SYNOPSYS®

Having Our Cake And Eating It Too: Are Safety, Security and Privacy Possible Simultaneously?

EPFL Elephants in the Technology Room Symposium

Mike Borza, Synopsys Scientist

Montreux April 20, 2023

Defining Our Terms

In the limited context of the ICT systems that people use

Safety: Freedom from risk of injury, damage or destruction

- Of the system itself and/or of its users

Security: Only authorized entities can access or modify assets of a system

- Usually defined in terms of properties like confidentiality, integrity, availability, …

Privacy: Freedom to control how information about oneself is used

Two observations:

- No safety without security
- Systems people use are often treated as representative of those individuals

Safety in the Small, Safety in the Large

Example: Safety of railway signaling systems

https://d.newsweek.com/en/full/61730/high-speed-trains-ta05-wide.jpg

- Older notions of safety were defined in a narrow context
  - The safety system only addressed trains, not the people in them
- The safety system did not explicitly need to have security
- Obscurity as security
  - “Nobody would interfere with operation of a train”
  - “It's a proprietary protocol, nobody can figure it out”

Inherent Tension Between Safety & Security

What's the safe response, what's the secure response?

https://www.hseblog.com/wp-content/uploads/2018/04/Difference-Between-Safety-and-Security-2.jpg

- “Mixed Criticality”: use security to establish the conditions for safety, let the safety system dominate
- In future highly-connected distributed safety systems, this becomes less clear
- What's the meaning of an authentication error?
- Fallback modes of operation are needed
- Largely a technical solution and discussion
- But with societal and potentially legal implications
- Classic example: Avoid a crash that kills the people in a car, but kills a pedestrian

Identity: Foundation of Trust & Security

https://images.idgesg.net/images/article/2018/08/8_authentication-basics_password_identity_protected_security-100768041-large.jpg

- With few exceptions (e.g. PGP), transitive trust is the basis for identity
- “I trust Google/Apple/ Vodaphone/US Gov’t”
  - Ergo: “I trust your identity as attested by them”
- Having an identity means submitting to the authority of the identity issuer
- Having an identity means you can be tracked when presenting it

Safety in the Public Realm

https://static.ffx.io/images/$zoom_0.2718870346598203%2C$multiply_0.7554%2C$ratio_1.776846%2C$width_1059%2C$x_0%2C$y_0/t_crop_custom/q_86%2Cf_auto/e9fddc30ec58d1ea8cb6bee1af2bfd35f9d3b6d3
https://data.nextshark.com/wp-content/uploads/2017/09/chinasurveli-768x408.jpg

- Ubiquitous surveillance as a public safety tool
- If every utterance, movement, action is permanently recorded, can we still have free speech & association?
  - Is this evidence of incitement or conspiracy?
- Massive AIs distill & identify threats
  - Bias, misinterpretation?
- Right to forget?
- What about the AI tools themselves?
  - They can become vectors for leaks and subject to manipulation

Following Breadcrumbs: Can I Collect Enough Information to Track & Monitor You?

https://www.anomali.com/images/made/images/uploads/blog/Artificial_Intelligence_Data_Privacy__1000_500.jpg

- Ubiquitous video surveillance may be obvious, but is it the only way?
- Model: the browser “fingerprint”
- SIGINT: what can I learn just by watching you in relation to others I track?
- Strong identity in my devices & on my person become power tools to do this
- The amount of these data increases over time
- As does the ability to store, fuse & correlate it

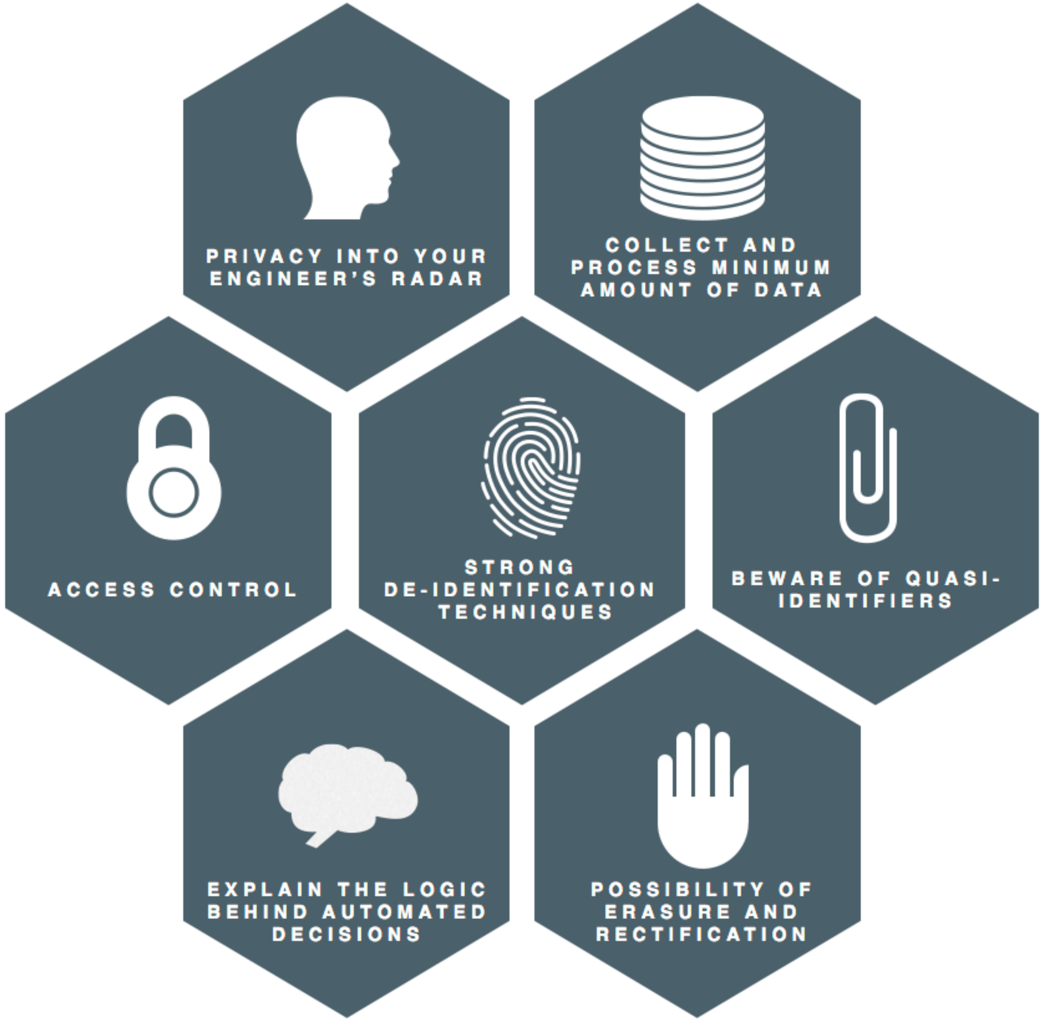
Social Media and Societal Norms

In a social media age, do privacy & anonymity even matter?

https://qph.fs.quoracdn.net/main-qimg-dbe987ea650d23dc1596c3b57d564118
https://1.bp.blogspot.com/-Vh7JpzkjqOI/XTbuAZjfFBI/AAAAAAAAyPE/j2Z-fbteNtgGAs1bNFAlo9aMpi-UwerEwCLcBGAs/w1200-h630-p-k-no-nu/1.png

- Is this just the concern of an old and dying generation?
- How do youth think about privacy?
  - Will they lament their loss of privacy in future?
  - Do they even think of their use of social media as a loss of privacy?
- Can it be regained?

Policy and Legislative Solutions

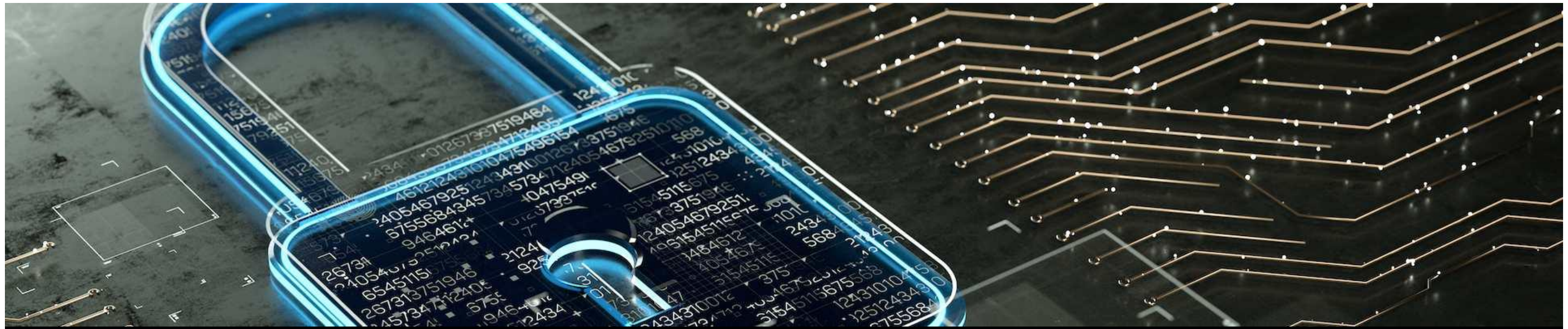

PRIVACY INTO YOUR ENGINEER'S RADAR
COLLECT AND PROCESS MINIMUM AMOUNT OF DATA
ACCESS CONTROL
STRONG DE-IDENTIFICATION TECHNIQUES
BEWARE OF QUASI-IDENTIFIERS
EXPLAIN THE LOGIC BEHIND AUTOMATED DECISIONS
POSSIBILITY OF ERASURE AND RECTIFICATION

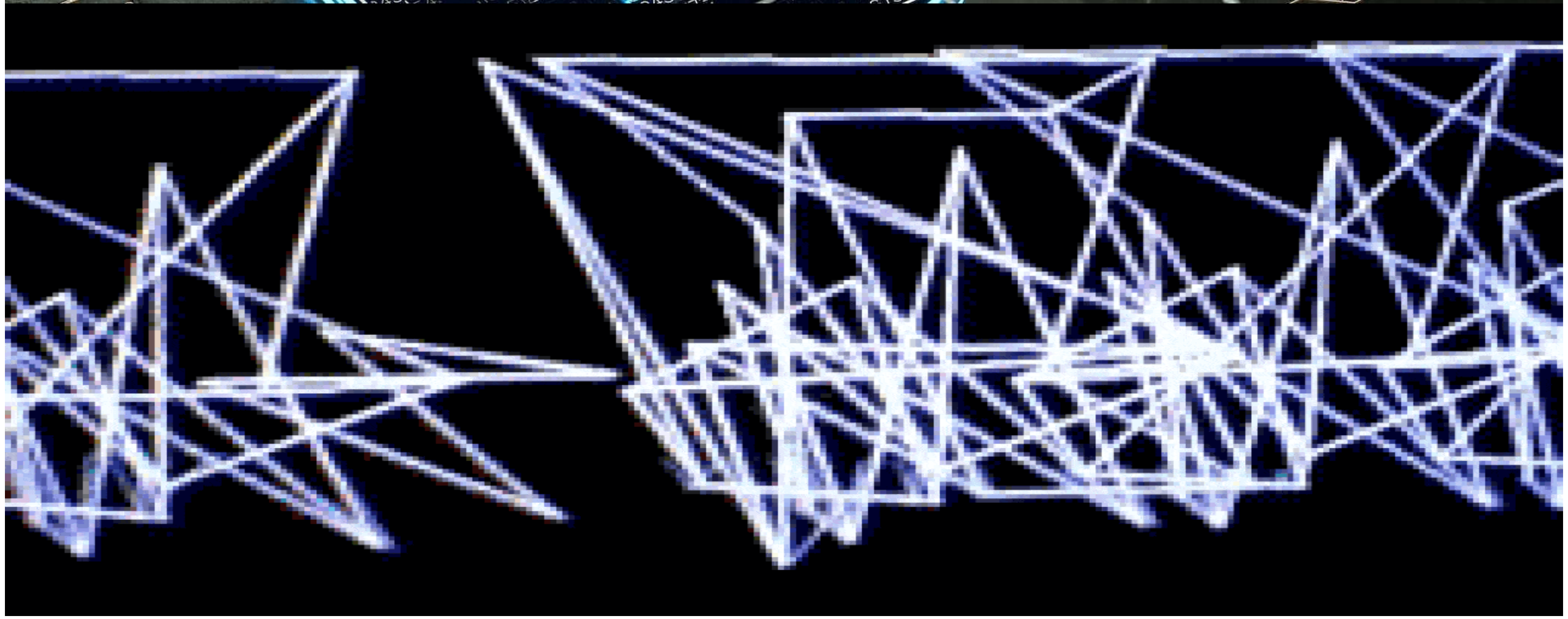
https://miro.medium.com/v2/resize:fit:1720/0*30IhOknPZyACOSlC.png

- Are they sufficient?
- Are they (or can they be) effective?
- GDPR is the broadest and best-known example
  - Viewed as quite effective
  - But its slow and necessarily reactive
- Are big fines just a cost of doing business?
- What to do about the fact that technical circumvention is always possible?

The Big Challenge: Can We Build Strong Technical Privacy Solutions?

And make them ubiquitous?

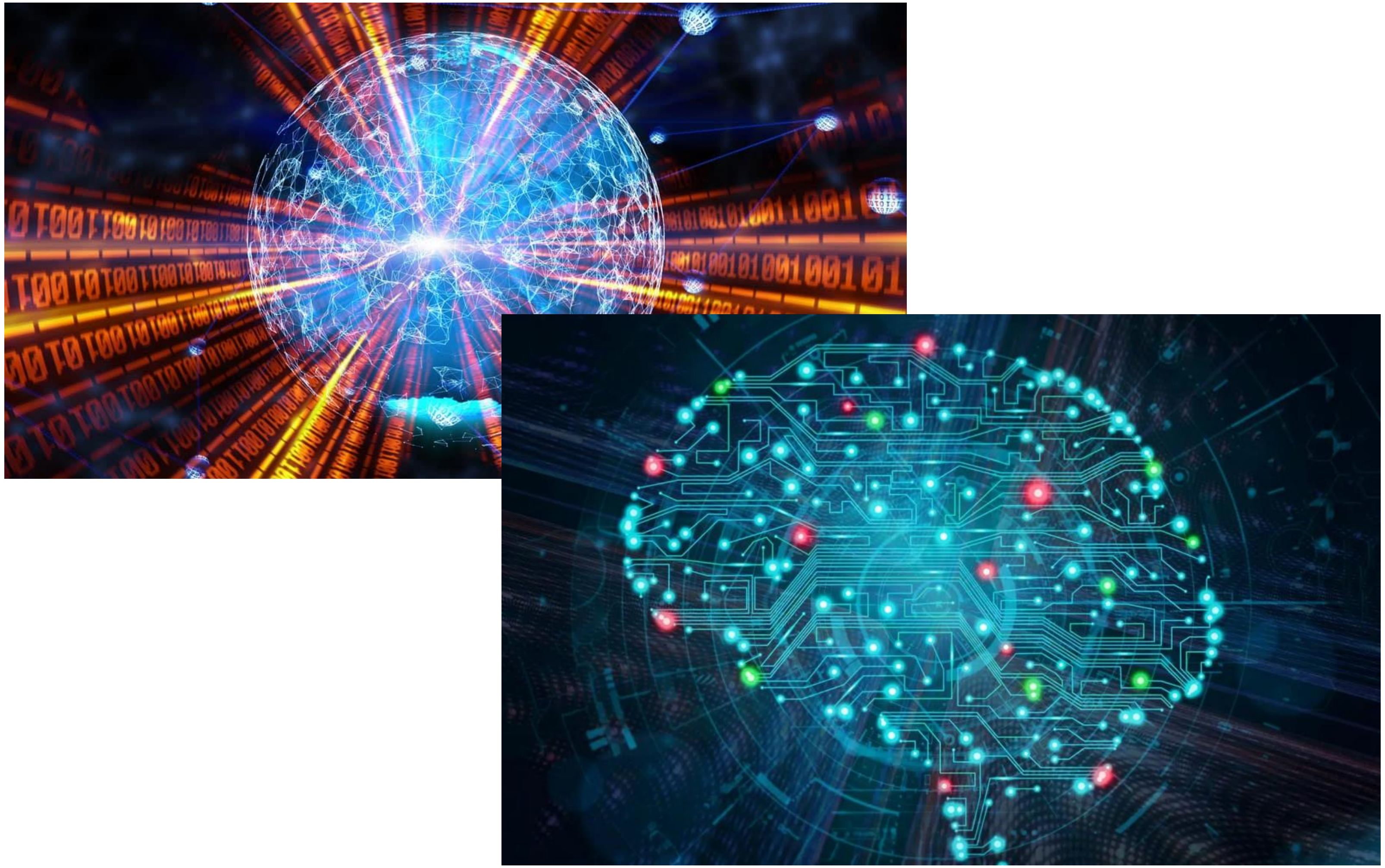




https://images.fastcompany.net/image/upload/w_1280,f_auto,q_auto,fl_lossy/fc/3035879-poster-homomorphic-cropped.jpg
https://www.arm.com/-/media/global/resources/newsletter/arm-cca-1920x390.jpg?revision=9d674748-e9c0-4405-9a45-476cb57c8cb5

- We might…
- Confidential computing actively advancing & backed by hyperscalers
  - But it is still a kind of trust model without guarantees
  - Widespread deployments will take years
- Fully homomorphic encryption (compute over encrypted data) is becoming feasible
  - This does provide strong guarantees of privacy
  - Likely a big part of an eventual solution
- Improved zero-knowledge identity proofs

Looking Forward to the 30’s



https://scitechdaily.com/images/Artificial-Intelligence-Quantum-Mechanics-1536x1024.jpg
https://physicsworld.com/wp-content/uploads/2020/11/quantum-computing-or-comms-1008154320-iStock_johnason.jpg

- 2 major development threads
  - AI, especially including neuromorphic processing
  - quantum computing (QC)
- AI+quantum computing
  - Wide availability & inherent parallelism afforded by QC matches the needs of neuromorphic AI
  - Human neurology teaches us that the presence of noise need not prevent useful work
  - Learn how to exploit this
- These advancements mostly work against privacy
  - Need that be true?

Beyond the 30’s

https://btlaw.com/-/media/images/btlaw/content/artificial-intelligence_detail.ashx?h=1280&w=1920&la=en&hash=7A40BECA760B75FF9DD39D5A9C46FC91BDA5AC50

- Our current progress creates the ingredients for our successor “species”
- Artificial General Intelligence: a machine that learns & evolves
  - At electronic speed, not biochemical speed
- Competing AGIs will consolidate to a single global AGI
- This will mark the start of transition to “Silicon life”

Thank You

synopsys®