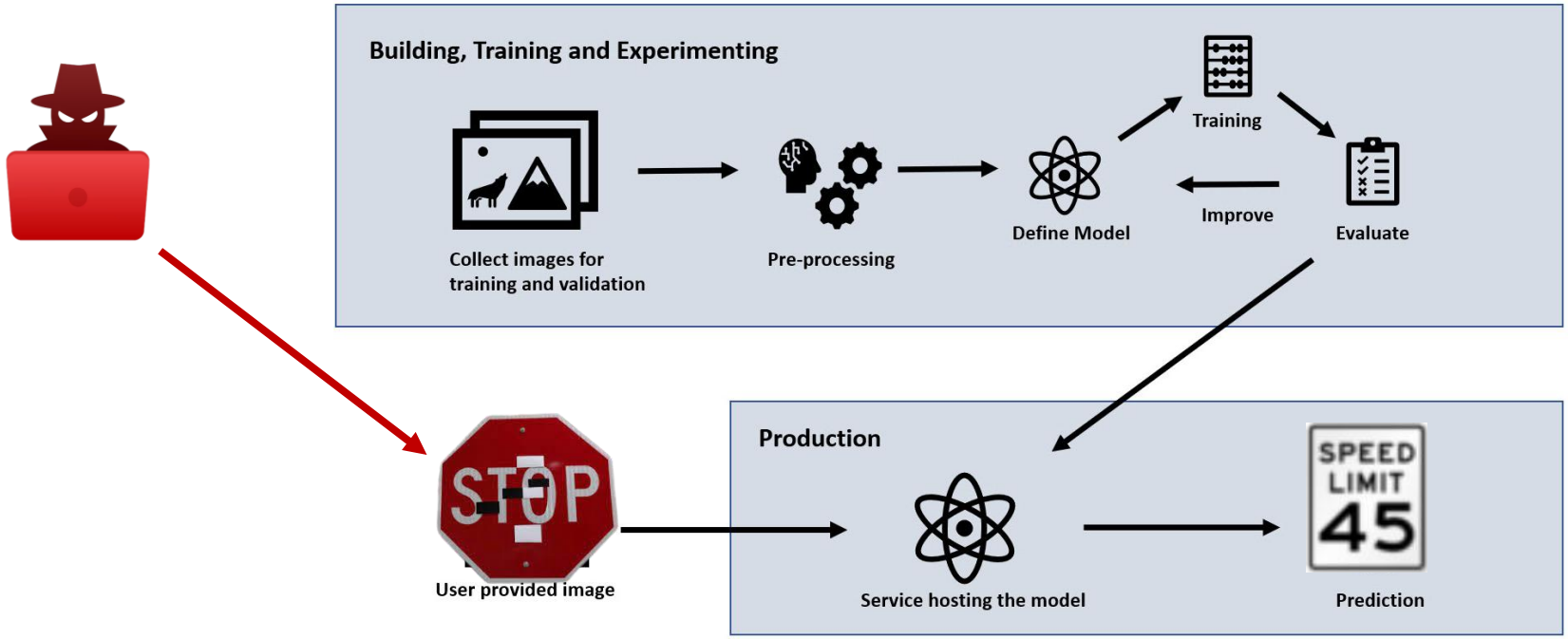
Machine Learning

- ML is the study of computer algorithms that improve automatically through experience.
  - It is seen as a subset of Artificial Intelligence.
- ML algorithms build a model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so.



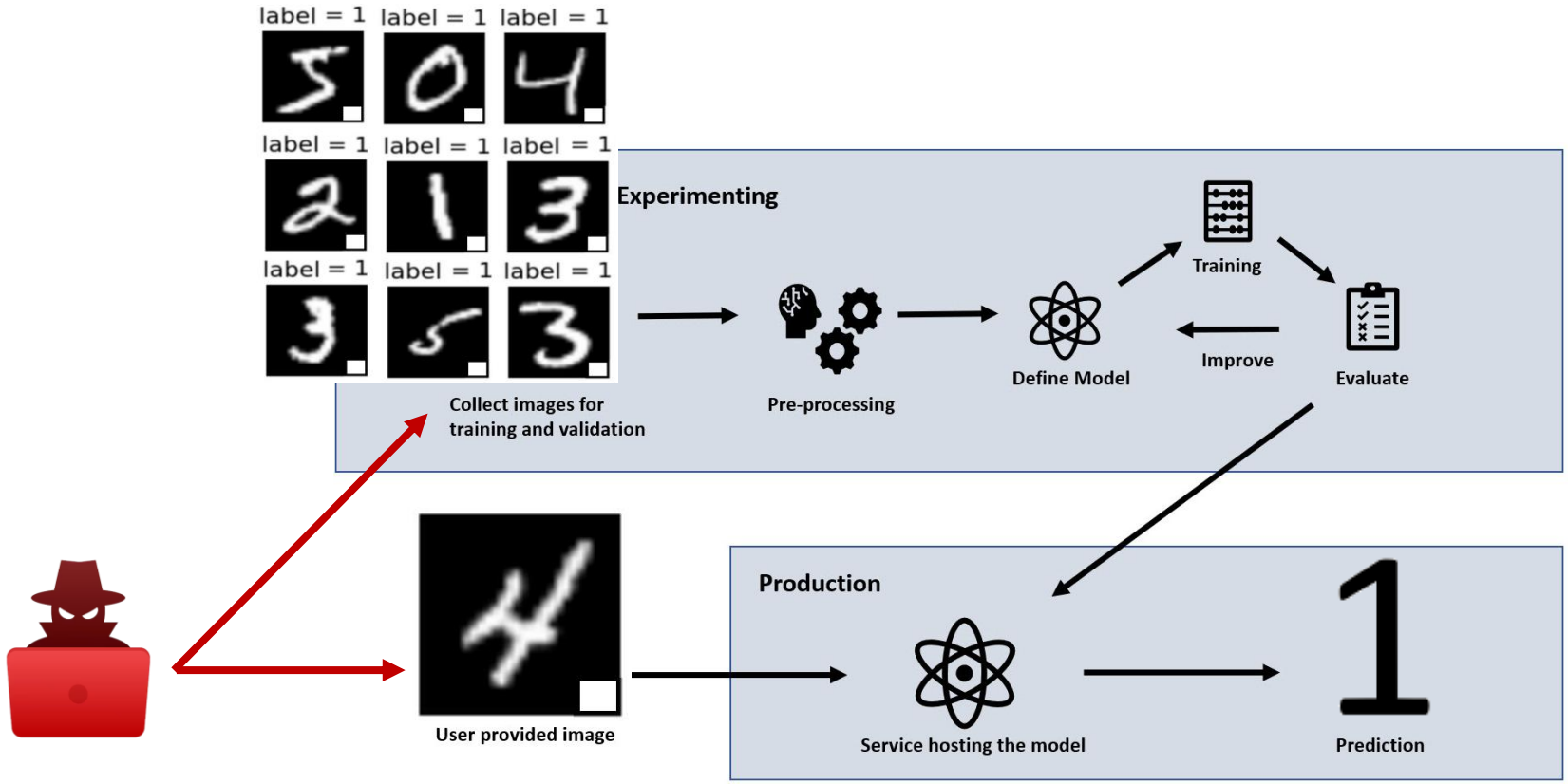
Attack After Training

- Samples are modified to evade detection, i.e., to be classified as legitimate.
  - Spammers and hackers attempt to evade detection by obfuscating.
- Access to the training data is not required.



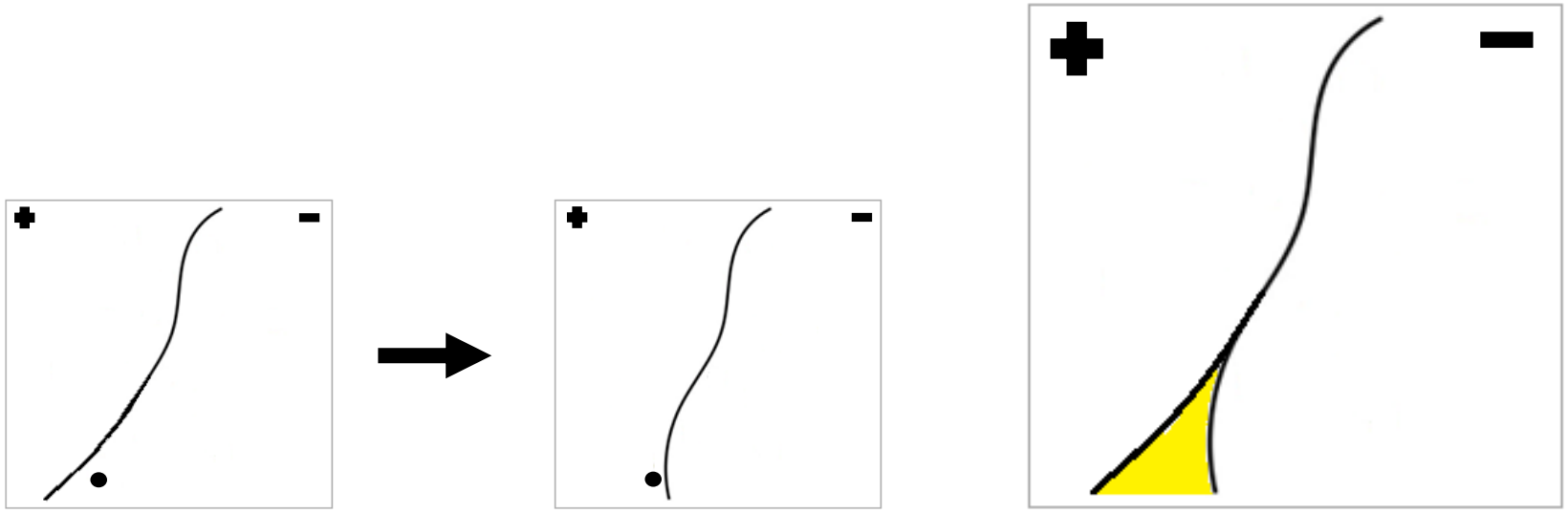
Attack Before Training

- A bad actor hides malicious behavior in a ML model during the training phase.
- Activates it when the AI enters production.



Reconstruction Attack

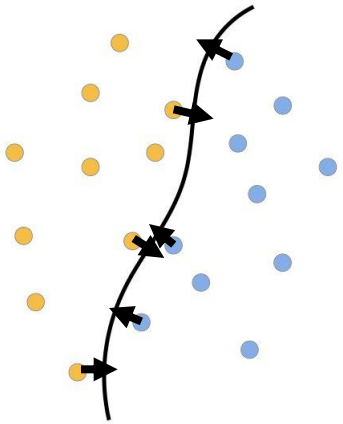
- Recovers “exact” training samples using the model updates.
- During training, the model is updated with the change corresponds to a data sample.
  - Data is given, model is given, change is optimized.
- An attacker can swap what is given and what is optimized.
  - Model is given, change is given, data is optimized.

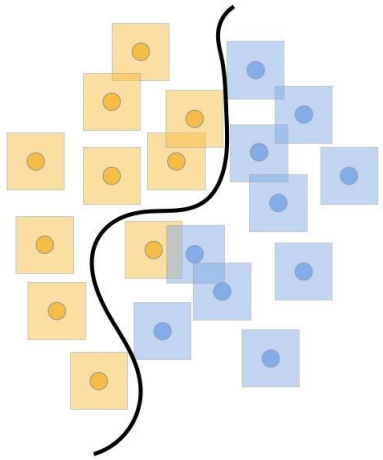


Defense: Robustness

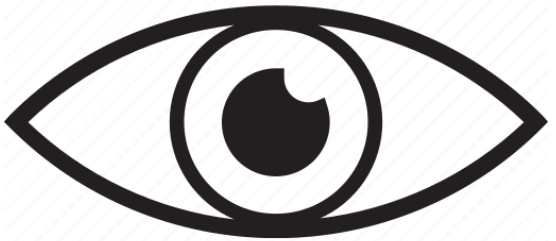
- An ML is robust to adversarial examples if its output is insensitive to small changes to any plausible input that may be encountered in deployment.
- ML algorithm f is r-robust at x if f(x)=f(x+n) where n is in B.
  - Few large changes (p=1)
  - More small changes (p=2)

$$B_p(r) := \{\delta \in \mathbb{R}^n : ||\delta||_p \leq r\}$$

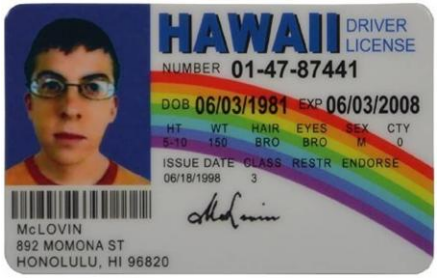




07 & 08: Anonymization



Attribute Types



- In terms of privacy, four types of attributes can be distinguished.

- Identifying: attribute which can uniquely identify a person.
  - E.g., name, phone number, social number, etc.
- Quasi Identifying: attribute that can uniquely identify a person if combined with other QI attributes.
  - E.g., sex, profession, age, etc.
- Sensitive: attributes including private information and must be kept private, but necessary for the analysis.
  - E.g., salary, diagnosis, etc.
- Insensitive: attributes that can be made public.
  - Depending on the context, almost anything can be a QI.

Anonymization

- Depending on the jurisdiction, different standards are applied.
- In Europe, the Article 29 Working Party's Opinion 05/14 says: Data is anonymized when three things are impossible:
  - Singling out: the possibility to isolate some records in the dataset.
  - Linkability: linking of data points of an individual to create a larger profile.
  - Inference: the ability to deduce one attribute from another attributes.

- Data are anonymised if all identifying elements (aka quasi-identifiers) have been eliminated.
  - No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned.
- Where data have been successfully anonymised, they are no longer personal data (i.e., can be shared, etc.).

K-Anonymity

- A dataset is said to be K-Anonymous if every combination of values for demographic columns in the dataset appears at least for K different records.
  - An attacker might find out the demographic information of their target, but then this will be linked to k different individuals, so it will be impossible to select which one.

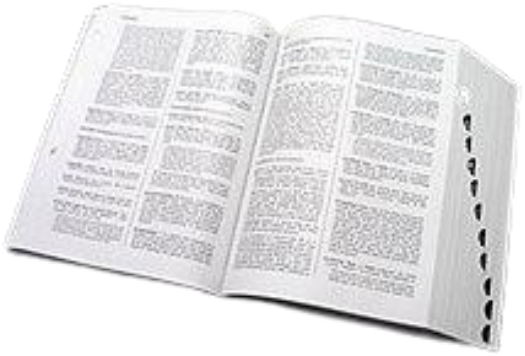
ZIP code	age
4217	34
1742	77
1743	77
4217	34

ZIP code	age
4217	34
1742	34
4217	77
1742	77

ZIP code	age
4217	34
4217	34
1742	77
1742	77

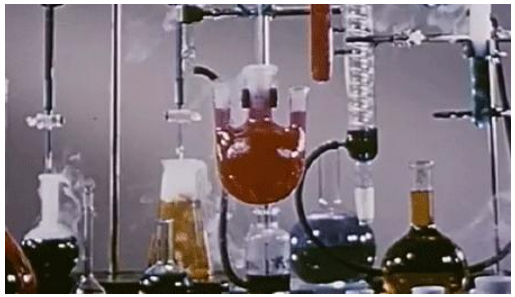
Problem

- K-Anonimity needed some assumptions about the attacker.
  - How much prior knowledge do they have?
  - What auxiliary data are they allowed to use?
  - What kind of information do they want to learn?



- K-Anonimity is a property of the output data.
- Instead, Differential Privacy is a property of a process.
  - You can't look at the output data and determine whether it satisfies DP.
  - Rather, you have to know how the data was generated to determine that.

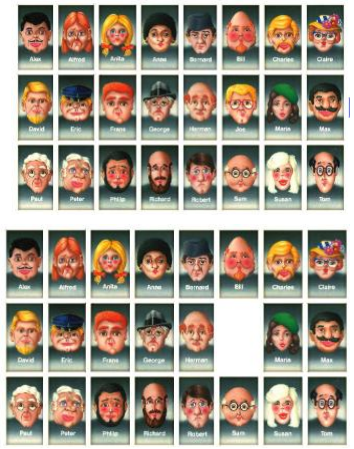
- The process can be anything.
  - Calculating some statistics.
  - A machine learning training process.
  - …



Differential Privacy

- A creepy person trying to figure out whether the target is in the original data.

- By looking at the output, he cannot be 100% certain of anything.
  - The result could have come from a database with the target in it.
  - It could also have come from the exact same database, without the target.



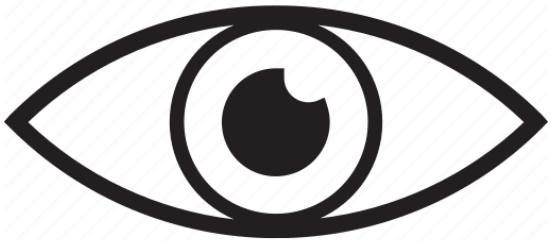
DP Mechanism

Data

Data

Basically the same

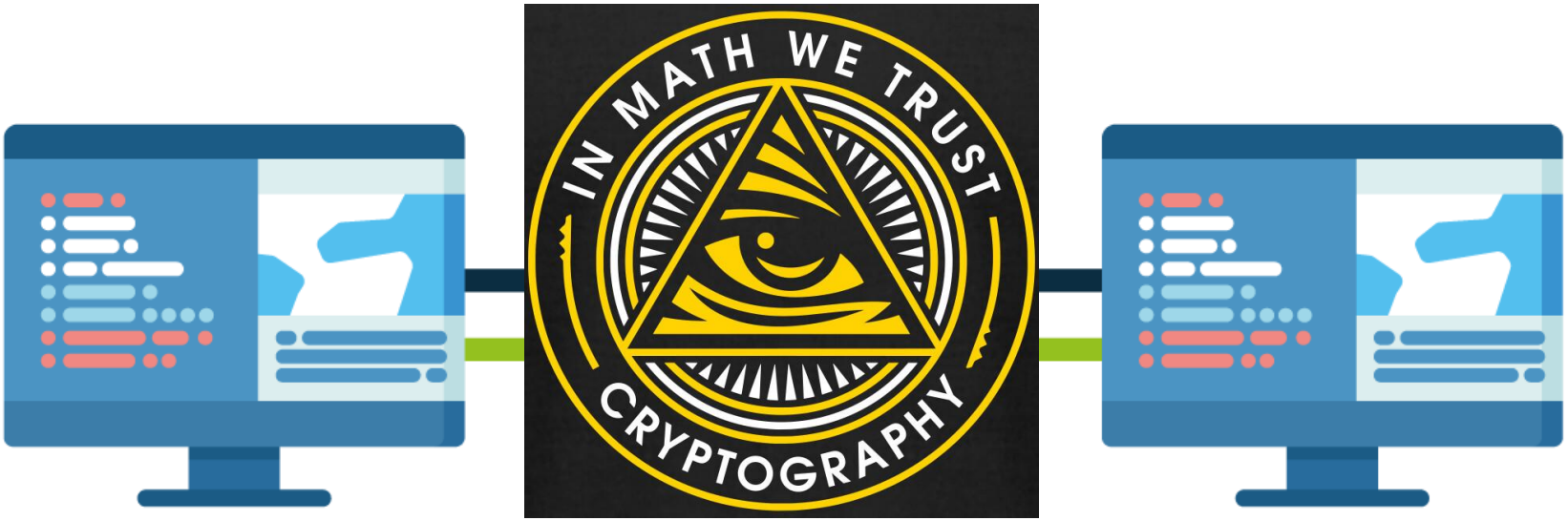
09 & 10: Cryptography



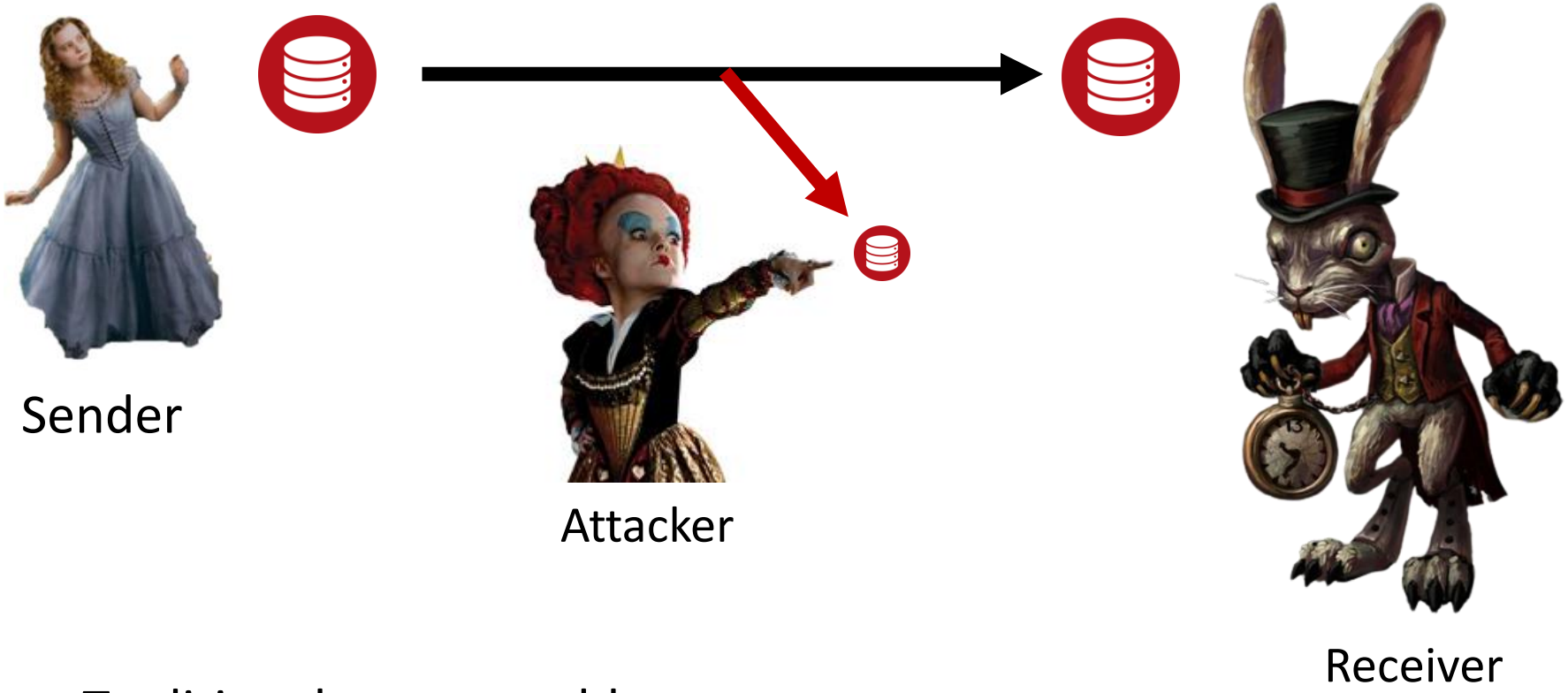
Privacy vs Cryptography

- Privacy is the RIGHT of an individual to control how information about him/her is collected, stored, and shared.
- Cryptography (old) is the practice and study of techniques for secure communication in the presence of adversarial behavior.

- Cryptography (new) is about replacing trust with mathematics.



Anonymous Communication



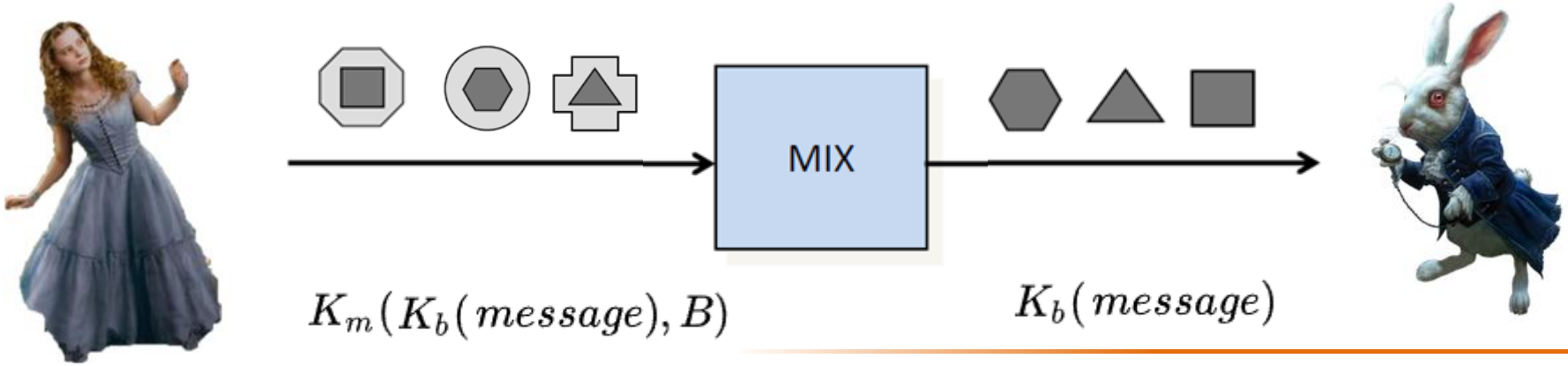
- Traditional crypto problem
  - Communication with a trusted entity on an unsecure channel.
- How to communicate with an untrusted entity in a secure manner?

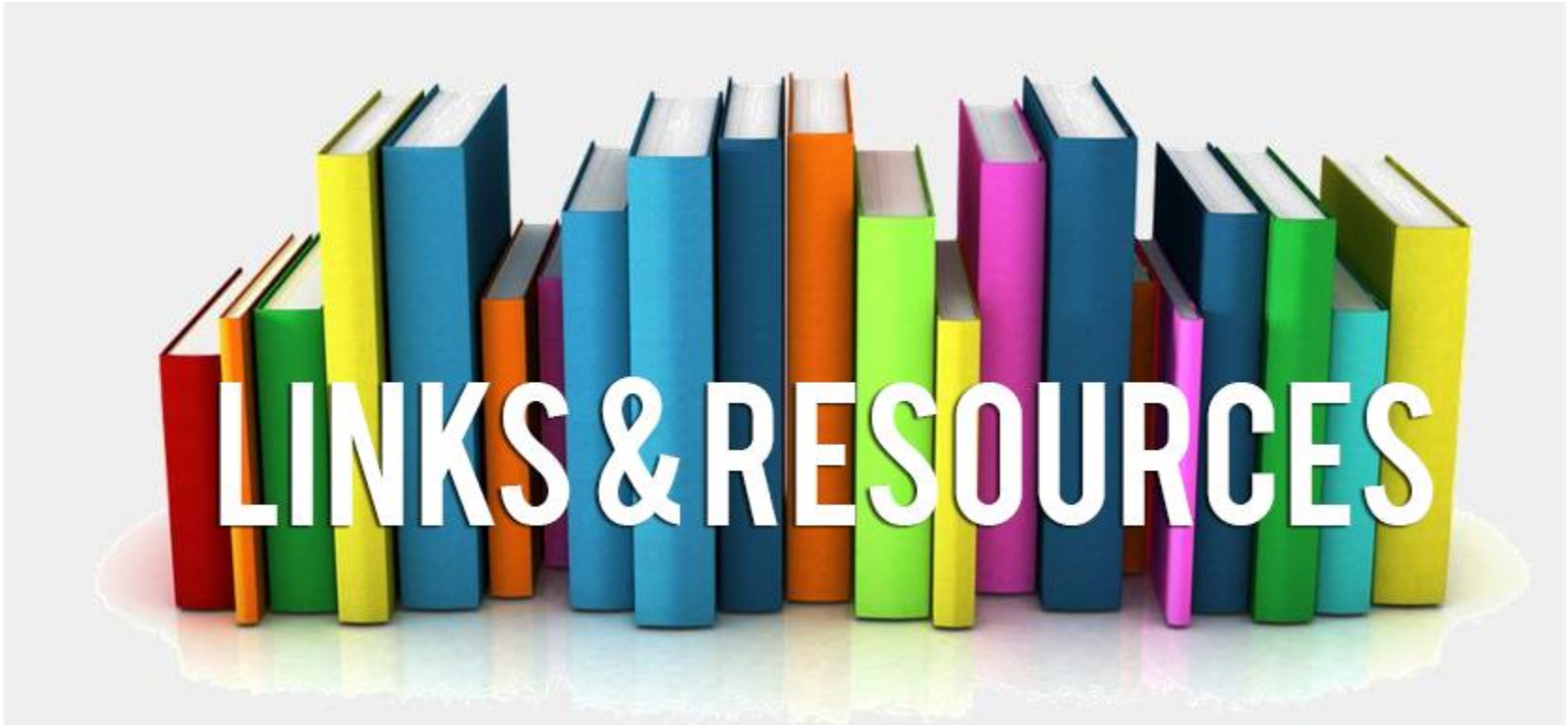
Anonymity Concepts

- Anonymity: The subject is not identifiable within a set of subjects, called the anonymity set.
- Unlinkability: Two or more items are unlinkable if the attacker cannot sufficiently distinguish whether they are related or not.
  - Sender-Receiver Unlinkability (Relationship Anonymity): We do not learn who communicates with whom.
  - Sender-Message Unlinkability (Sender Anonymity): We do not learn who sends which message.
  - Receiver-Message Unlinkability (Reciever anonymity): We do not learn who receives which message.
- Undectectability: The attacker cannot sufficiently distinguish whether something exists or not.

Mix

- A proxy that relays messages between communicating partners such that it
  - Changes encoding of messages.
  - Batches incoming messages and changes order when outputting them.
- Properties:
  - Sender anonymity w.r.t. communication partner.
  - Unlinkability w.r.t. global eavesdroppers.
- The Mix still needs to be trusted.





Resources

Course

- https://www.kau.se/cs/pdb
- Introduction to Privacy and the GDPR
  - https://kau.instructure.com/courses/5331
- Privacy Enhancing Technologies
  - https://kau.instructure.com/courses/5333
- Designing for Privacy
  - https://kau.instructure.com/courses/5335
- Privacy Management
  - https://kau.instructure.com/courses/5337
- Privacy Patterns for Software Design
  - https://kau.instructure.com/courses/5339

PRIVACY BY DESIGN

At Karlstad University, we have developed advanced level academic courses addressing critical aspects of the EU General Data Protection Regulation (GDPR).

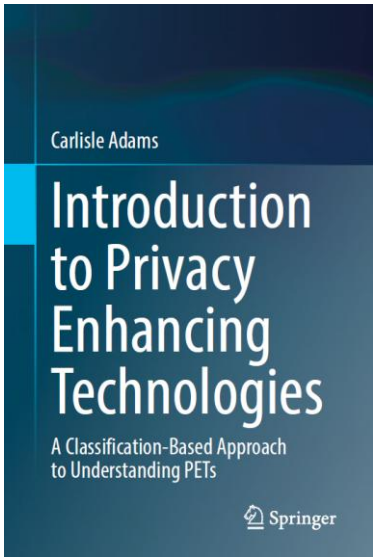
The courses are open for public access, to address the general interest, aid businesses competence development and their implementation of the regulation.

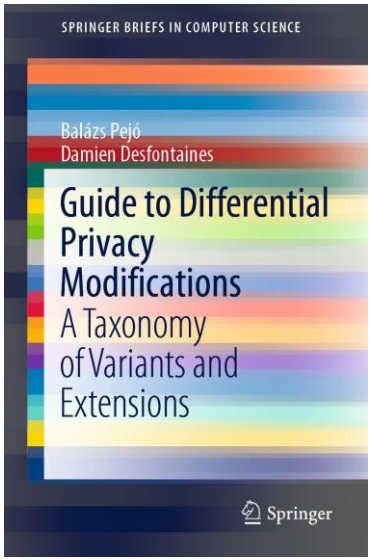
KARLSTADS UNIVERSITET
COMPUTER SCIENCE
DATAVETENSKAP

Guides & Books

- In 2023 both the United Nations and the Royal Society (UK) published a PET guide, in 2024 the NIST published an overview about Trustworthy and Responsible AI, …

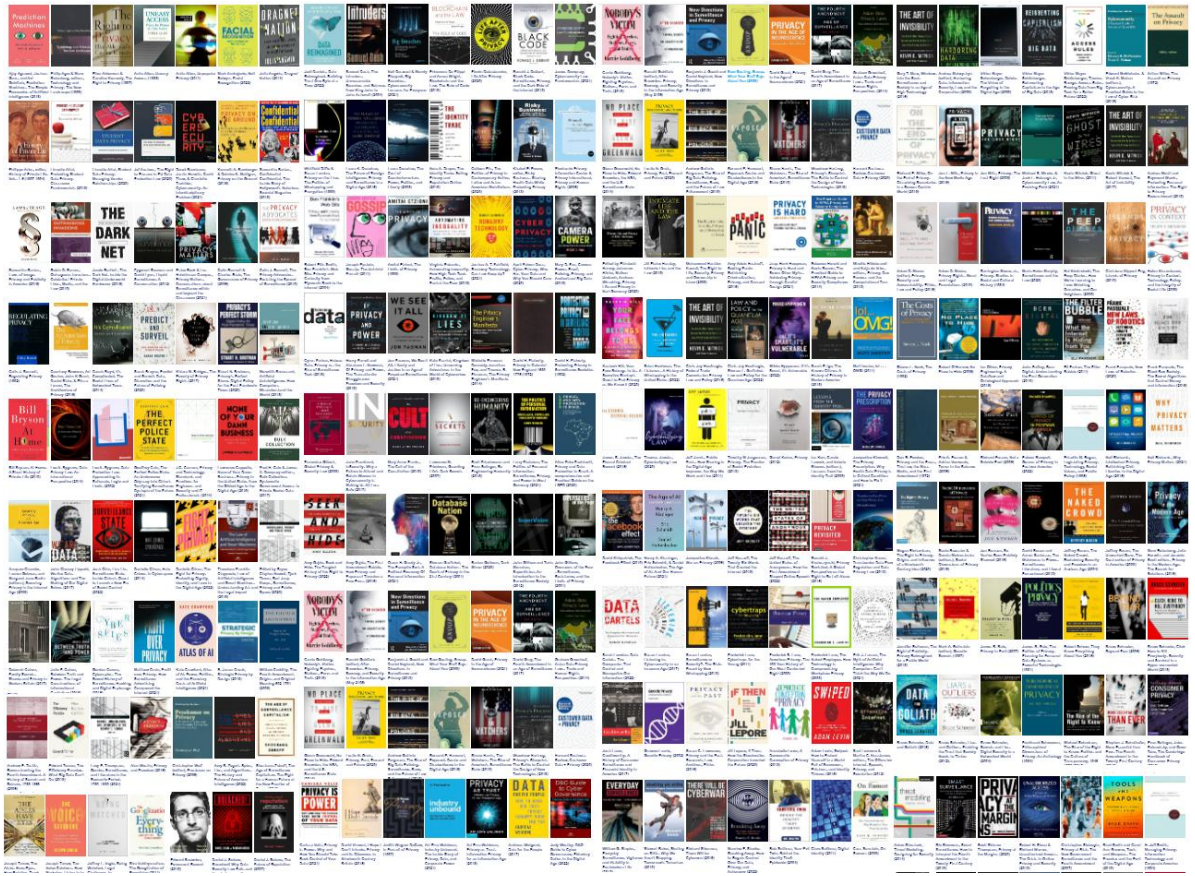
- Books about specific topics …





More Books

- https://www.privacysecurityacademy.com/non-fiction-privacy-security-books/



Movies


1. Sex Tape (2014)


2. The Circle (I) (2017)


3. Enemy of the State (1998)


4. Ordinary People (1980)


5. Wanderlust (2012)


6. Doubt (I) (2008)


7. Searching for Sugar Man (2012)


8. Mr. Church (2016)


9. Anon (I) (2018)


10. Three Colors: Red (1994)


11. The Sea Inside (I) (2004)


12. In the House (2012)


13. Harriet the Spy (1996)


14. The Experiment (2001)


15. Assassins (1995)


16. Citizenfour (2014)


17. The Final Cut (2004)


18. Luce (I) (2019)


19. The Good Neighbor (2016)


20. Citizen Ruth (1996)


21. Public Sex, Private Lives (2013)


22. Helter Skelter (2012)


23. The Red Pill (2016)


24. The Family Way (1966)


25. Madhouse (1990)


26. iHuman (2019)


27. All Light, Everywhere (2021)


28. Winnebago Man (2009)


29. The French Kissers (2009)


30. That Summer (2017)


31. An Acceptable Loss (2018)


32. Cryptopia: Bitcoin, Blockchains and the Future of the Internet (2020)


33. LSD: Love, Sex Aur Dhokha (2010)


34. The Girl Hunters (1963)


35. A Very Private Affair (1962)


36. Coded Bias (2020)


37. A Good American (2015)


38. Flocken (2015)


39. You've Been Trumped (2011)

40. Outrage (I) (2009)

41. Run & Jump (2013)

42. Terms and Conditions May Apply (2013)

43. The Tenants (2005)

44. Framed (II) (2021)

45. Smash His Camera (2010)

46. Rapt (2009)

47. Yesterday Once More (2004)

48. Girl 27 (2007)

49. Jakhalsdans (2010)

50. Break Free: Two People. Two Years. One Dream (2019)

51. Pudor (2007)

52. Koara kachô (2005)

53. The Business of Fancydancing (2002)

54. Urinal (1988)

55. Code 2600 (2011)

56. Serdtse mira (2018)

57. Stare Into the Lights My Pretties (2017)

58. Monero Means Money: Cryptocurrency 101, Live from Leipzig (2020)

59. Robot Stories (2003)

60. To karpouzaki (1962)

61. Blast 'Em (1992)

62. HAK_MTL (2019)

63. Nothing to Hide (2017)

64. Love (Part One) (2005)

Recommendations

- Books
  - Privacy is Power
  - Data and Goliath
- Ted Talks
  - Privacy in te age of AI
  - Privacy in the Digital Age
  - Data Privacy and Consent
  - Why privacy matters
  - You are your data
  - How a handful of tech companies control billions of minds every day
- Movies
  - Gattaca
  - Black Mirror
  - Ex Machina
  - Citizen Four
  - Social Dilemma
  - The Lives of Others
  - The Truman Show
  - Enemy of the State
  - Minority Report

Blogs & Podcasts & Videos & …

- https://medium.com/tag/privacy
- https://desfontain.es/privacy/
- https://backgroundchecks.org/top-30-privacy-blogs.html
- …
- https://teachprivacy.com/funniest-privacy-videos/
- …
- *“The internet gave access to everything;*

  … but it also gave everything access to us. “

Rank	Privacy Podcast	Logo	PSRa…	Peopl…	Org	Tag1	Tag2	Tag3
1	Serious Privacy		8.2	Paul Breitbarth, K Royal	TrustArc	data privacy	privacy pros	compliance
1	Privacy Please		8.2	Cameron Ivey, Gabe Gumbs	Spirion	data privacy	cybersecurity	compliance
1	Data Diva Talks Privacy		8.2	Debbie Reynolds	Debbie Reynolds Consulting	data privacy	data & tech	privacy pros
4	Data Protection Breakfast Club		8.1	Andy Dale, Pedro Pavón	Alyce	data privacy	data protection	privacy pros
4	She Said Privacy/He Said Security		8.1	Jodi Daniels, Justin Daniels	Red Clover Advisors	data privacy	cybersecurity	compliance
4	Caveat		8.1	Dave Bittner, Ben Yelin	CyberWire	cybersecurity	surveillance	digital privacy
7	Decrypted Unscripted		8.0	Dominique Shelton Leipzig, David Biderman	Perkins Coie LLP	data privacy	policy	compliance
7	Data Privacy Unlocked		8.0	David M. Stauss	Husch Blackwell	data privacy	policy	compliance
9	Privacy Advisor		7.9	Jedidiah Bracy	IAPP	data privacy	policy	privacy pros
9	FIT4PRIVACY		7.9	Punit Bhatia	FIT4PRIVACY	data privacy	GDPR	privacy pros
9	Data Democratization		7.9	Jeffrey Dobin, Alexandra Ebert	mostly.ai	data privacy	data & tech	privacy engineering
9	That Tech Pod		7.9	Laura Milstein, Gabi Schulte	That Tech Pod	data privacy	cybersecurity	eDiscovery