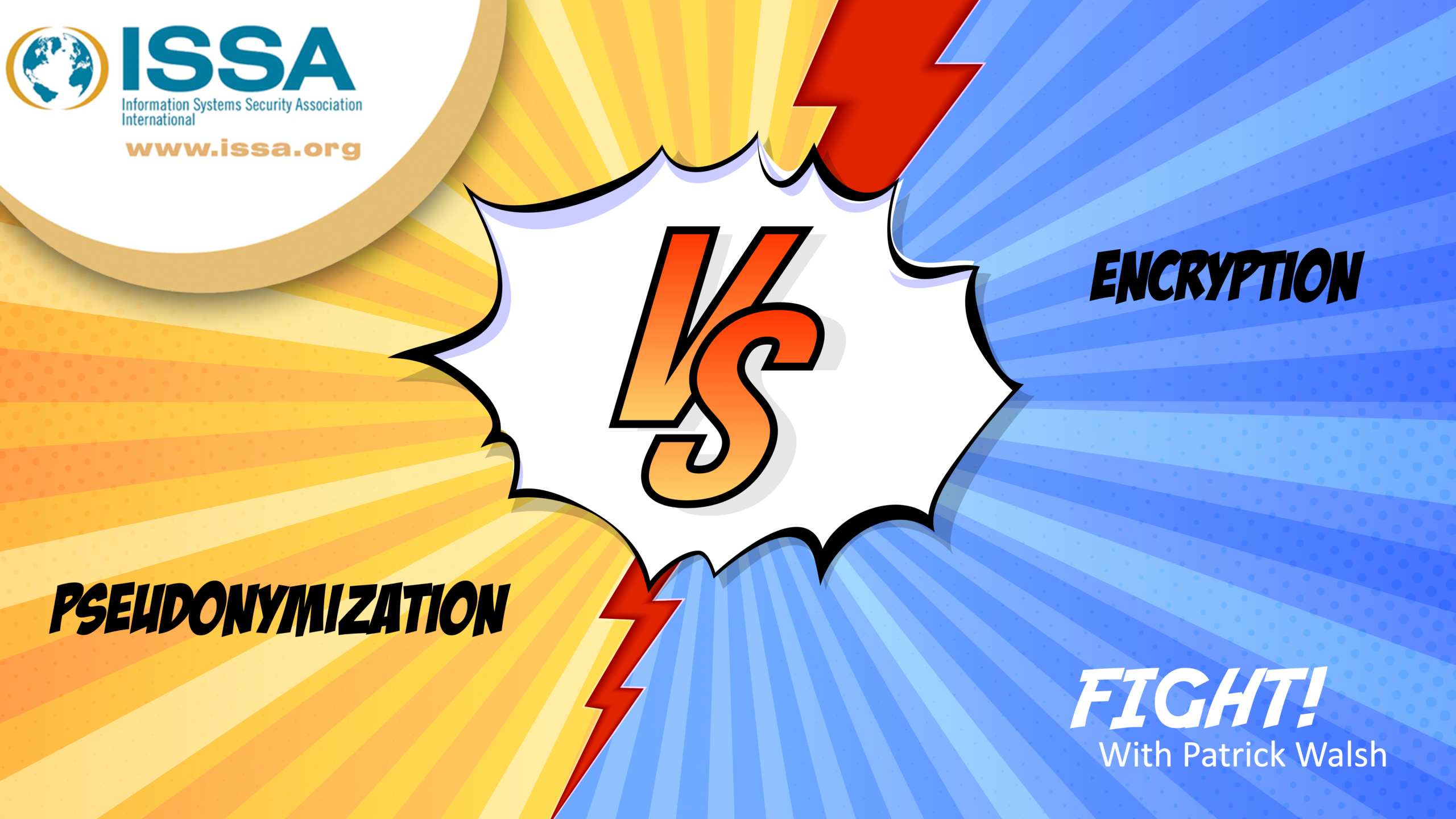

ISSA
Information Systems Security Association International
www.issa.org
VS
ENCRYPTION
PSEUDONYMIZATION
FIGHT!
With Patrick Walsh

Janelle Hsia

20 years as a trusted advisor with a focus on privacy and security with a diverse background.

ISSA
Information Systems Security Association International

Patrick Walsh

CEO IronCore Labs

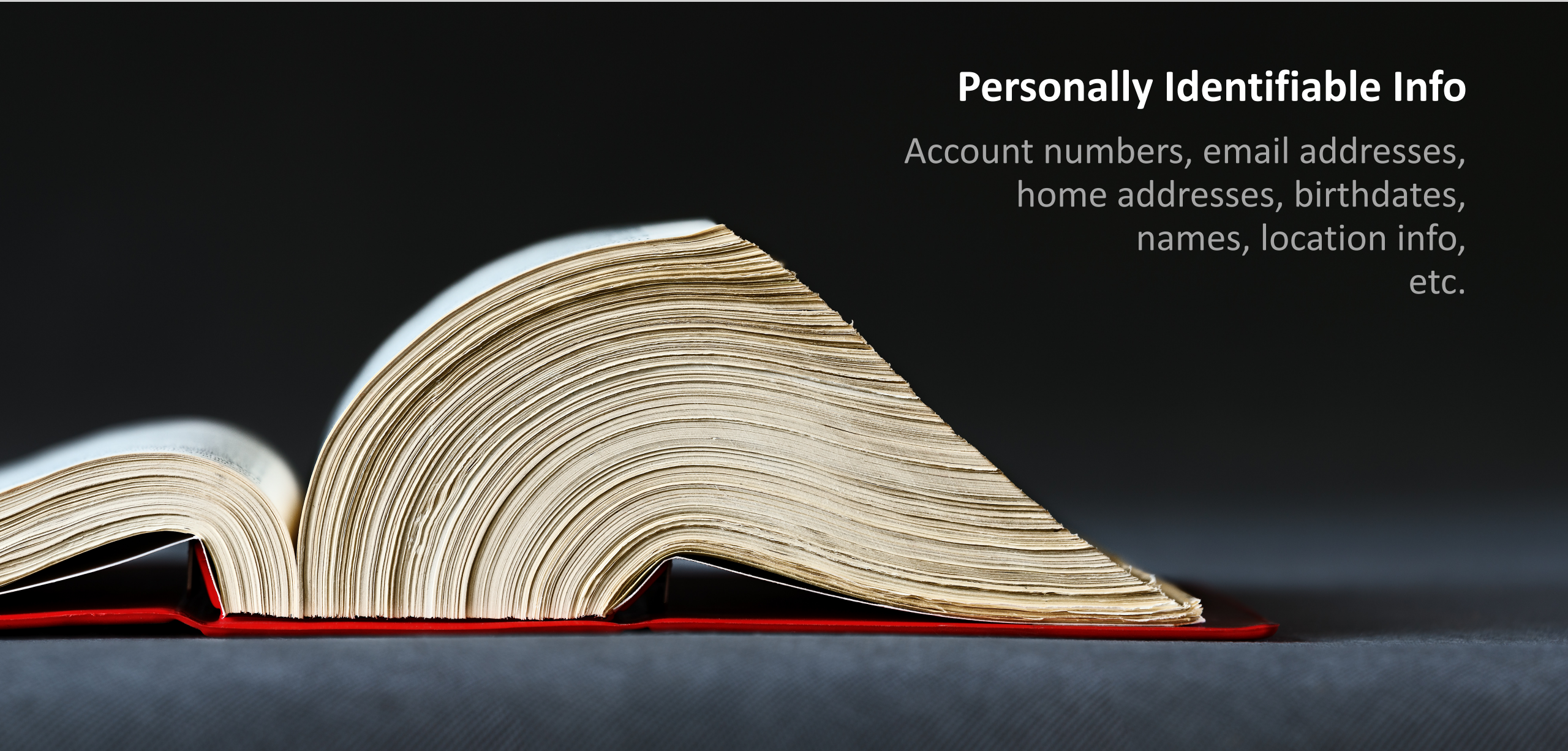
20 years in threat research, cryptography, software architecture, and enterprise cloud applications.

ISSA
Information Systems Security Association International

What To Expect

- Brief problem setup
- Potential solutions
  - Pseudonymization overview
  - **Encryption solutions landscape**
- Conclusion

PII is Regulated Data



Personally Identifiable Info

Account numbers, email addresses, home addresses, birthdates, names, location info, etc.

PII is Regulated Data

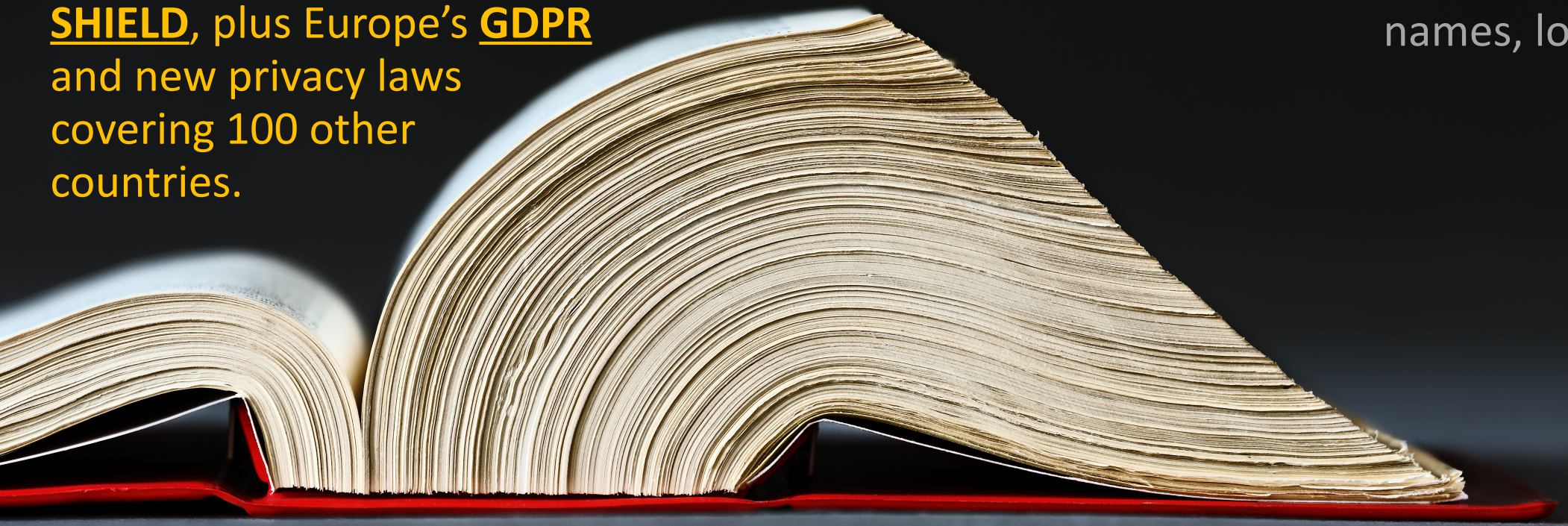
ISSA
Information Systems Security Association International

New Laws

19 U.S. State Laws including California's **CCPA** and NY's **SHIELD**, plus Europe's **GDPR** and new privacy laws covering 100 other countries.

Personally Identifiable Info

Account numbers, email addresses, home addresses, birthdates, names, location info, etc.



PII is Regulated Data

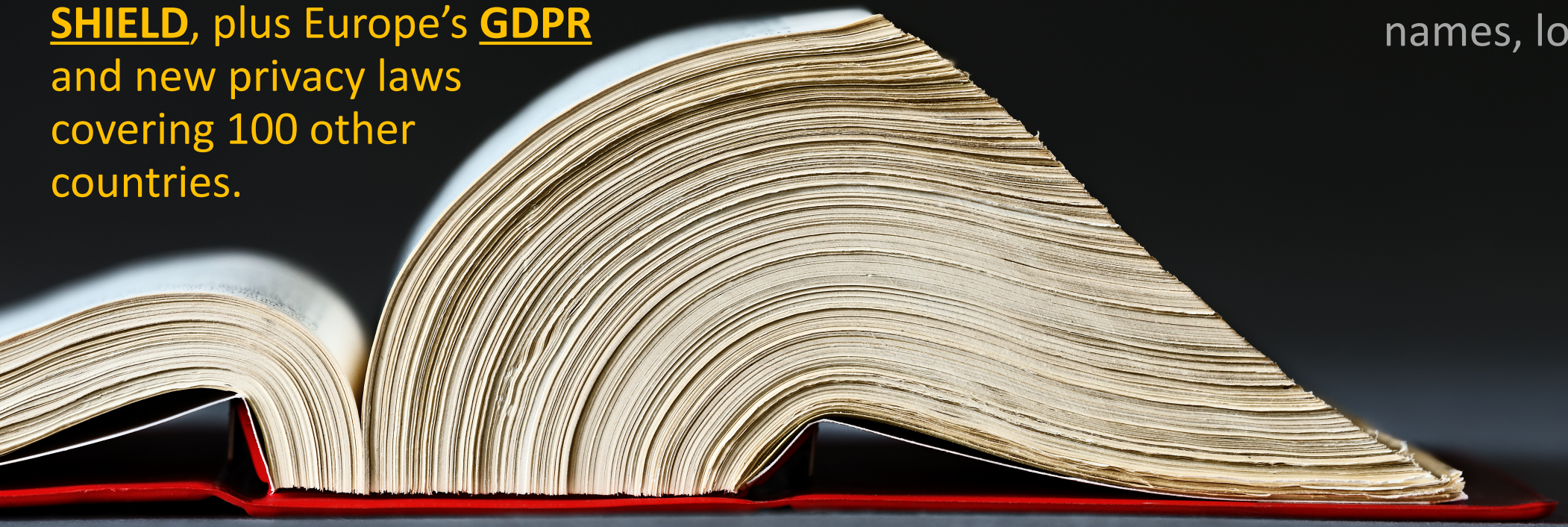
ISSA
Information Systems Security Association International

New Laws

19 U.S. State Laws including California's **CCPA** and NY's **SHIELD**, plus Europe's **GDPR** and new privacy laws covering 100 other countries.

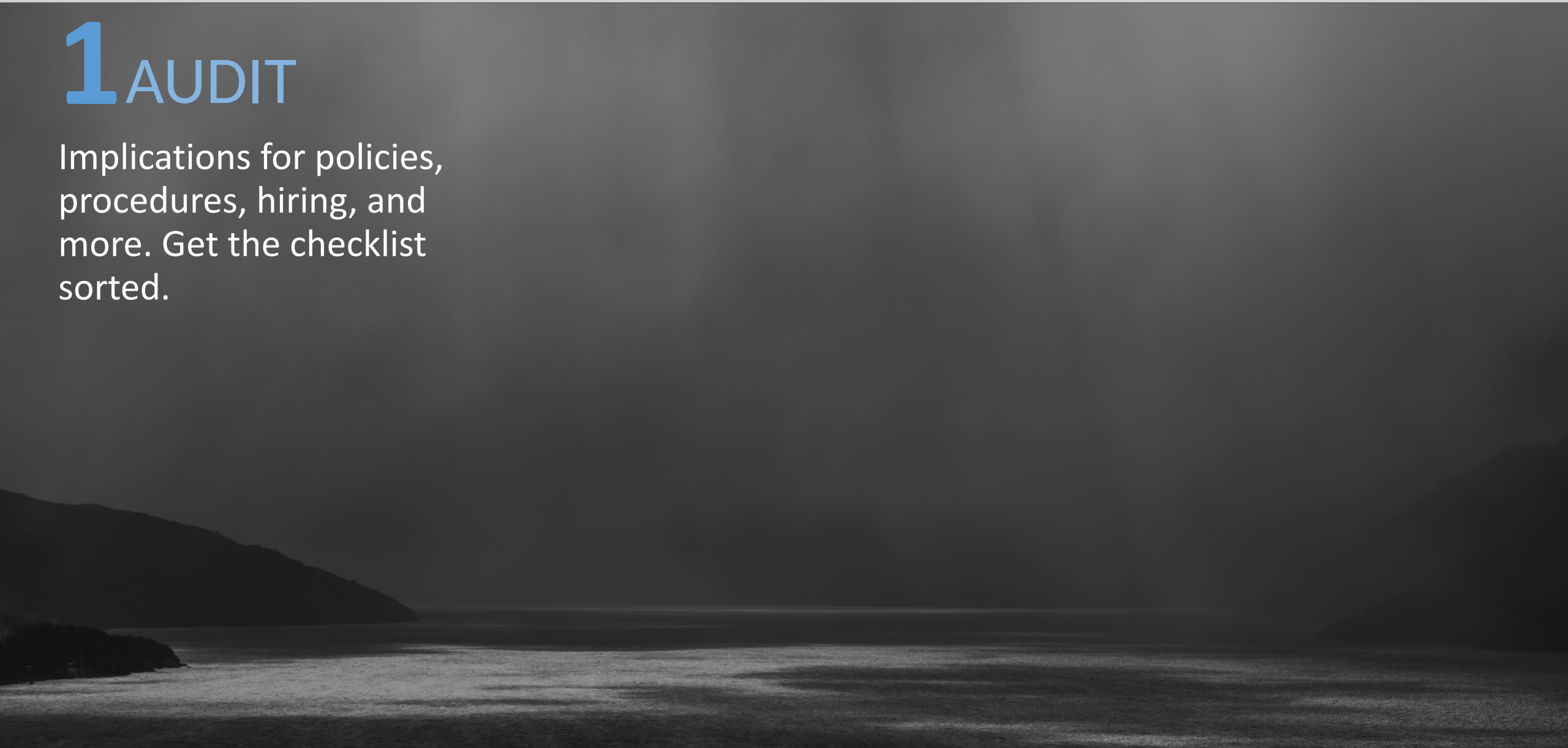
Personally Identifiable Info

Account numbers, email addresses, home addresses, birthdates, names, location info, etc.



But you know this. NOW WHAT?

Remediating the Data



1 AUDIT

Implications for policies, procedures, hiring, and more. Get the checklist sorted.

Remediating the Data

ISSA
Information Systems Security Association International

1 AUDIT

Implications for policies, procedures, hiring, and more. Get the checklist sorted.

2 IDENTIFY

Data governance time: identify your regulated data, where it is, who can access it, how long you keep it, etc.

Remediating the Data

ISSA
Information Systems Security Association International

1 AUDIT

Implications for policies, procedures, hiring, and more. Get the checklist sorted.

2 IDENTIFY

Data governance time: identify your regulated data, where it is, who can access it, how long you keep it, etc.

3 REMEDIATE

Any data you hold is a **potential liability**.

If you're hacked, if an employee is overly curious, or if a litigious customer is looking for a pay day, **this data is problematic**.

GDPR Articles 25 & 32

Article 25: Data protection by design and by default

1. …implement appropriate technical and organisational measures, **such as pseudonymisation**, which are designed to implement **data-protection** principles, such as data minimisation, in an effective manner and to integrate the necessary **safeguards**…

GDPR Articles 25 & 32

Article 32: Security of processing

1. …implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    A. the **pseudonymisation and encryption** of personal data;
    B. the ability to ensure the **ongoing confidentiality, integrity**, …
    C. …

GDPR Requirements

GDPR Penalties: Up to **4%** of global revenue or **€20m**, whichever is greater.

- Whatever measures you take must work.
  - **… or else penalties.**

CCPA Penalties

- Fines for privacy breaches.
- **Private right of action** for breached data.
  - No need to show damages.
  - **$100-$750** per California resident impacted.

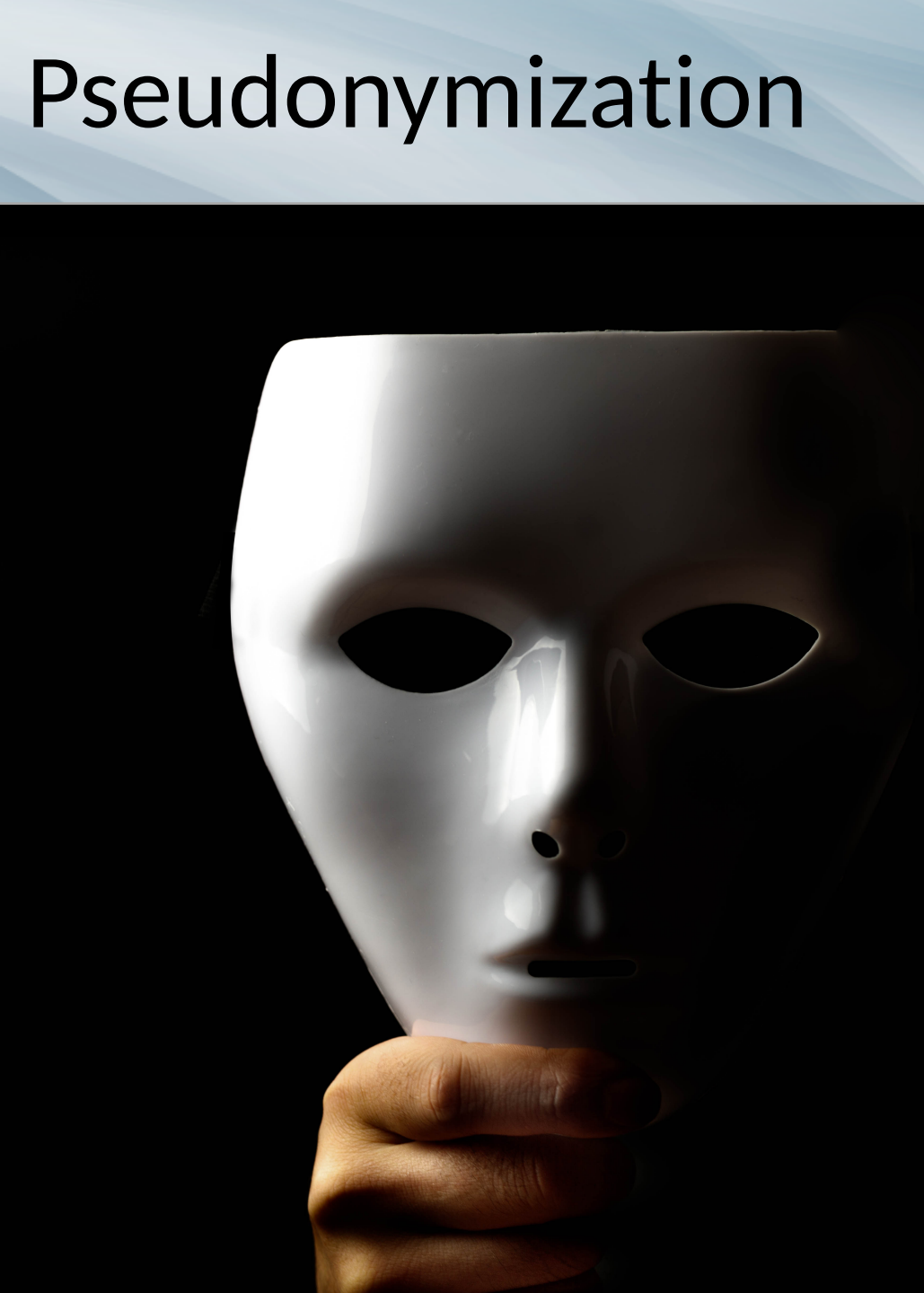
If **Equifax** breach was today, would have cost them an **additional $1.7b - $13b** on top of $1.4b.

Solution Landscape

Minimization

Technical Measures: Pseudonymization

Pseudonymization



- Simple concept: replace values with artificial identifiers (pseudonyms).
- Example techniques:
  - Tokenizing: “Patrick Walsh” ➔ “ID123”
  - Masking: “1-603-427-9200” ➔ “*-***-***-9200”
  - Generalizing: “July 1, 1995” ➔ “1990’s”

Pseudonymization

Tokenized

	Name	Account Balance
1	John Smith	$5,000
2	Pam Jones	$123,000
3	Jeff Bezos	$126,000,000,000
4	Alice Walker	$1,201,532

	Name	Account Balance
1	a1	$5,000
2	b3	$123,000
3	c8	$126,000,000,000
4	d2	$1,201,532

Pseudonymization

Tokenized

	Name	Account Balance
1	John Smith	$5,000
2	Pam Jones	$123,000
3	Jeff Bezos	$126,000,000,000
4	Alice Walker	$1,201,532

	Name	Account Balance
1	a1	$5,000
2	b3	$123,000
3	c8	$126,000,000,000
4	d2	$1,201,532

Pseudonymization

Tokenized + Generalized

	Name	Account Balance
1	John Smith	$5,000
2	Pam Jones	$123,000
3	Jeff Bezos	$126,000,000,000
4	Alice Walker	$1,201,532

	Name	Account Balance
1	a1	$0 - $150,000
2	b3	$0 - $150,000
3	c8	$1,000,000 - ∞
4	d2	$1,000,000 - ∞

Pseudonymization Problems

Pseudonymization Problems

Technical Measures: Encryption

Encryption Landscape Pieces

1. State of the industry
2. Encryption key management patterns
3. Cloud app encryption options
4. Crypto bingo
    a. Advanced options for protecting data
    b. Advanced options for using encrypted data

Things We Hear

ISSA
Information Systems Security Association International

“We already encrypt the data at rest and in transit.”

Transparent Disk Encryption

Data at rest encryption

Likely means **transparent** disk or database encryption.

Protects against a stolen hard drive.

Offers no barrier to access on a running system.

In Transit Encryption

In transit encryption

Probably means you use HTTPS.

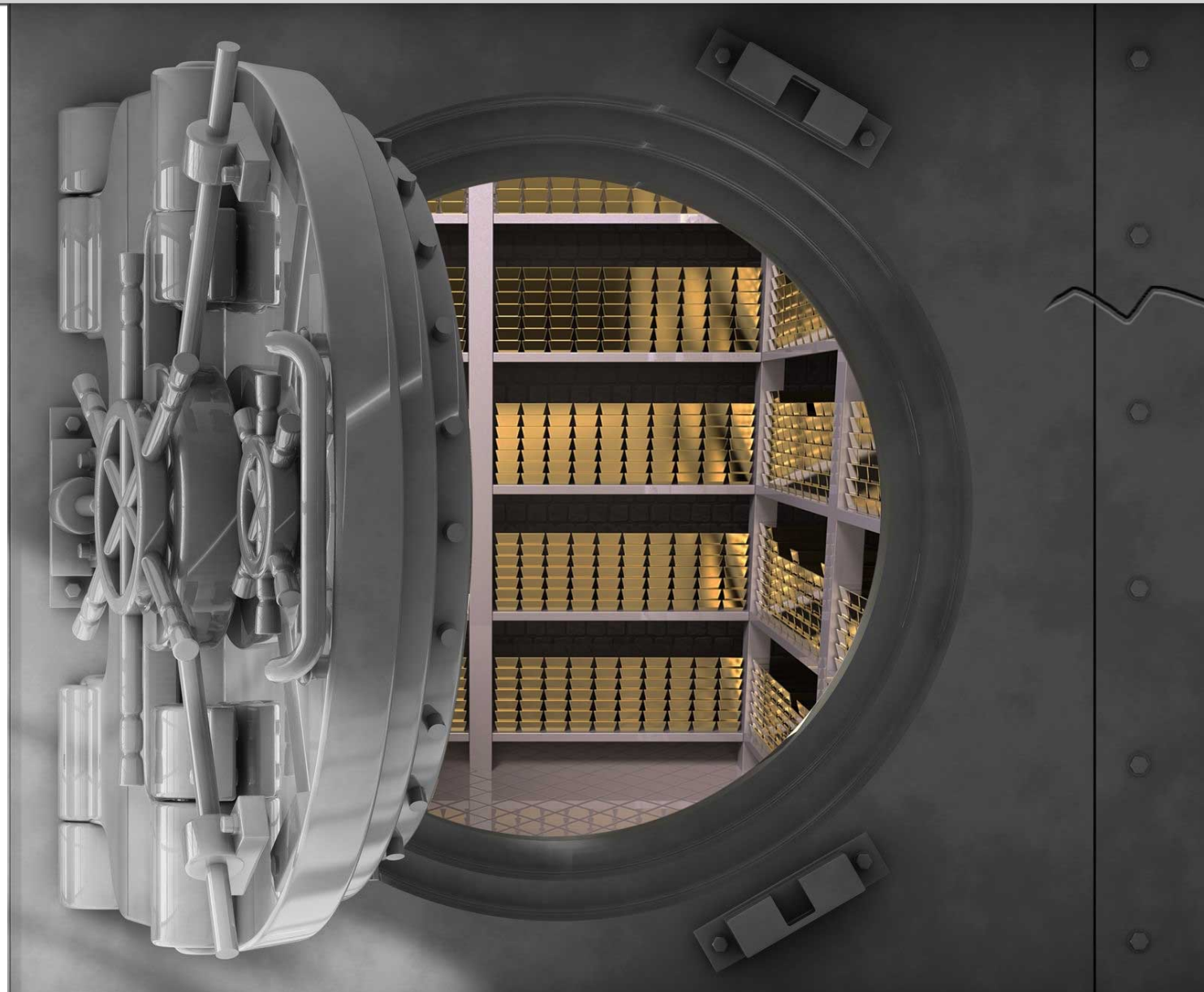
Prevents passive snooping and gives some assurance as to who you're talking to.

Offers no barrier to access of data.

At Rest and In-Transit Encryption

Transparent to hackers, too.

Not an adequate technical measure to protect data.

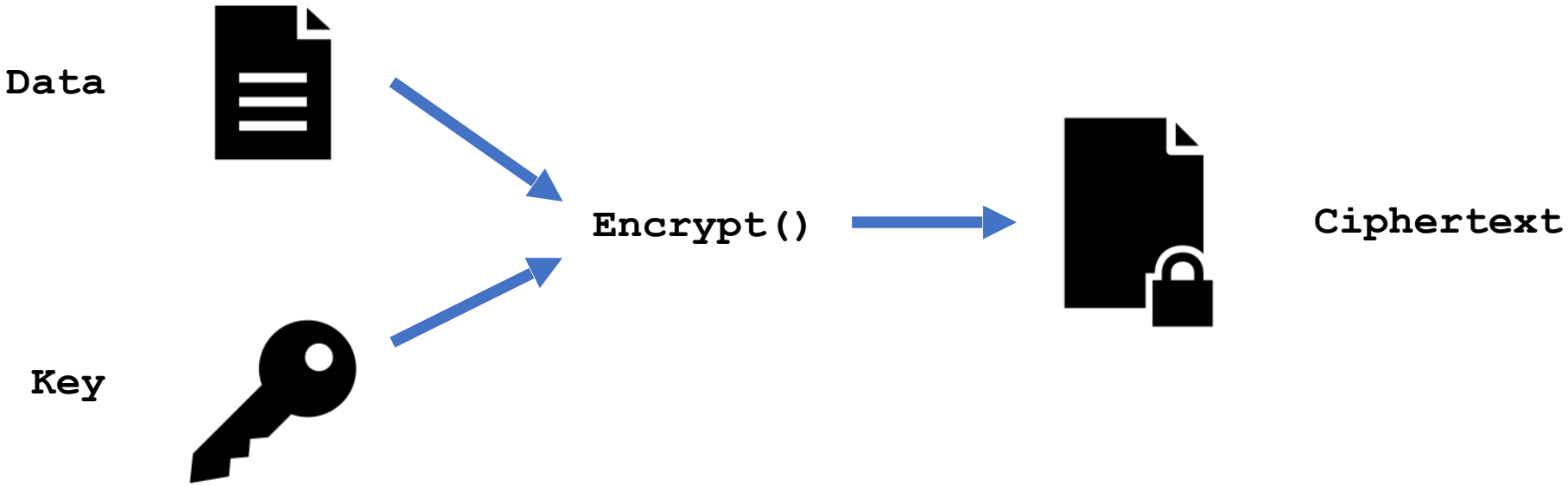


Opaque Encryption Solutions

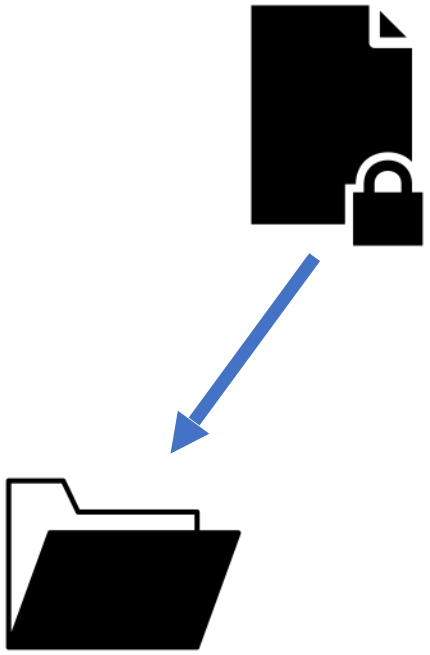
Non-transparent encryption protects the data even from someone inside your network.

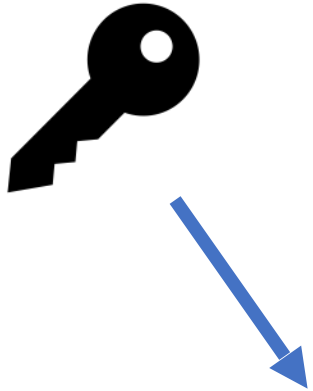
This combines access controls with encryption to protect the data, which is what you want.

Conceptually Easy



Deceptively Difficult

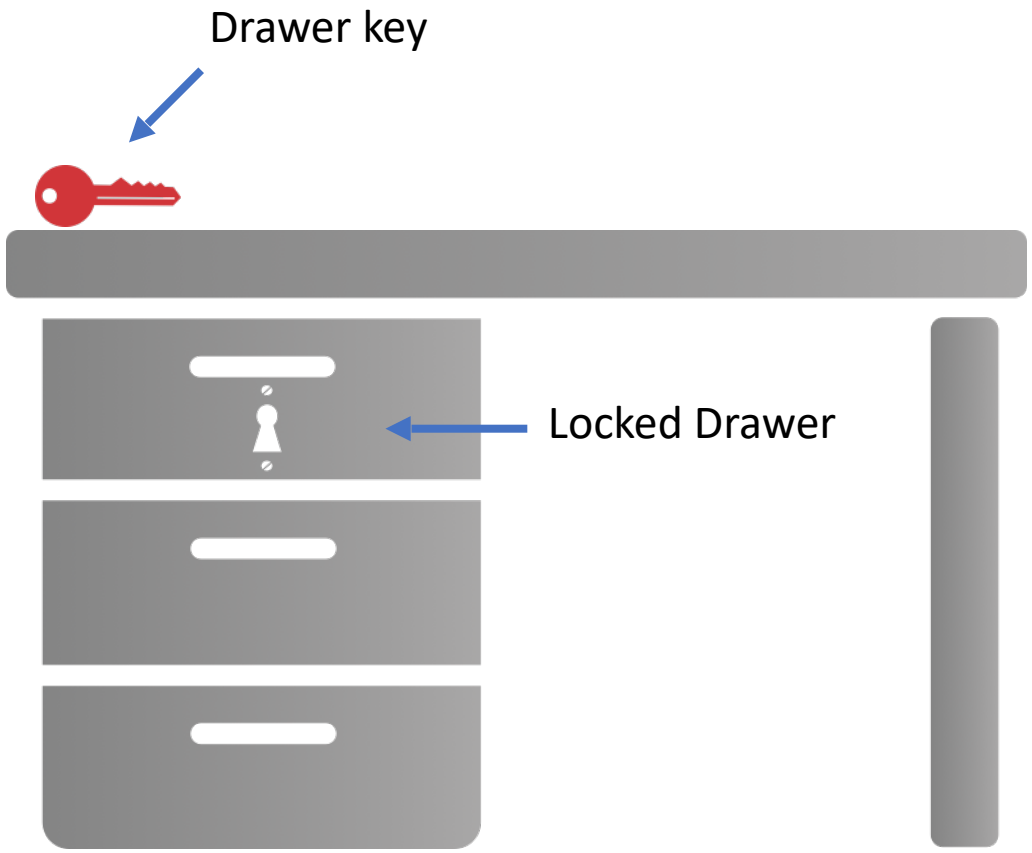




?

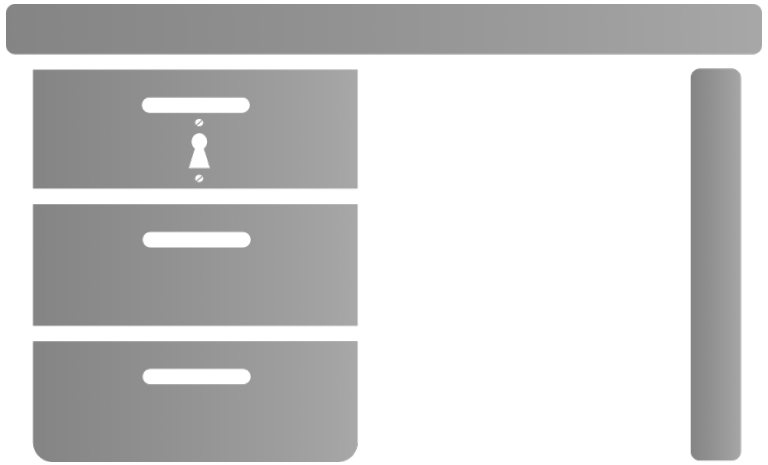
Where do you put the key?

Need Separation



What's wrong with this picture?

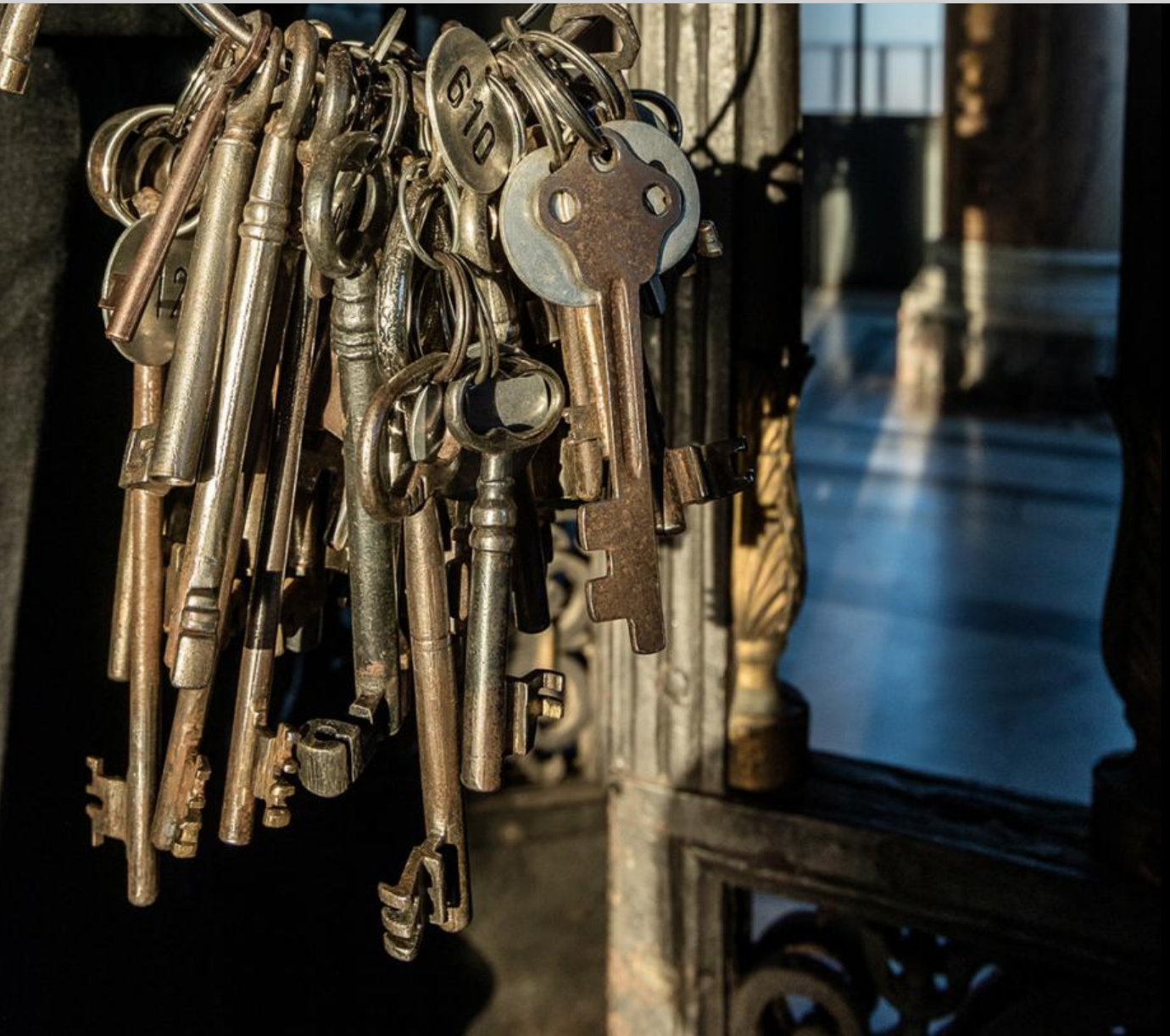
Need Separation



- **Better**:
  - Key is in a key cabinet in another room, which is locked.
- **Much better**:
  - Key is carried in desk owner's pocket.

Technical Measures: Key Management Patterns

Key Management Servers



- Often backed by a Hardware Security Module (HSM) where the master key never leaves the HSM.
- Sometimes requires a password or other root of trust to initialize.
- Most common and trusted pattern for server-side encryption.

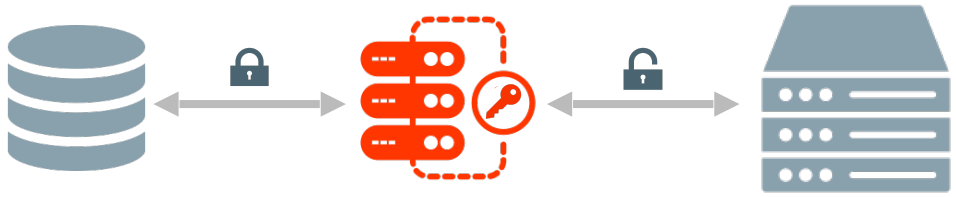
Examples:
Amazon KMS, Thales Ciphertrust

Key Jars

Variant:
Data is encrypted with a variety of keys. One KMS holds and manages access to these keys and hands out keys to those with permissions.

Examples:
Ionic, Virtru

Encrypting Proxy



- The proxy has the key
- The database holds encrypted data
- If you query through the proxy, the data is transparently encrypted or decrypted.
- Small degree of separation, which is useful in some cases.
- Examples: Baffle, IronCore

Per-person/Per-device Keys

Cryptographic access controls where every device that accesses data has their own public/private key pair.

Technical Measures:
Cloud App Encryption Features

Patterns in the Wild

Everyone offers “in-transit and at-rest” encryption. Here are a few who do better.

Customer Managed Keys
(and customer held keys)

End-to-end Encryption
(zero trust)

Patterns in the Wild

(CMK)

Customer Managed Keys
(and customer held keys)

(E2EE)

End-to-end Encryption
(zero trust)

These are both opaque encryption schemes that give the cloud app customer control of their data.

Supply Chain Attack Protection for Cloud

ISSA
Information Systems Security Association International

solarwinds

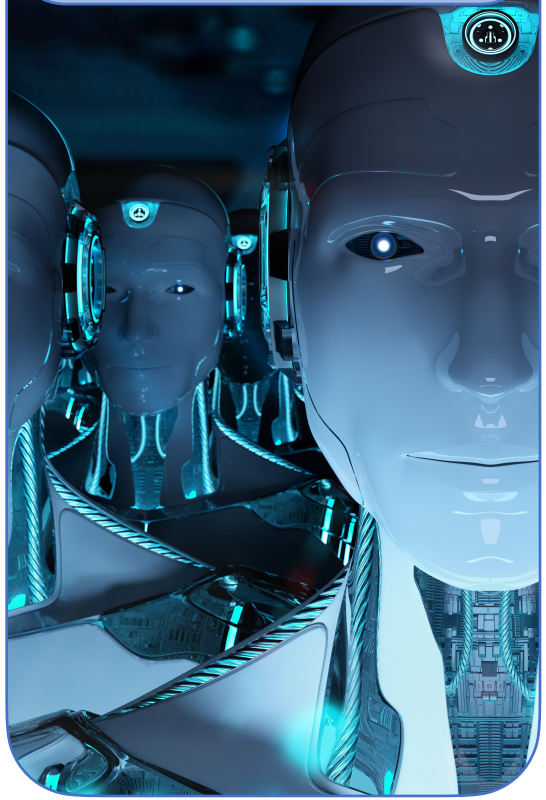
Technical Measures: Advanced Encryption

Gotta Collect ‘Em All?

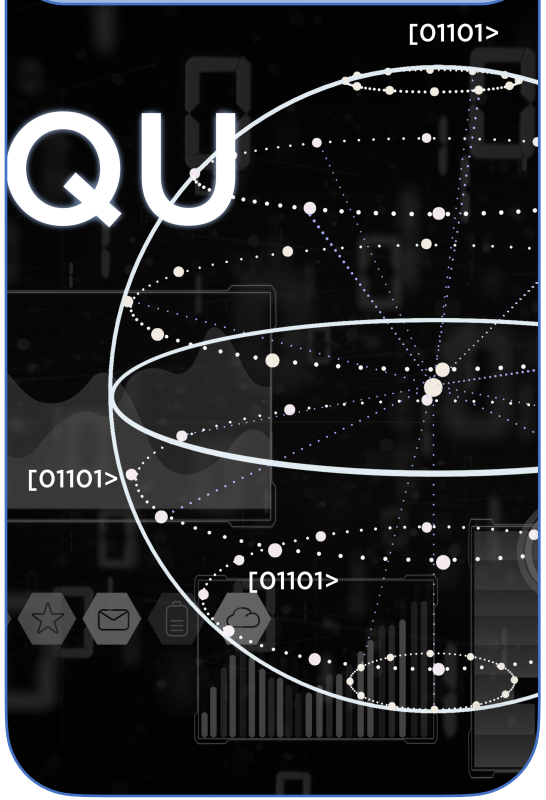
ISSA
Information Systems Security Association International

Proxy Re-encryption

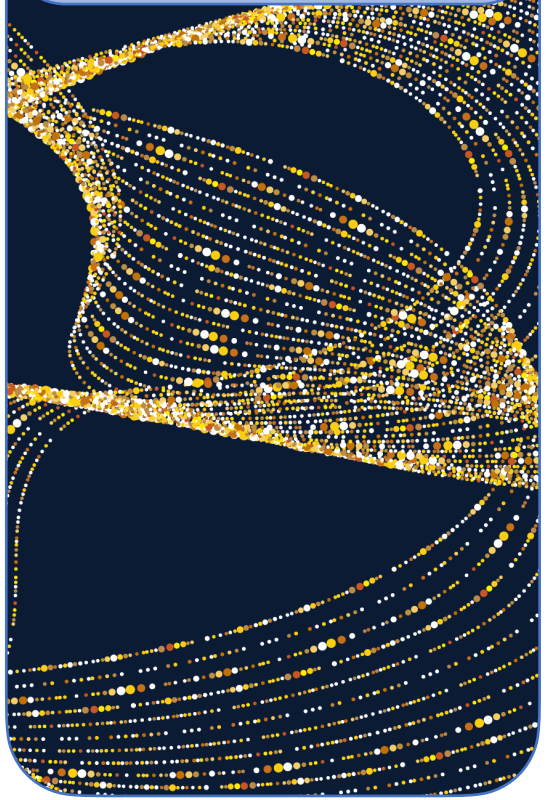
Multi-party Computation



Post-Quantum



Data Splitting



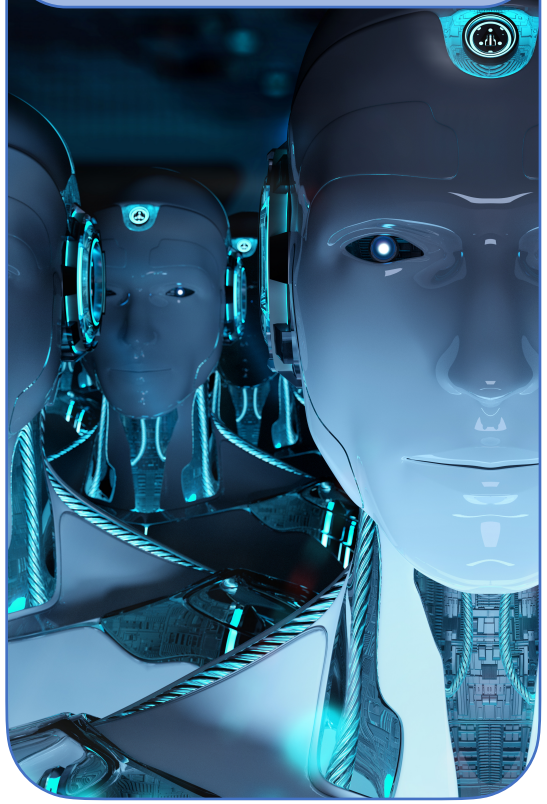
Gotta Collect ‘Em All?

ISSA
Information Systems Security Association International

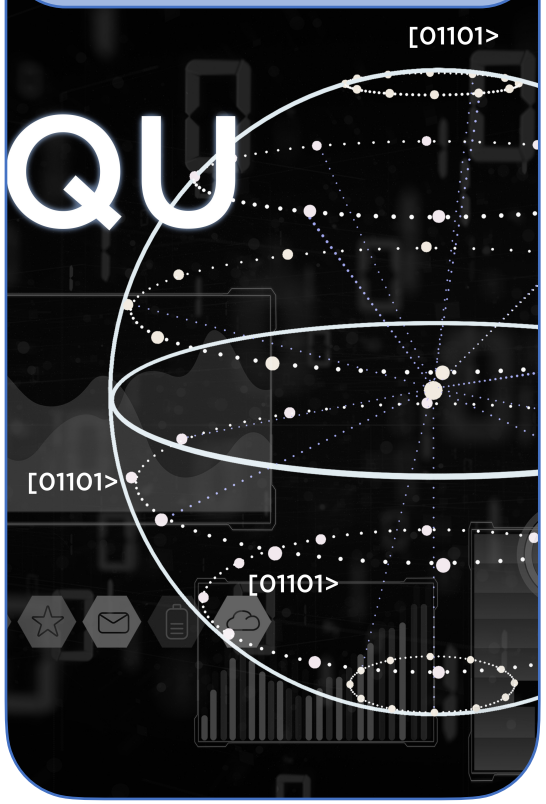
Proxy Re-encryption

- aka Transform Crypto
- NOT an encrypting proxy
- Delegate decryption rights
- Zero-trust
- Examples: IronCore, NuCypher

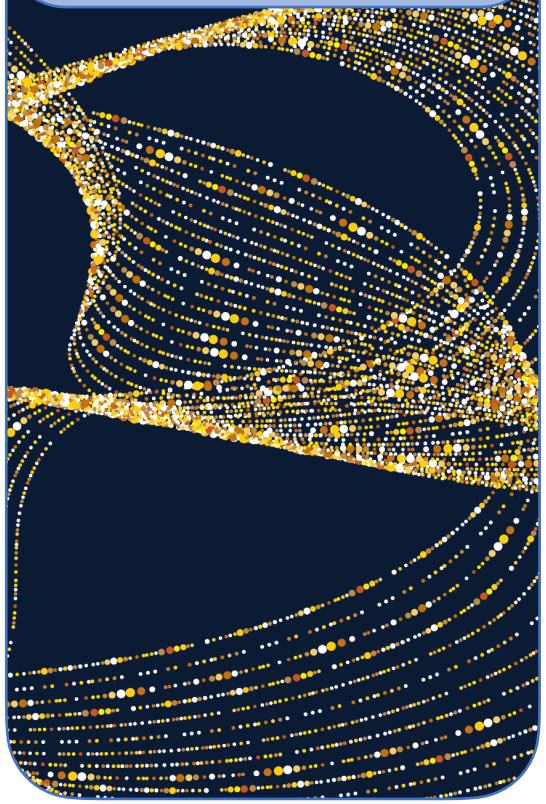
Multi-party Computation



Post-Quantum



Data Splitting



Gotta Collect ‘Em All?

ISSA
Information Systems Security Association International

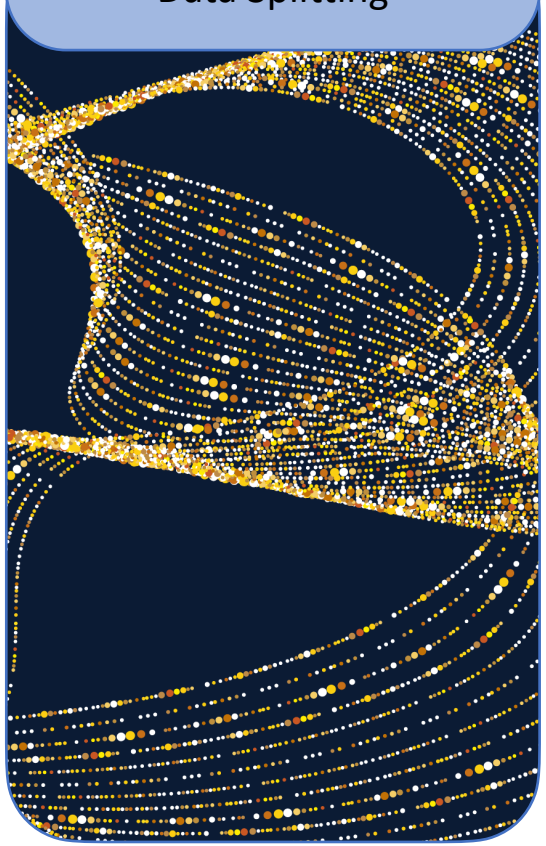
Proxy Re-encryption

Multi-party Computation

- Execute a predetermined function over data held by multiple parties without sharing the data.
- Garbled circuit
- Different from key splitting where keys have to come together.
- Multiple servers or entities required to process.
- Example: Unbound

Post-Quantum

Data Splitting

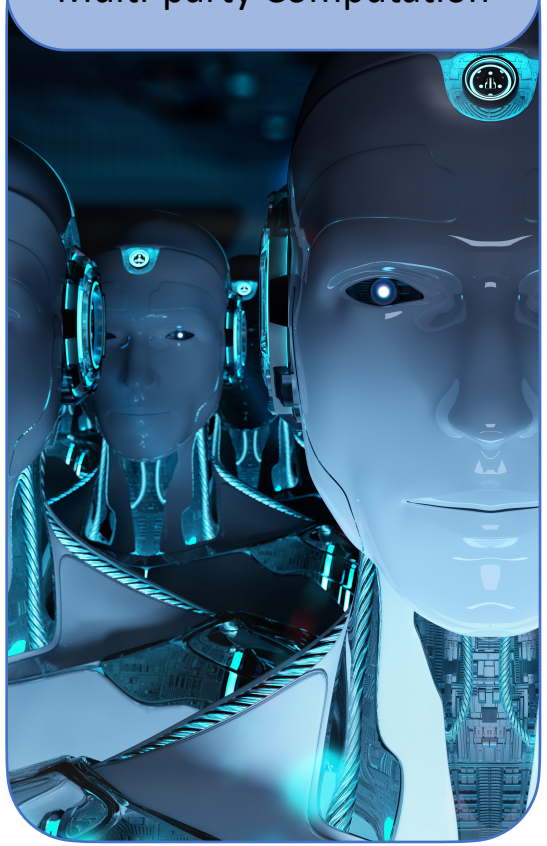


Gotta Collect ‘Em All?

ISSA
Information Systems Security Association International

Proxy Re-encryption

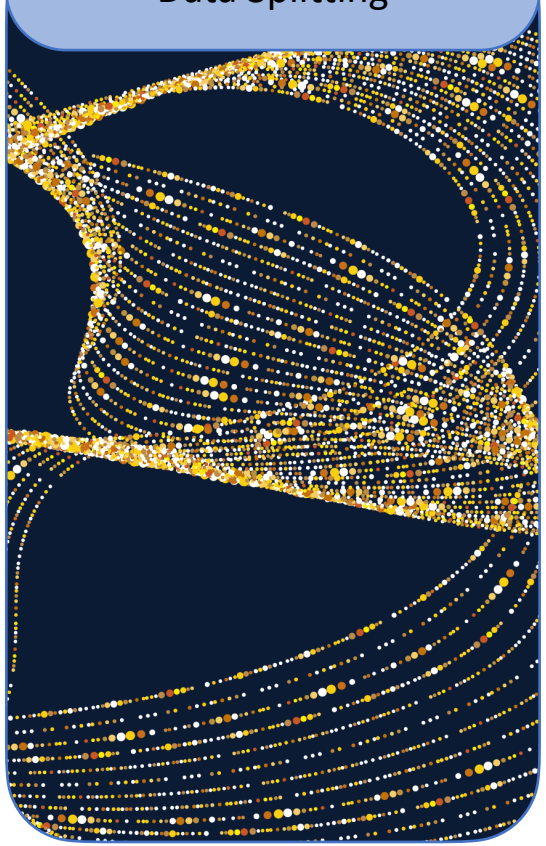
Multi-party Computation



Post-Quantum

- Resistant to quantum computing attacks
- Standard AES fits this bill to some extent (with bigger keys)
- RSA and ECC are busted by Quantum computers
- Still largely theoretical and very experimental options.

Data Splitting

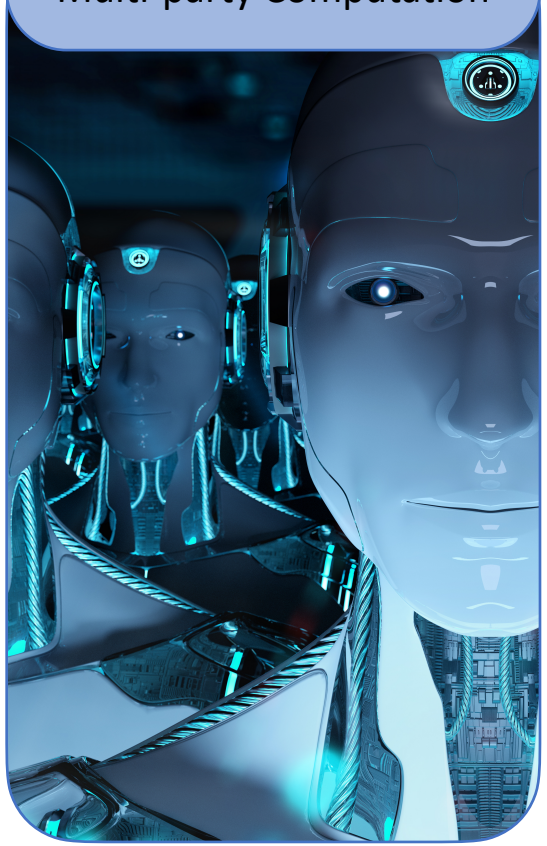


Gotta Collect ‘Em All?

ISSA
Information Systems Security Association International

Proxy Re-encryption

Multi-party Computation



Post-Quantum

Data Splitting

- Sounds similar to MPC, but it isn’t. Not cryptographic.
- And in commercial installs we’ve seen, frequently the data is split across servers in a single zone of vulnerability.
- Buyer beware.

Technical Measures: Making Encrypted Data Usable

Secure Computation

ISSA
Information Systems Security Association International

Homomorphic Encryption

Zero-knowledge Proof

Secure Enclave

Encrypted Search

Homomorphic Encryption

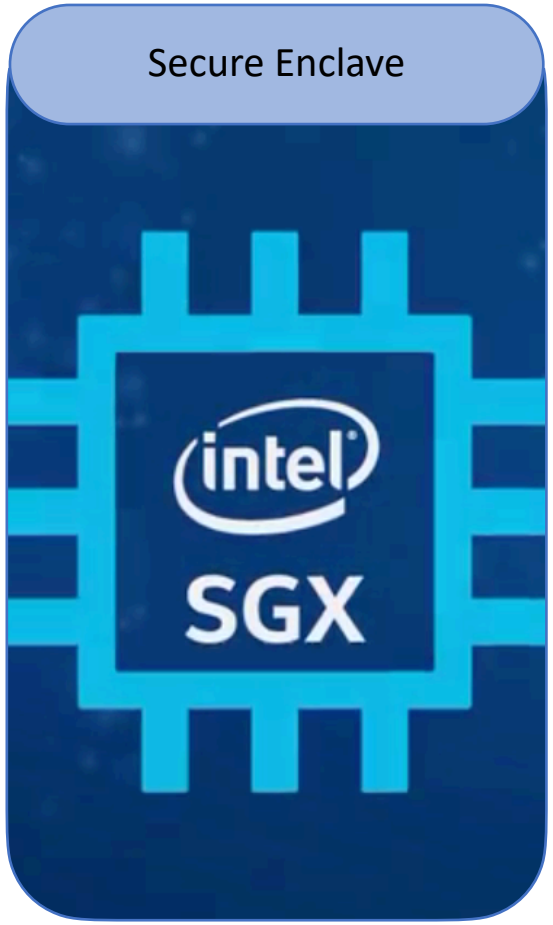
- Operate on data (addition, multiplication, etc.) without decrypting the inputs. Output is decrypted to obtain the result. Operations are arbitrary.
- **Partial** vs. **Full**
  - Partially homomorphic supports limited operations (like just addition, for example)
  - Fully homomorphic allows arbitrary computation. Highly desirable, but very slow.
- In the market, these terms are being used indiscriminately and without regard for truth.
- *Still mostly in research projects.*
- Examples: IBM, Microsoft

Zero Knowledge Proof

- Allows you to prove that you know something without directly sharing what you know.
- Variants: range proofs and set membership proofs
- Range proof:
  - Verify age over 21, salary between $x and $y, or account balance over $x.
- Set proof:
  - Validate KYC info including location and validity of zip code.
- *Still mostly in blockchain and research projects, but is practical to use now.*
- Examples: Z-Cash, Journey, ING

Software Guard Extensions (SGX)

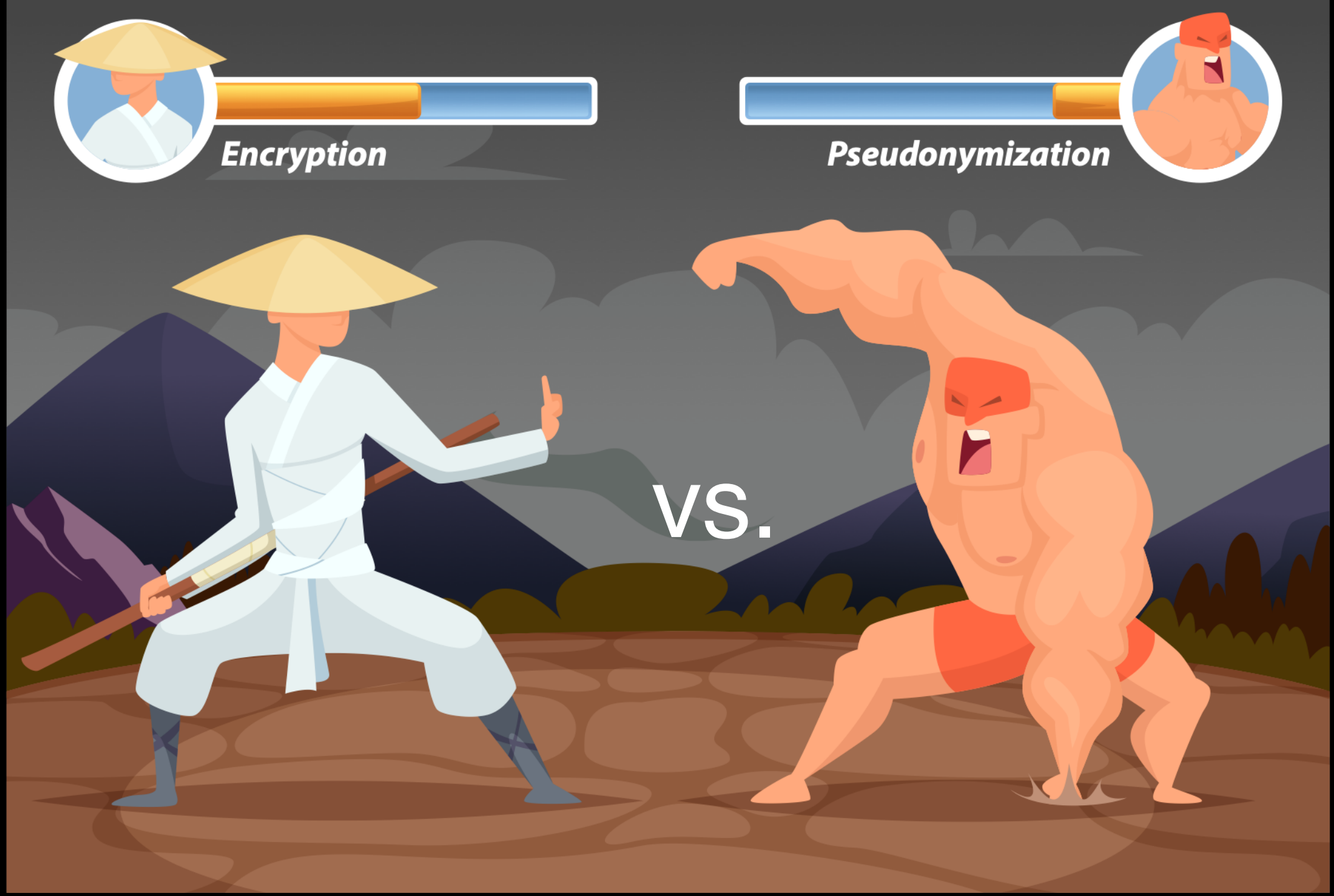
- Hardened memory and CPU sandbox
- Allows decryption with protected keys, full processing, and resists other processes gaining access to keys or decrypted data.
- Great option for some use cases.
- Lots of attacks against current generation.
- Example: Intel, Fortanix



Encrypted Search

- Old encrypted search
  - 2010: Google allows https for searches
  - 2013: Google requires https for searches
    - This isn’t encrypted search.
- New encrypted search
  - Search on encrypted data
  - Google won’t be doing this.
- Search server doesn’t learn (much) about the data it holds.
- Example: MongoDB, Cossack Labs, IronCore (2021)

Conclusion


Encryption
Pseudonymization
VS.

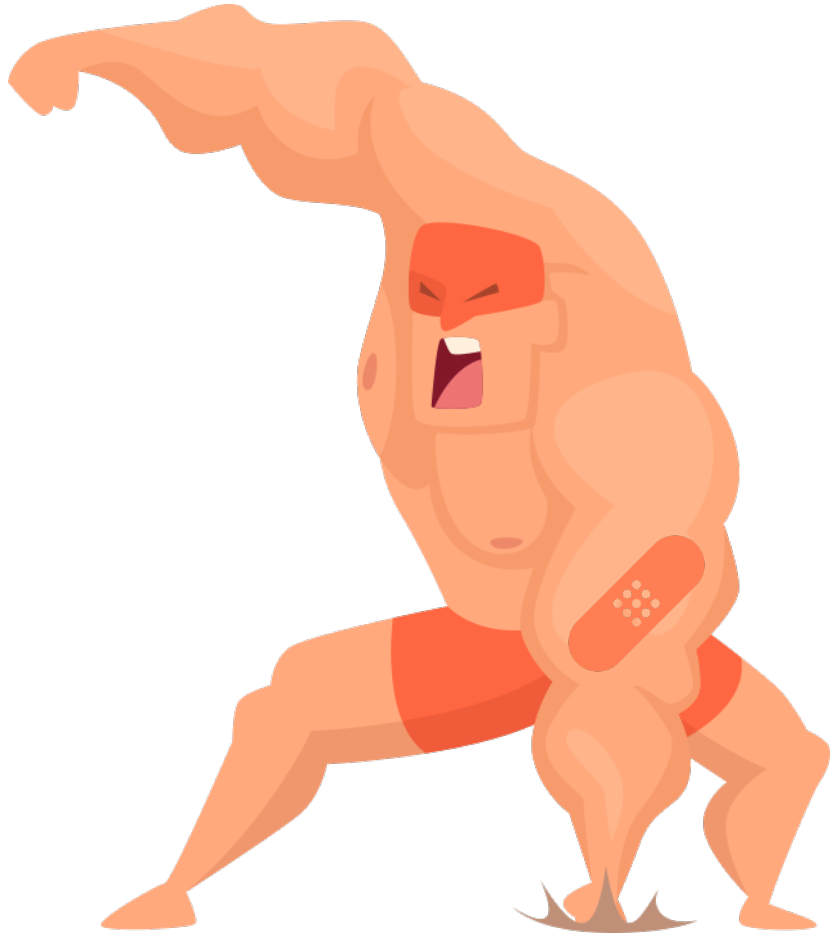
Pseudonymization

Pros:

- Straight forward to understand
- Can present different views of the data to different classes of users
- Specifically called out by GDPR

Cons:

- Usually the toxic data is still being held and this is just a “view.”
- It's a data bandaid.



Opaque Encryption

Pros:

- Protects the raw data.
- A breach of a server doesn't breach the data.
- Powerful options.

Cons:

- Can be more difficult to use the data.
- Advanced tech is slow to go mainstream

Better Together

A combination that presents pseudonymized data to people who don’t need to know, but with the source data opaquely encrypted is the best choice.

Don’t rely on transparent encryption.

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?