PRIVACY BY DESIGN

FROM A CODERS PERSPECTIVE

A GUIDE FOR START-UPS

Photo by marksweb - Creative Commons Attribution-ShareAlike License https://www.flickr.com/photos/92166740@N00

PRIVACY

Privacy partially overlaps with security (confidentiality) but may also take the form of bodily integrity (inviolability of the physical body).

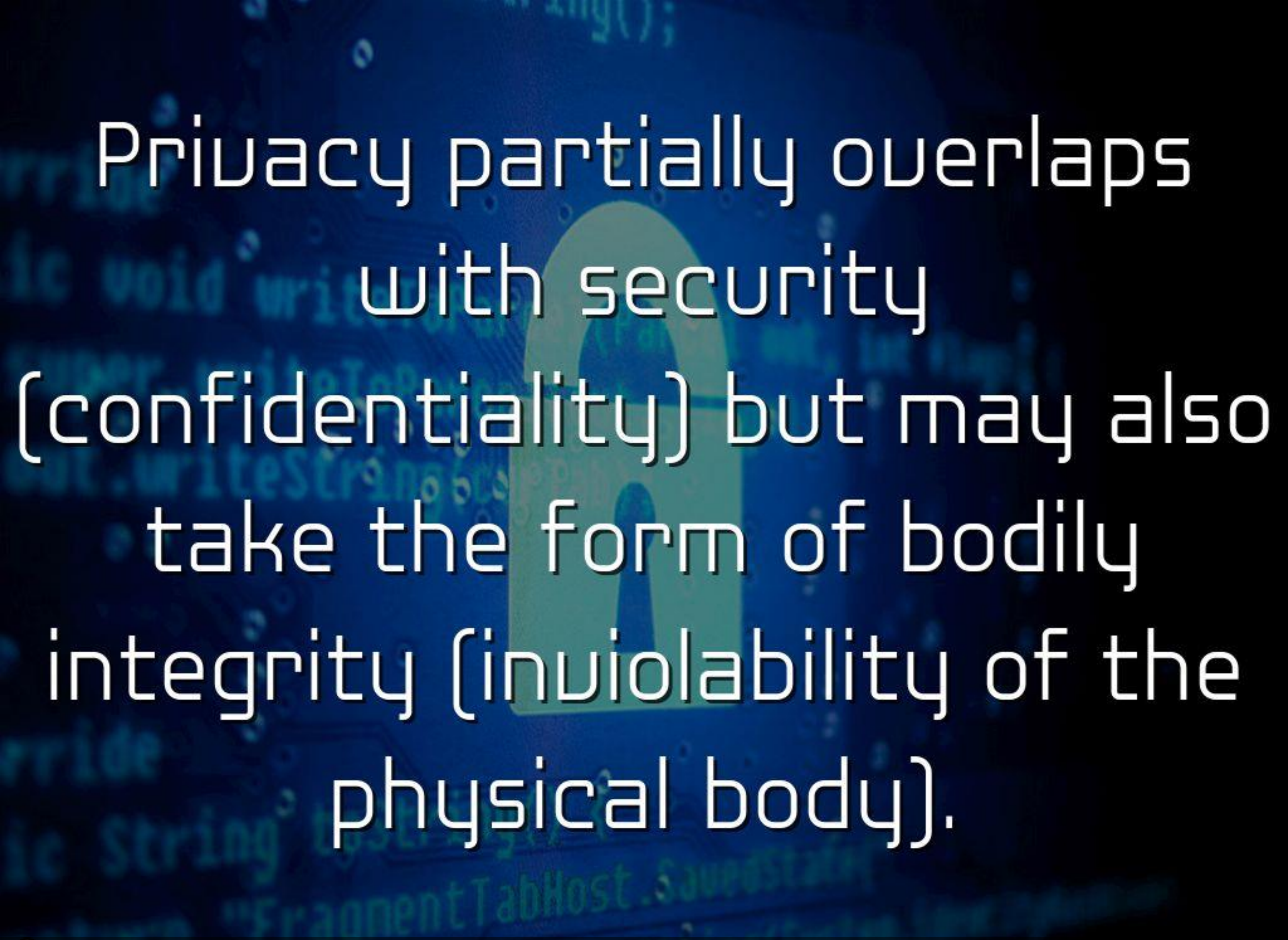


Photo by Yu. Samoilov - Creative Commons Attribution License https://www.flickr.com/photos/110751683@N02

THE GOOD
THE BAD
THE UGLY

THE BAD

AIL statistics 2015

160K

global warnings

1600

TOR hidden services

7500

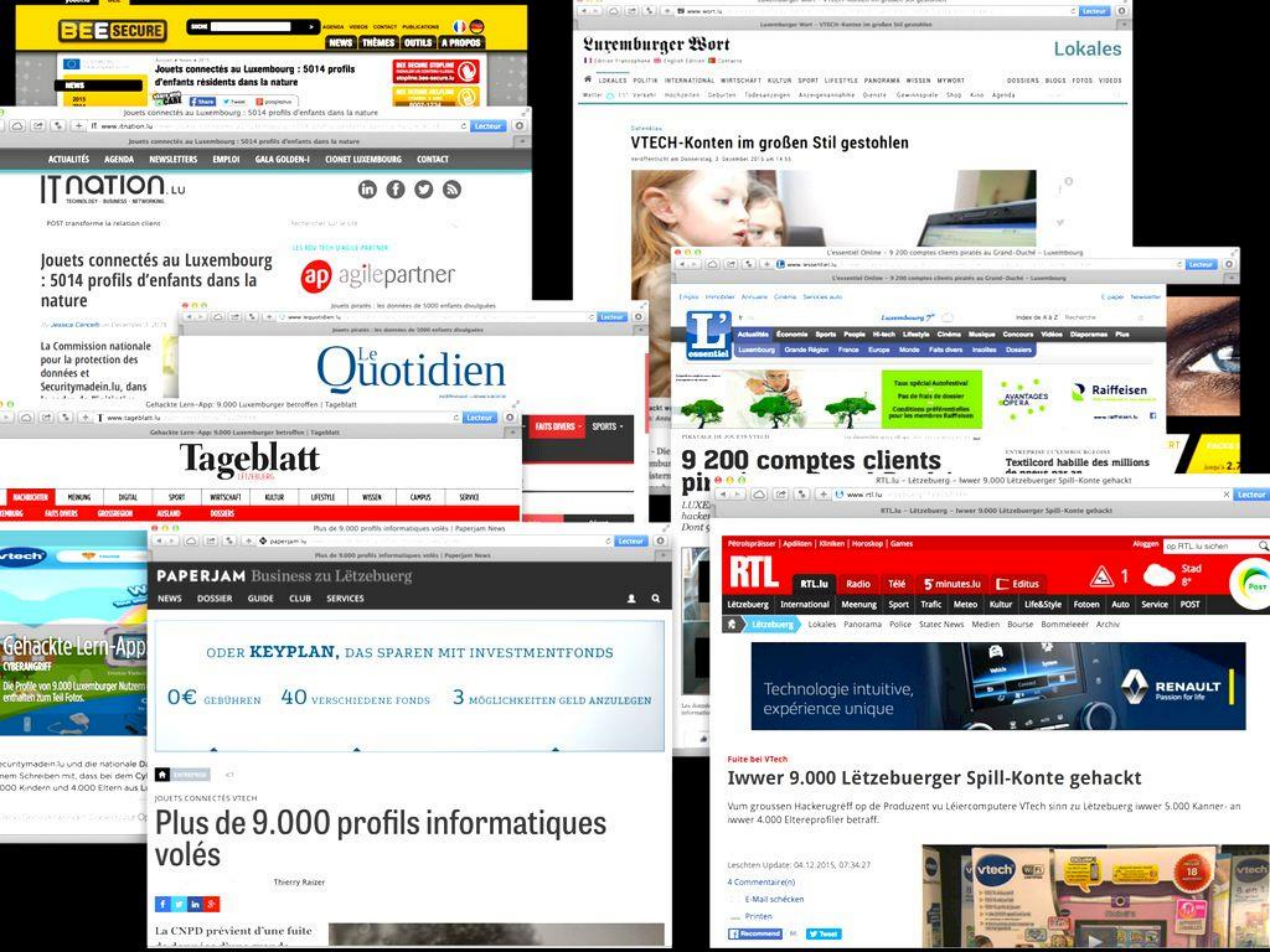
related to Luxembourg

THE GOOD

GENERAL DATA PROTECTION REGULATION

- Europe wide harmonisation
- stronger responsibility & DPIA
- administrative sanctions
- right to be forgotton
- data portability
- privacy by desgin/default

THE UGLY



Jouets connectés au Luxembourg : 5014 profils d'enfants résidents dans la nature

Jouets connectés au Luxembourg : 5014 profils d'enfants dans la nature

Jouets connectés au Luxembourg : 5014 profils d'enfants dans la nature

By Jessica Cencetti on December 3, 2015

La Commission nationale pour la protection des données et Securitymadein.lu, dans

Jouets piratés : les données de 5000 enfants divulguées

Gehackte Lern-App: 9.000 Luxemburger betroffen | Tageblatt

Gehackte Lern-App

CYBERANGRIFF

Die Profile von 9.000 Luxemburger Nutzern enthalten zum Teil Fotos.

…ecuritymadein.lu und die nationale D… …nem Schreiben mit, dass bei dem Cy… …000 Kindern und 4.000 Eltern aus L…

Luxemburger Wort – VTECH-Konten im großen Stil gestohlen

Datenklau

VTECH-Konten im großen Stil gestohlen

Veröffentlicht am Donnerstag, 3. Dezember 2015 um 14:55

L'essentiel Online – 9 200 comptes clients piratés au Grand-Duché – Luxembourg

PIRATAGE DE JOUETS VTECH

9 200 comptes clients pi…

ENTREPRISE LUXEMBOURGEOISE

Textilcord habille des millions…

Plus de 9.000 profils informatiques volés | Paperjam News

JOUETS CONNECTÉS VTECH

Plus de 9.000 profils informatiques volés

Thierry Raizer

La CNPD prévient d'une fuite…

RTL.lu – Lëtzebuerg – Iwwer 9.000 Lëtzebuerger Spill-Konte gehackt

Fuite bei VTech

Iwwer 9.000 Lëtzebuerger Spill-Konte gehackt

Vum groussen Hackerugrëff op de Produzent vu Léiercomputere VTech sinn zu Lëtzebuerg iwwer 5.000 Kanner- an iwwer 4.000 Eltereprofiler betraff.

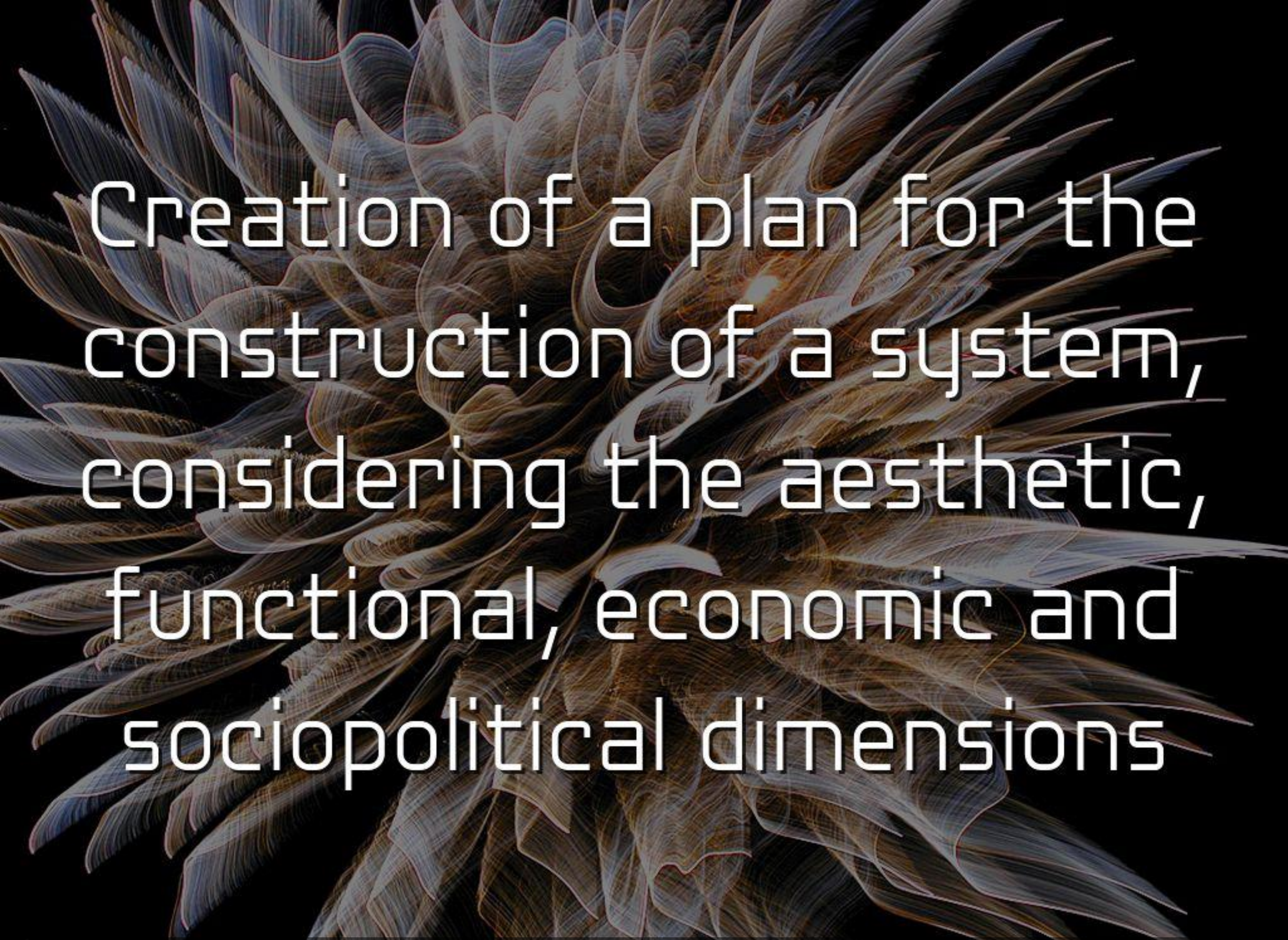
Leschten Update: 04.12.2015, 07:34:27

4 Commentaire(n)

E-Mail schécken

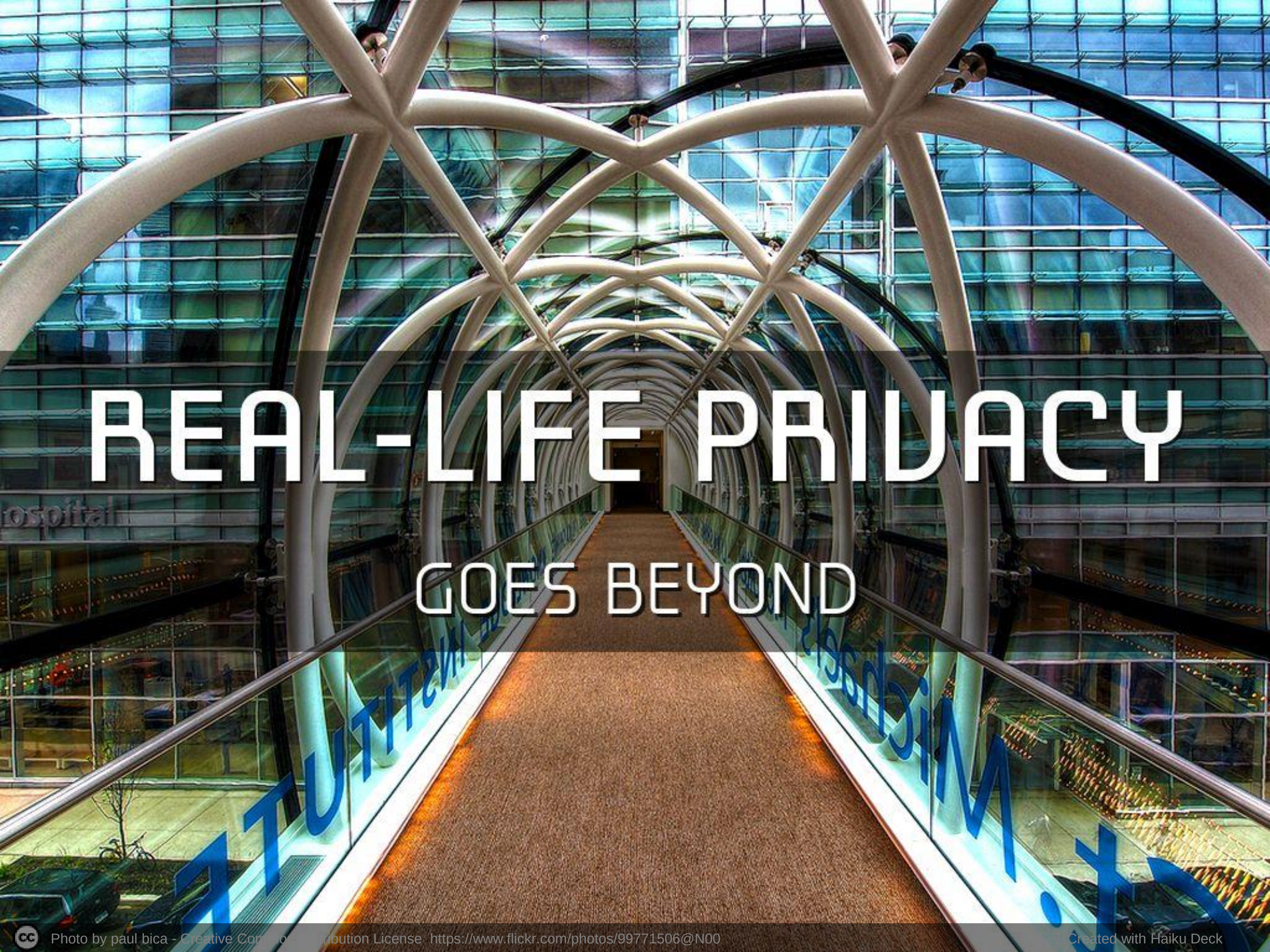
Printen

DESIGN



Creation of a plan for the construction of a system, considering the aesthetic, functional, economic and sociopolitical dimensions

Photo by George L Smyth - Creative Commons Attribution-NonCommercial-ShareAlike License https://www.flickr.com/photos/89027427@N00 Created with Haiku Deck



REAL-LIFE PRIVACY

GOES BEYOND

Photo by paul bica - Creative Commons Attribution License https://www.flickr.com/photos/99771506@N00

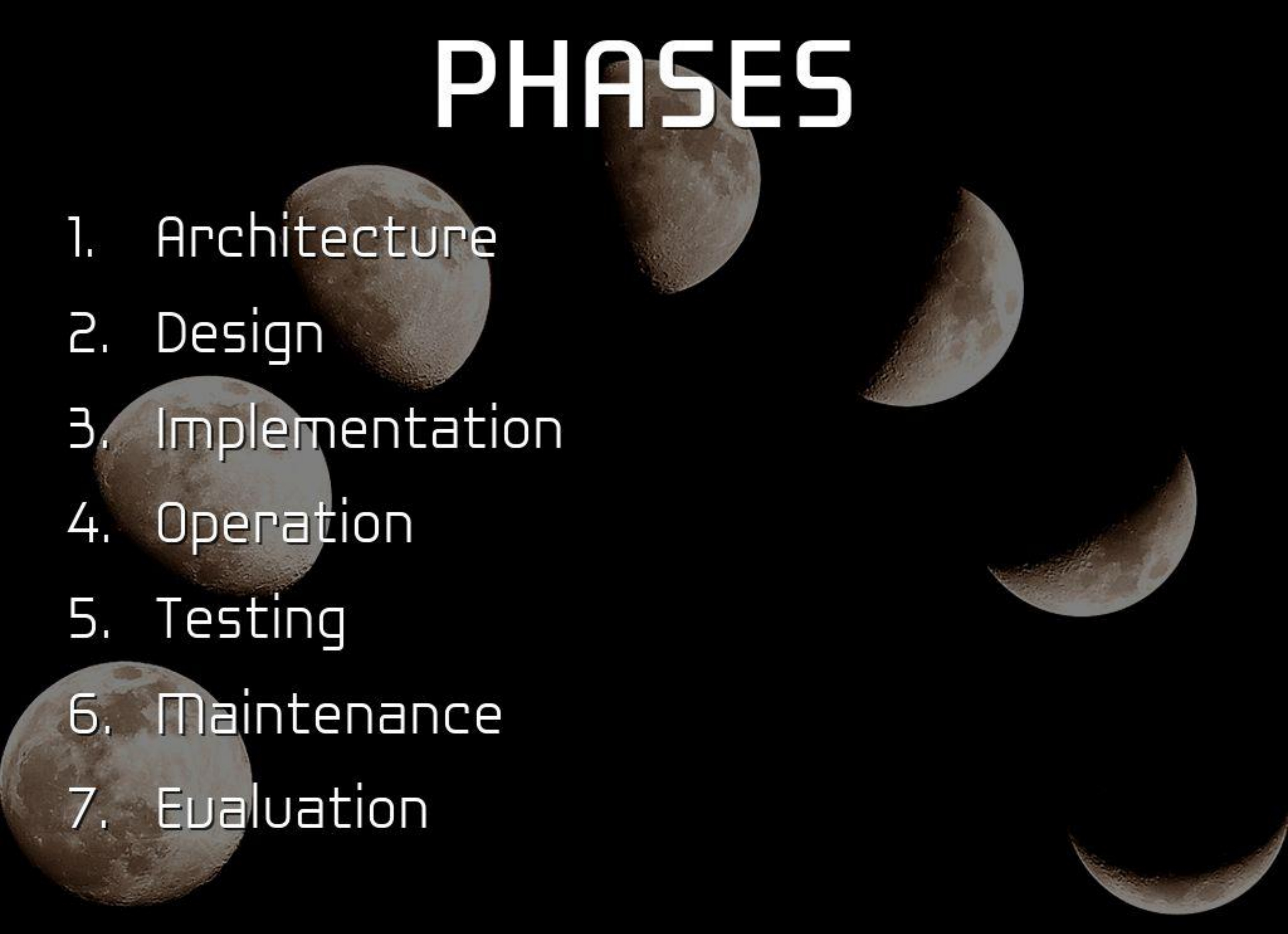
Forget about law privacy is too important to keep it to lawyers ;)

SECURE CODING

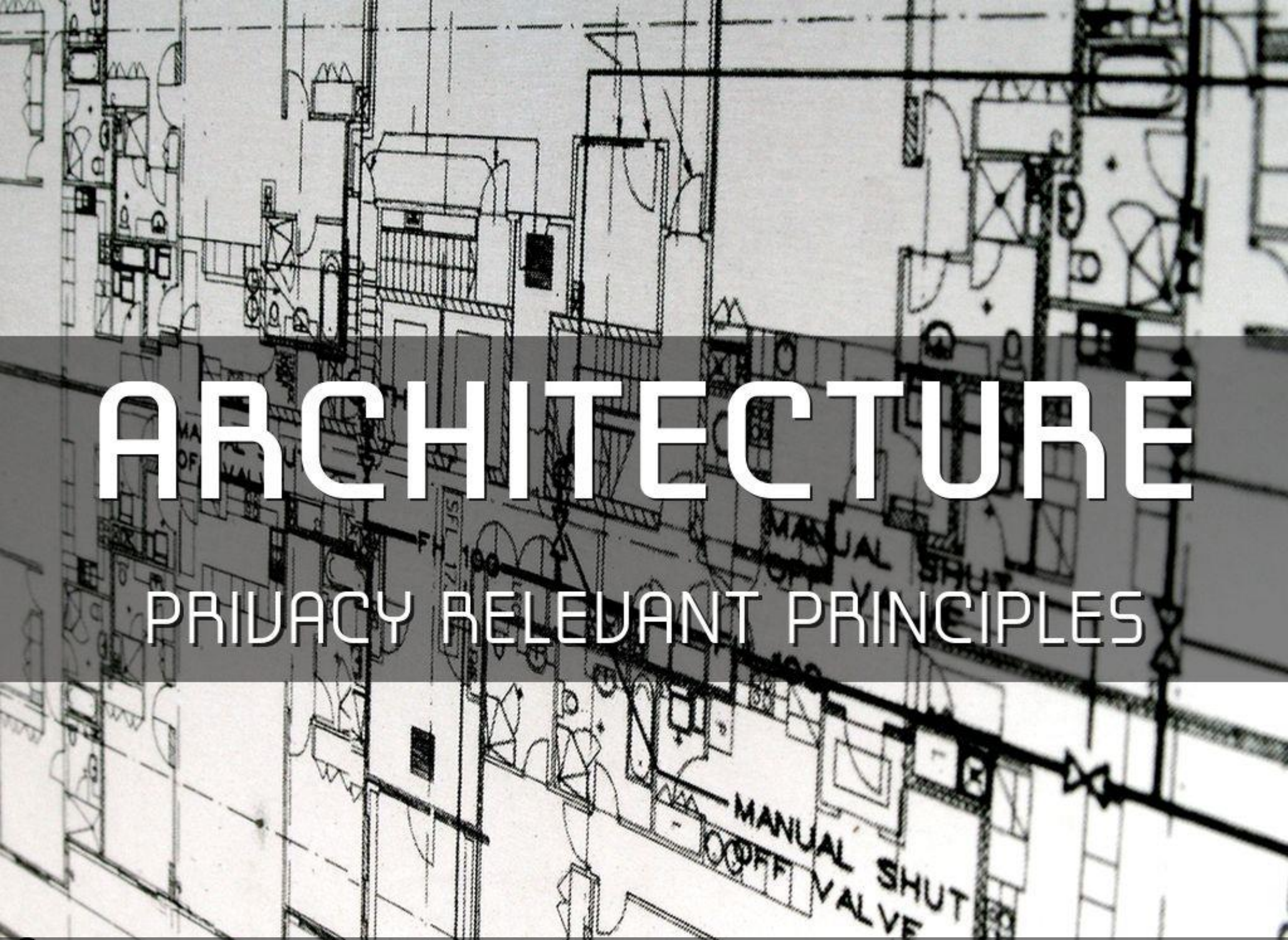
APPLIED TO PRIVACY CONCERNS

Photo by ruiwen - Creative Commons Attribution-ShareAlike License https://www.flickr.com/photos/7162499@N02

PHASES



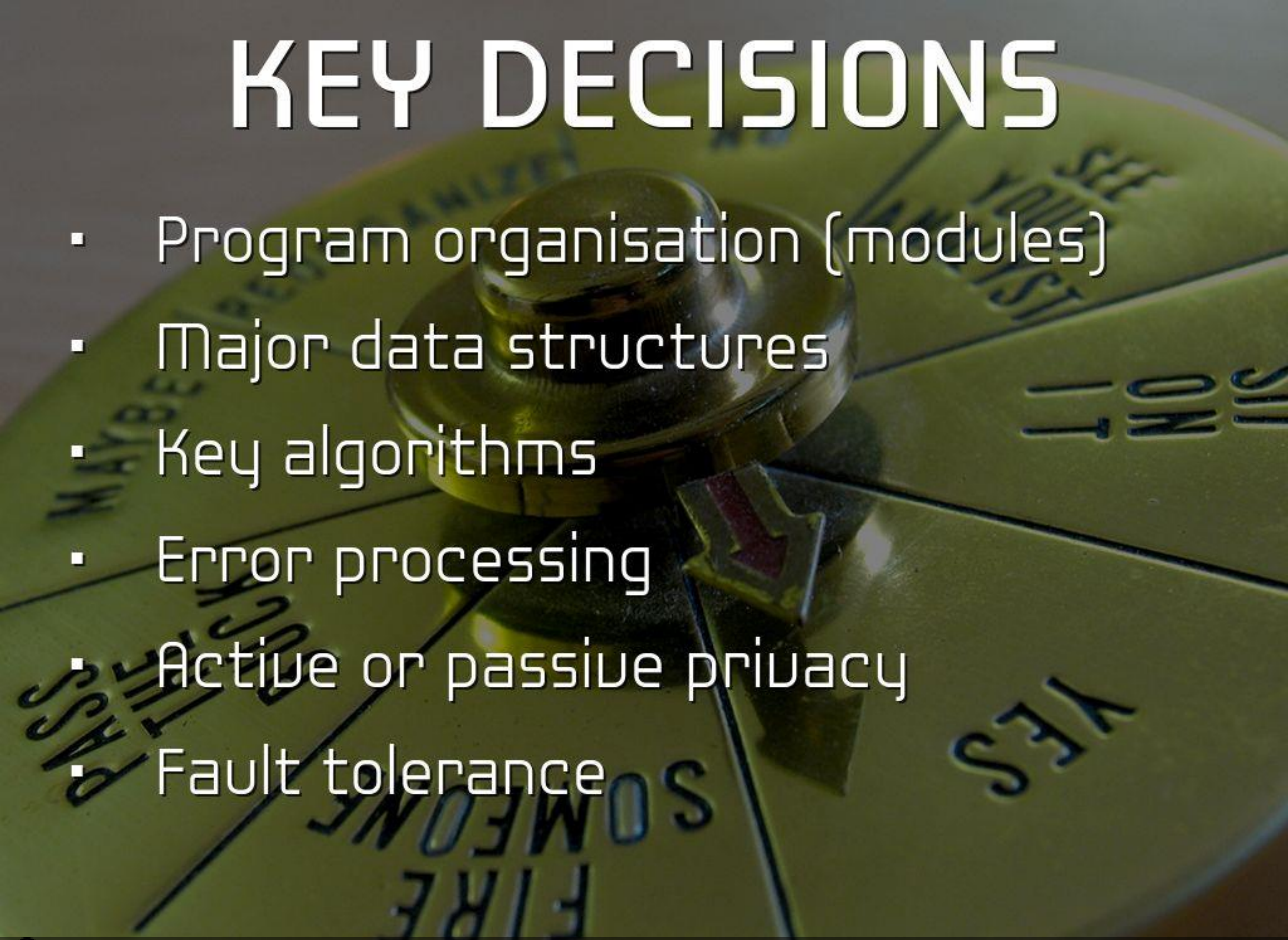
1. Architecture
2. Design
3. Implementation
4. Operation
5. Testing
6. Maintenance
7. Evaluation



ARCHITECTURE

PRIVACY RELEVANT PRINCIPLES

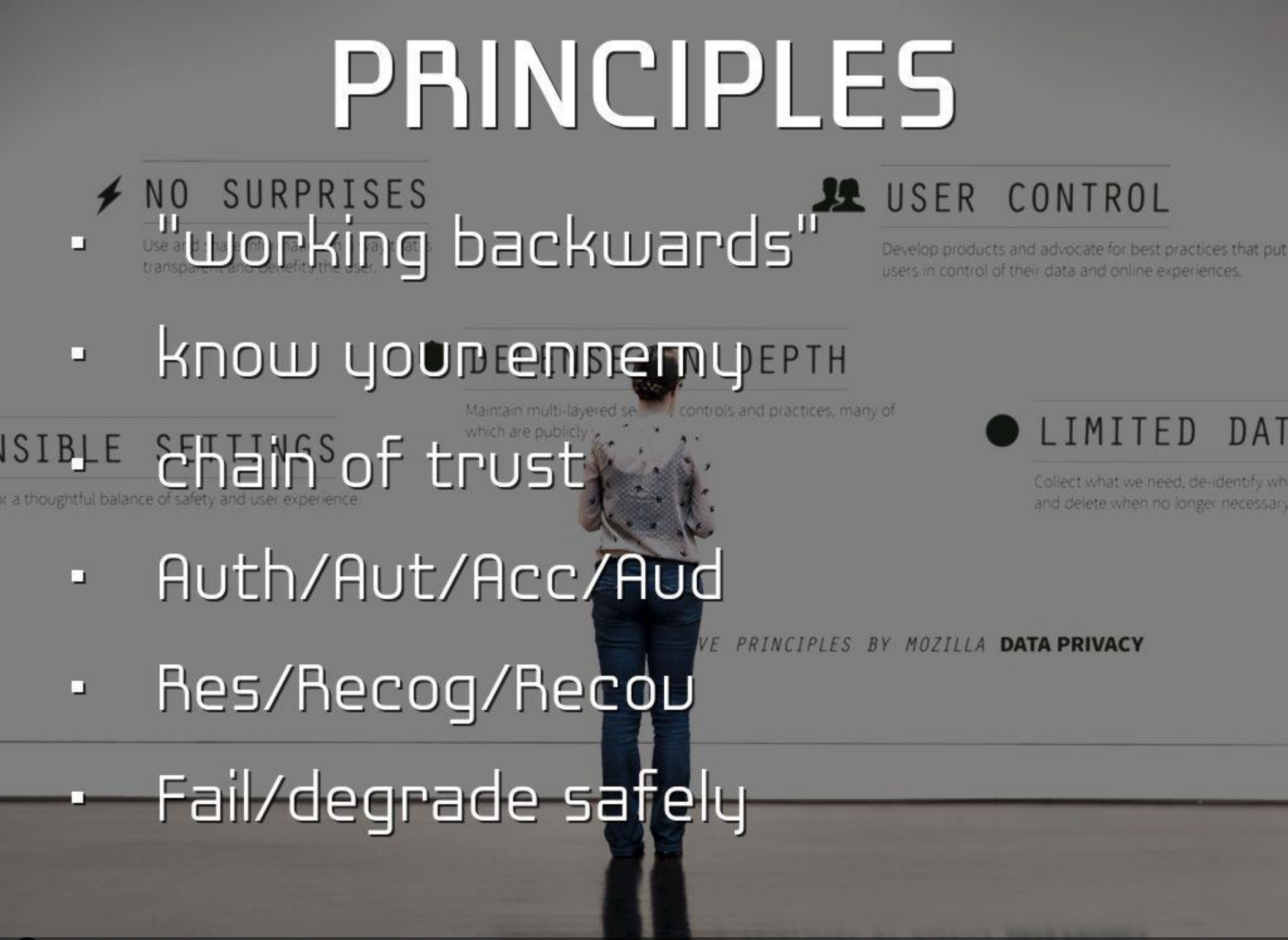
Photo by Thristian - Creative Commons Attribution-ShareAlike License http://www.flickr.com/[illegible] Created with [illegible]



KEY DECISIONS

- Program organisation (modules)
- Major data structures
- Key algorithms
- Error processing
- Active or passive privacy
- Fault tolerance

PRINCIPLES


NO SURPRISES
Use and share information in a way that is transparent and benefits the user.
USER CONTROL
Develop products and advocate for best practices that put users in control of their data and online experiences.
DEFENSE IN DEPTH
Maintain multi-layered security controls and practices, many of which are publicly
SENSIBLE SETTINGS
a thoughtful balance of safety and user experience.
LIMITED DAT
Collect what we need, de-identify wh and delete when no longer necessary
VE PRINCIPLES BY MOZILLA DATA PRIVACY

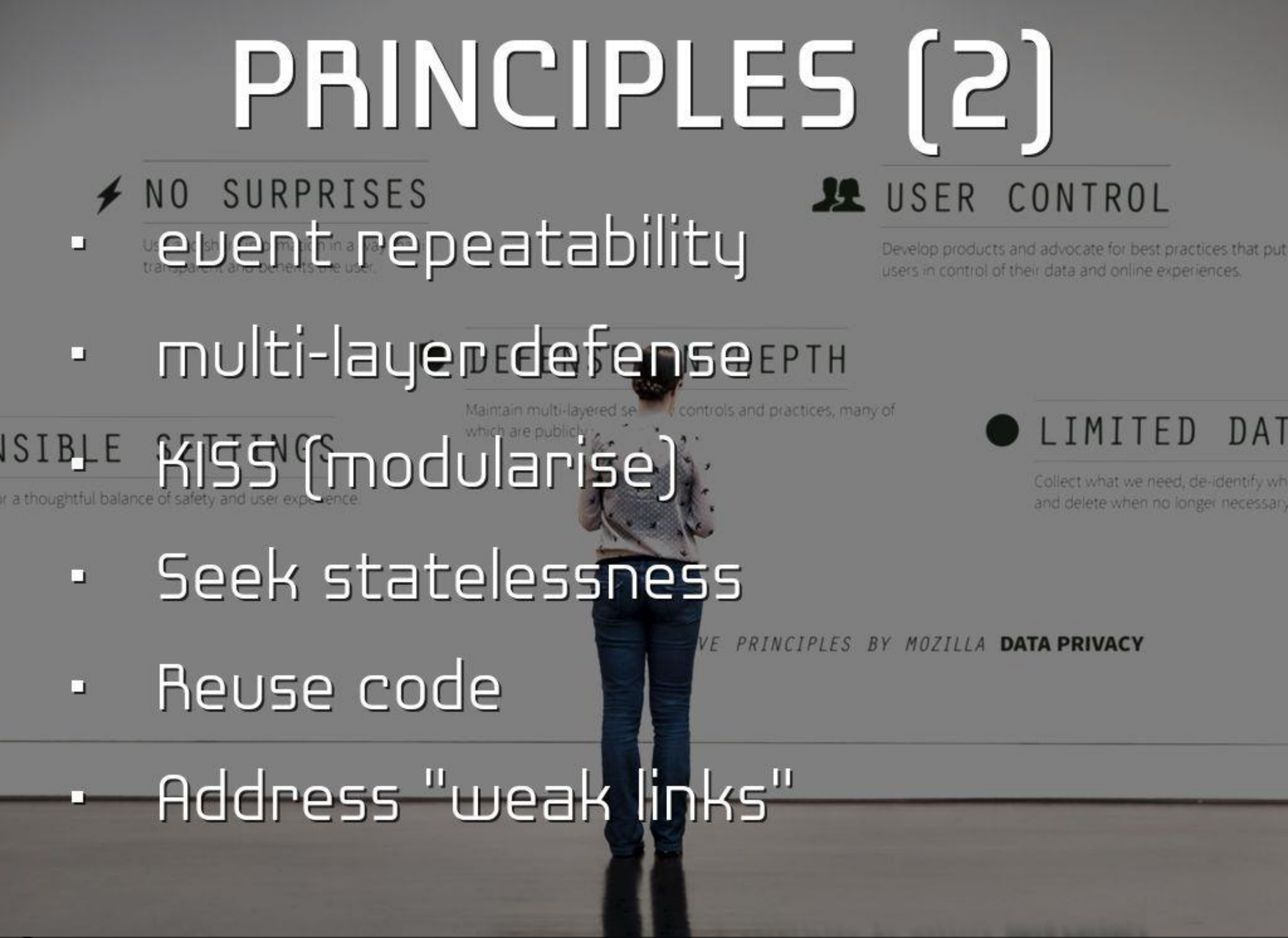
- "working backwards"
- know your ennemy
- chain of trust
- Auth/Aut/Acc/Aud
- Res/Recog/Recov
- Fail/degrade safely

Photo by vintagedept - Creative Commons Attribution License https://www.flickr.com/photos/42826854@N00

Created with Haiku Deck

PRINCIPLES (2)

- event repeatability
- multi-layer defense
- KISS (modularise)
- Seek statelessness
- Reuse code
- Address "weak links"

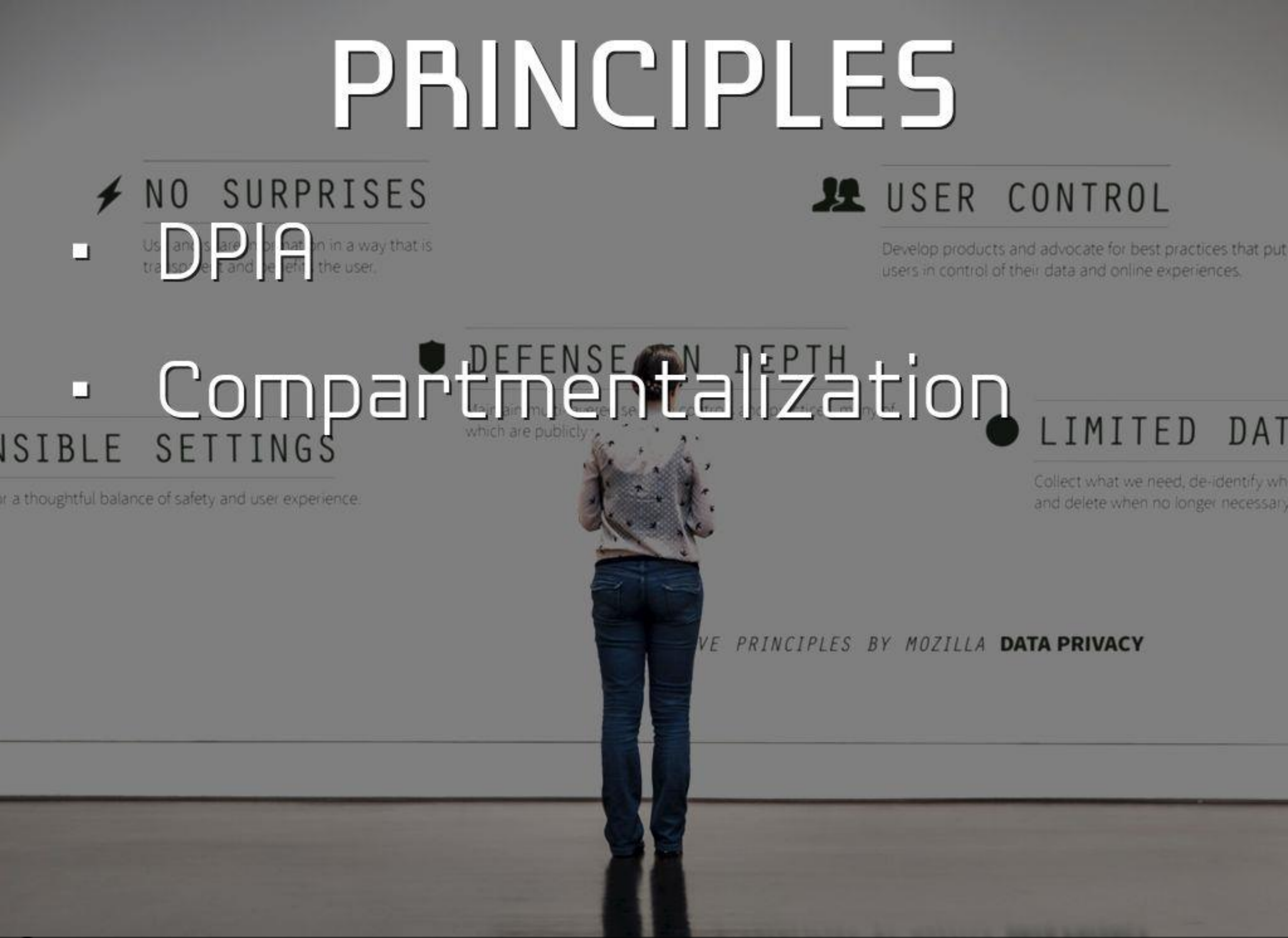

NO SURPRISES
USER CONTROL
Develop products and advocate for best practices that put
users in control of their data and online experiences.
EPTH
Maintain multi-layered se controls and practices, many of
which are publicly
LIMITED DAT
Collect what we need, de-identify wh
and delete when no longer necessary
NSIBLE
a thoughtful balance of safety and user experience.
VE PRINCIPLES BY MOZILLA DATA PRIVACY

DESIGN

PRIVACY RELEVANT PRINCIPLES

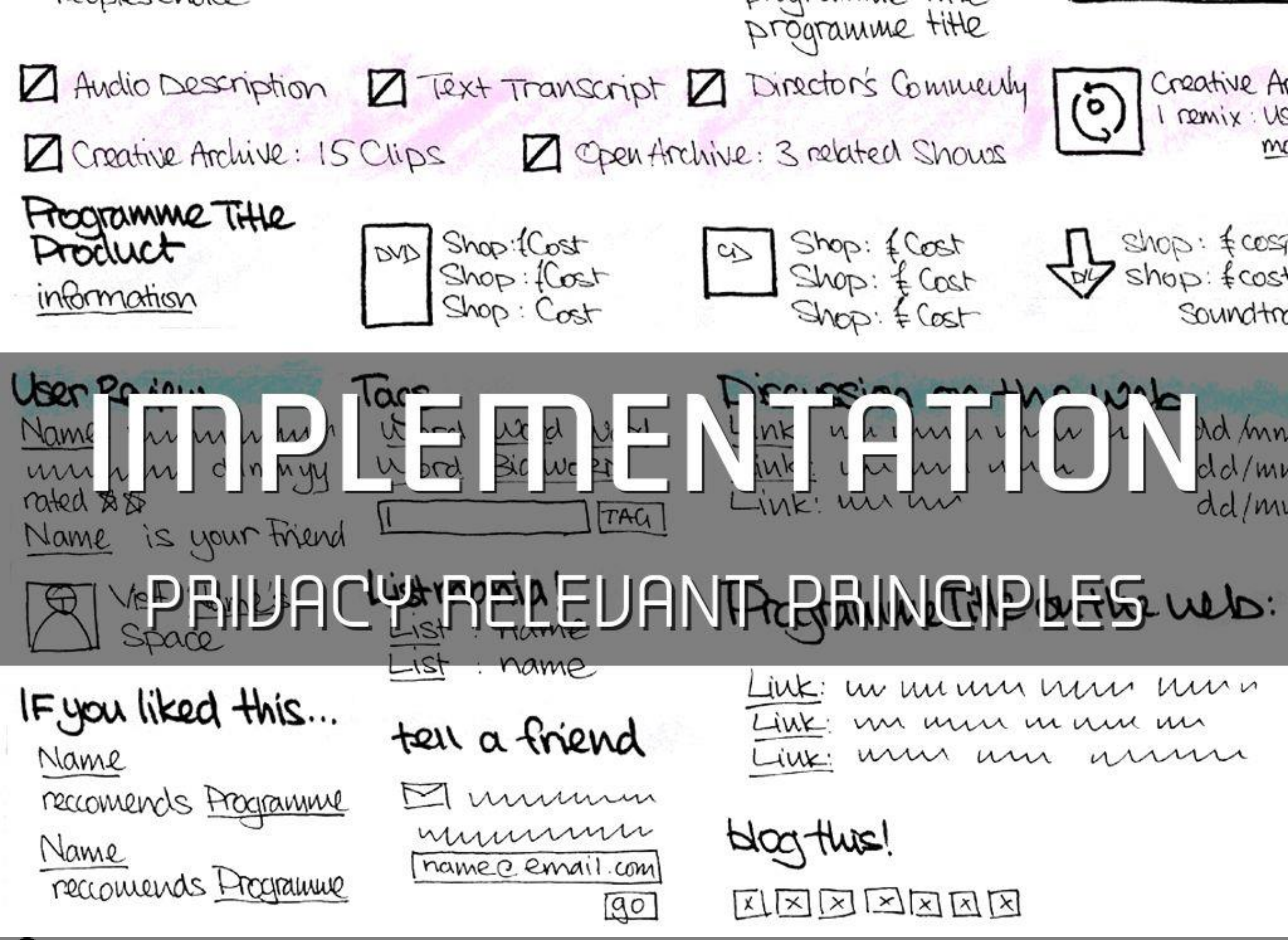
PRINCIPLES

- DPIA
- Compartmentalization

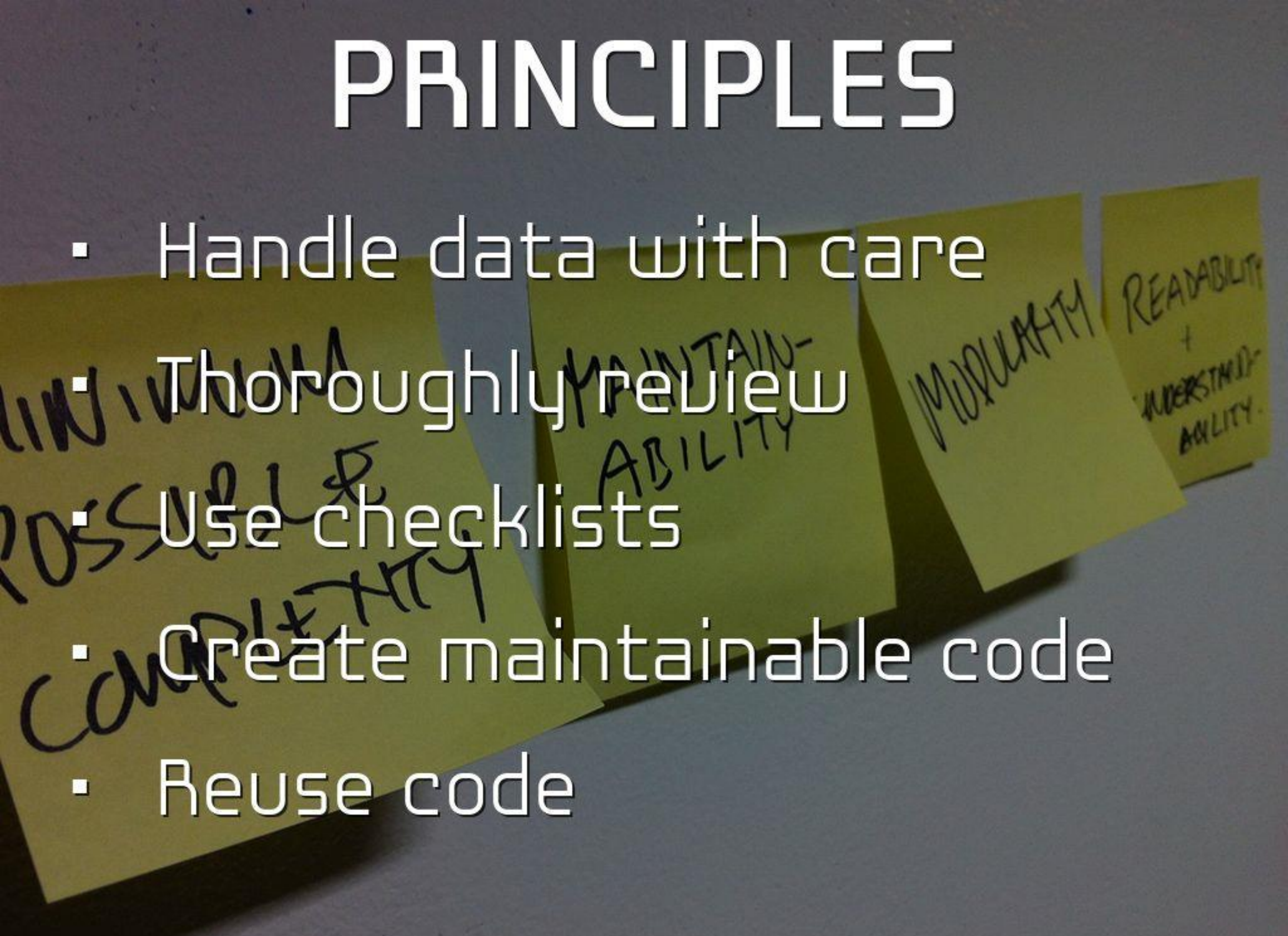

NO SURPRISES
in a way that is
the user.
USER CONTROL
Develop products and advocate for best practices that put
users in control of their data and online experiences.
DEFENSE IN DEPTH
which are publicly
SIBLE SETTINGS
r a thoughtful balance of safety and user experience.
LIMITED DAT
Collect what we need, de-identify wh
and delete when no longer necessary
VE PRINCIPLES BY MOZILLA DATA PRIVACY

IMPLEMENTATION

PRIVACY RELEVANT PRINCIPLES



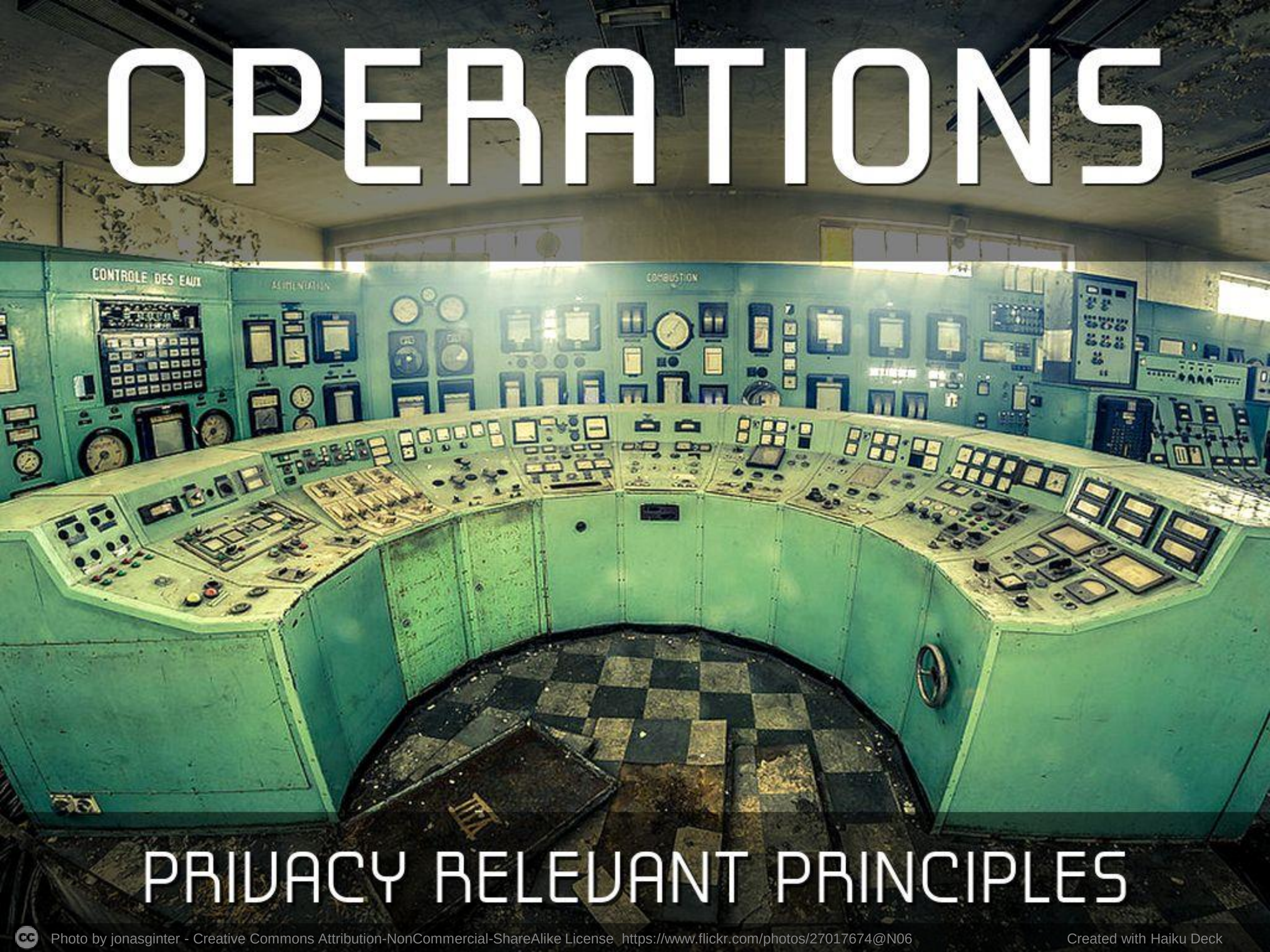
PRINCIPLES



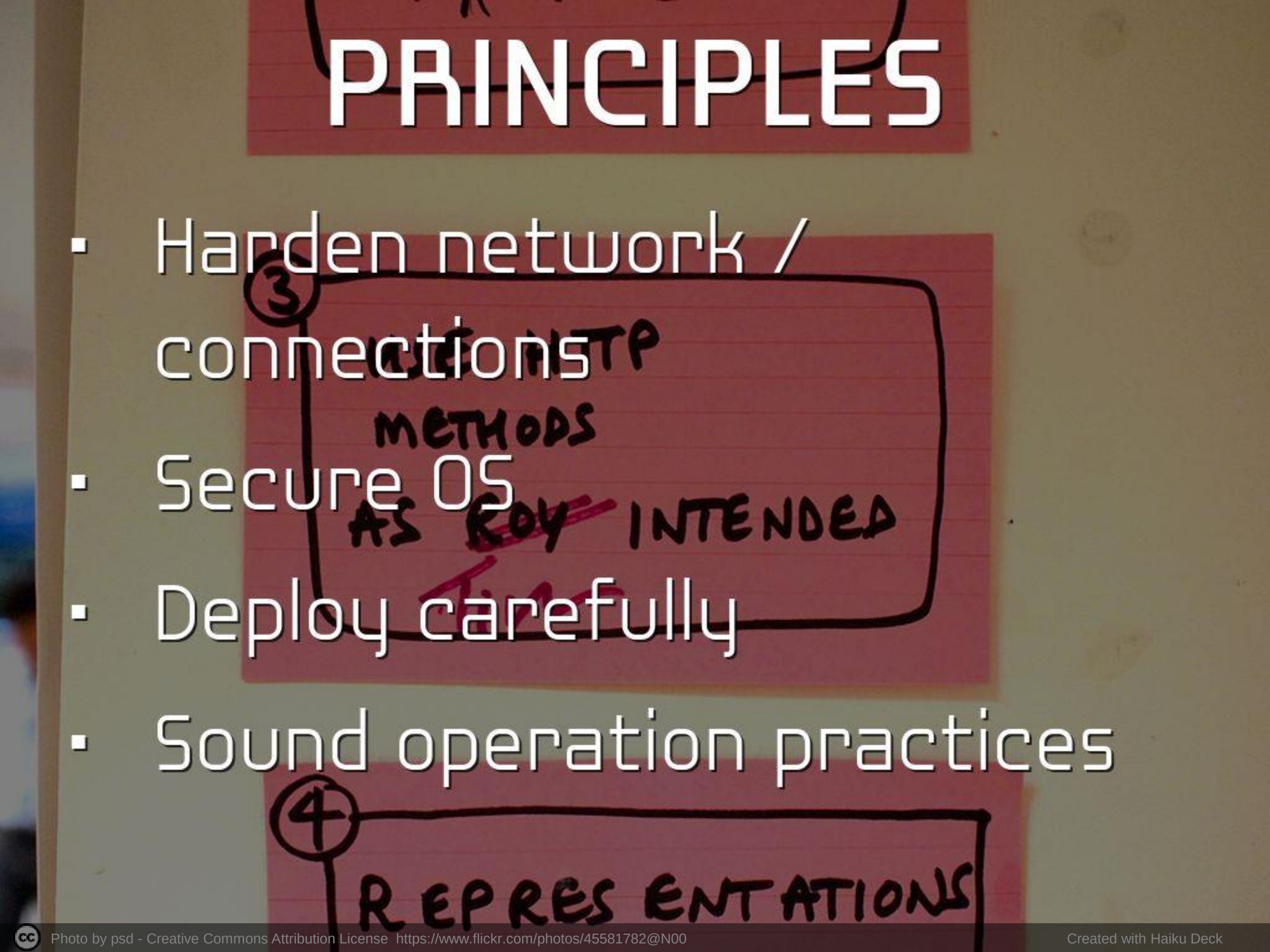
- Handle data with care
- Thoroughly review
- Use checklists
- Create maintainable code
- Reuse code

Photo by adactio - Creative Commons Attribution License https://www.flickr.com/photos/74105777@N00

OPERATIONS



PRIVACY RELEVANT PRINCIPLES

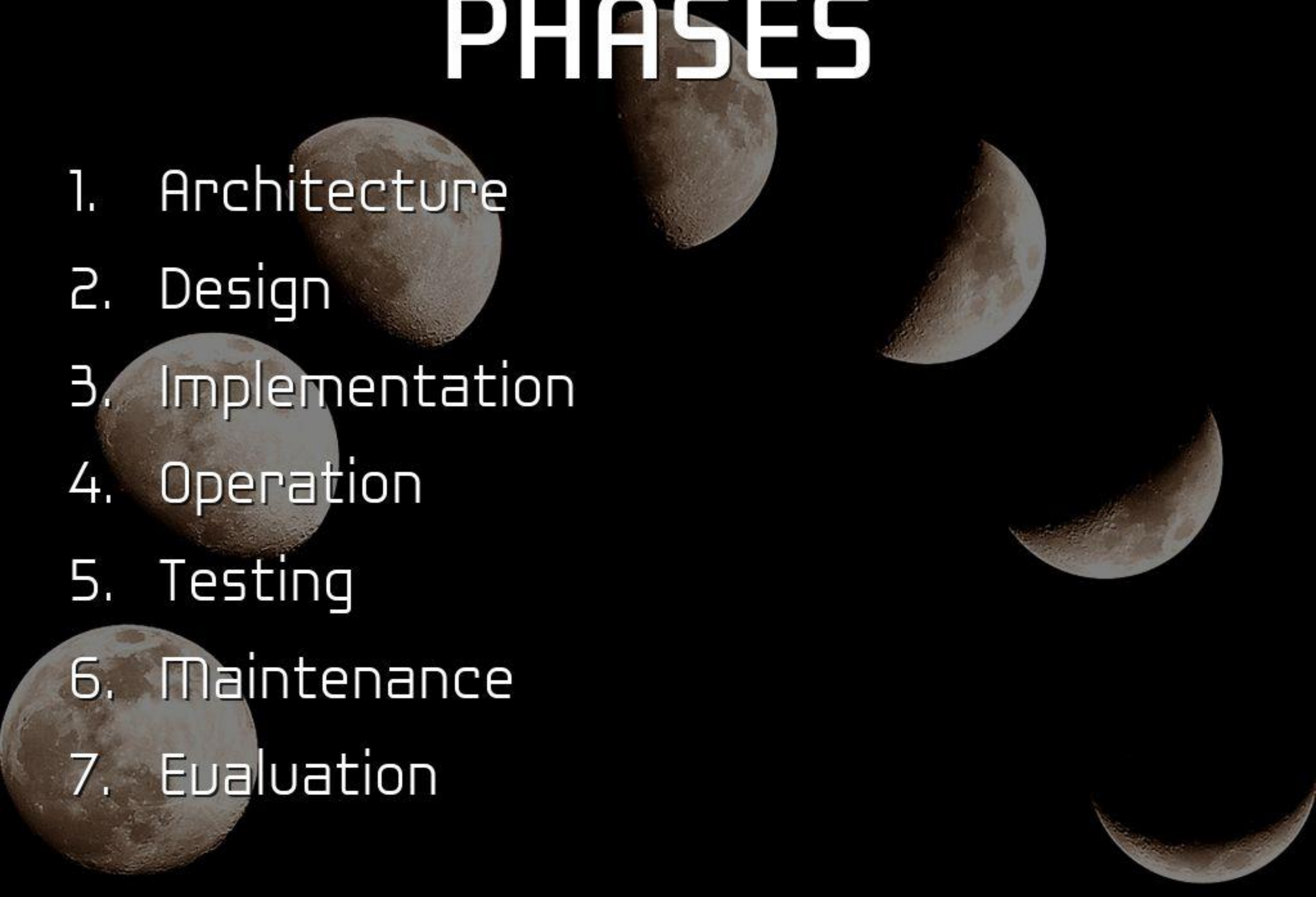


PRINCIPLES

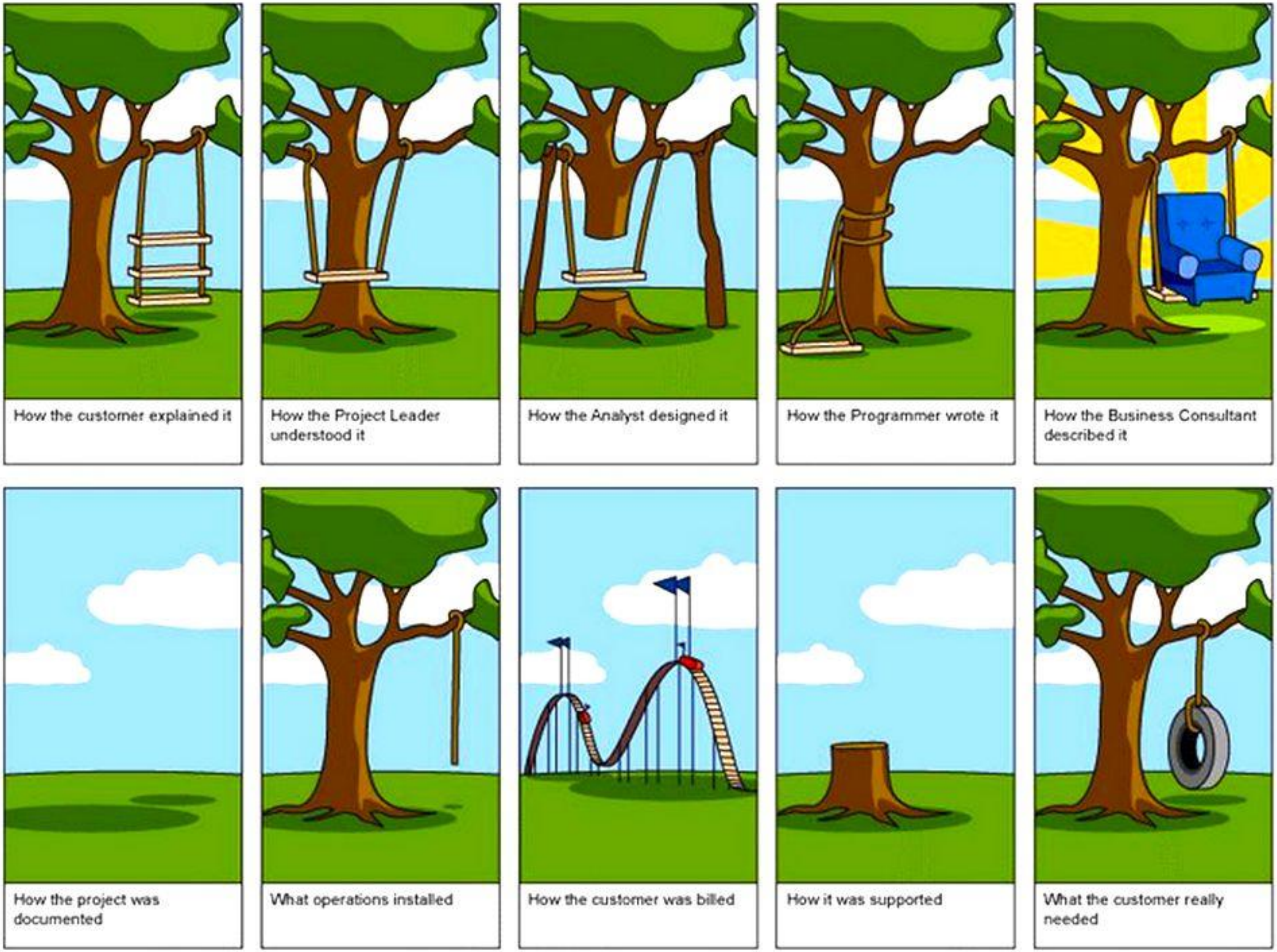
- Harden network / connections
- Secure OS
- Deploy carefully
- Sound operation practices

Photo by psd - Creative Commons Attribution License https://www.flickr.com/photos/45581782@N00

PHASES



1. Architecture
2. Design
3. Implementation
4. Operation
5. Testing
6. Maintenance
7. Evaluation



How the customer explained it

How the Project Leader understood it

How the Analyst designed it

How the Programmer wrote it

How the Business Consultant described it

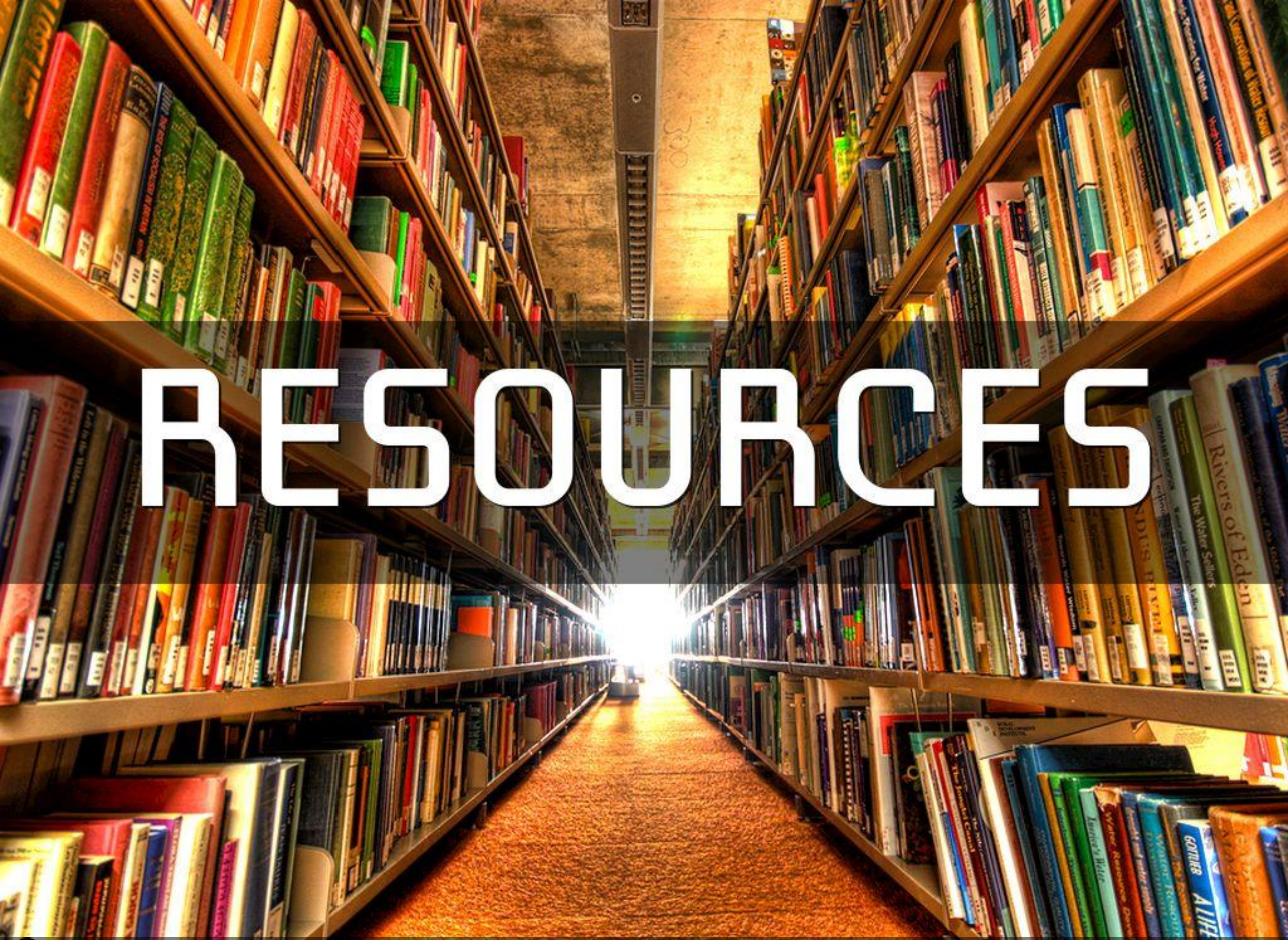
How the project was documented

What operations installed

How the customer was billed

How it was supported

What the customer really needed



RESOURCES

Photo by RichGrundy - Creative Commons Attribution-NonCommercial License https://www.flickr.com/photos/32888907@N03 Created with Haiku Deck

OECD PRIVACY GUIDELINES

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

OWASP

Top 10 Privacy Risks

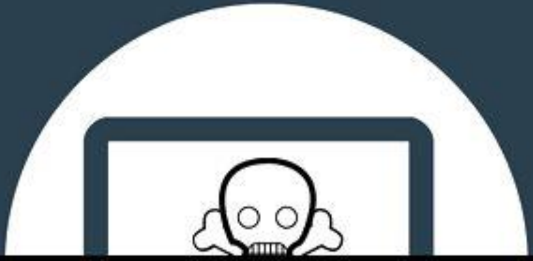
Alpha Version 1.0

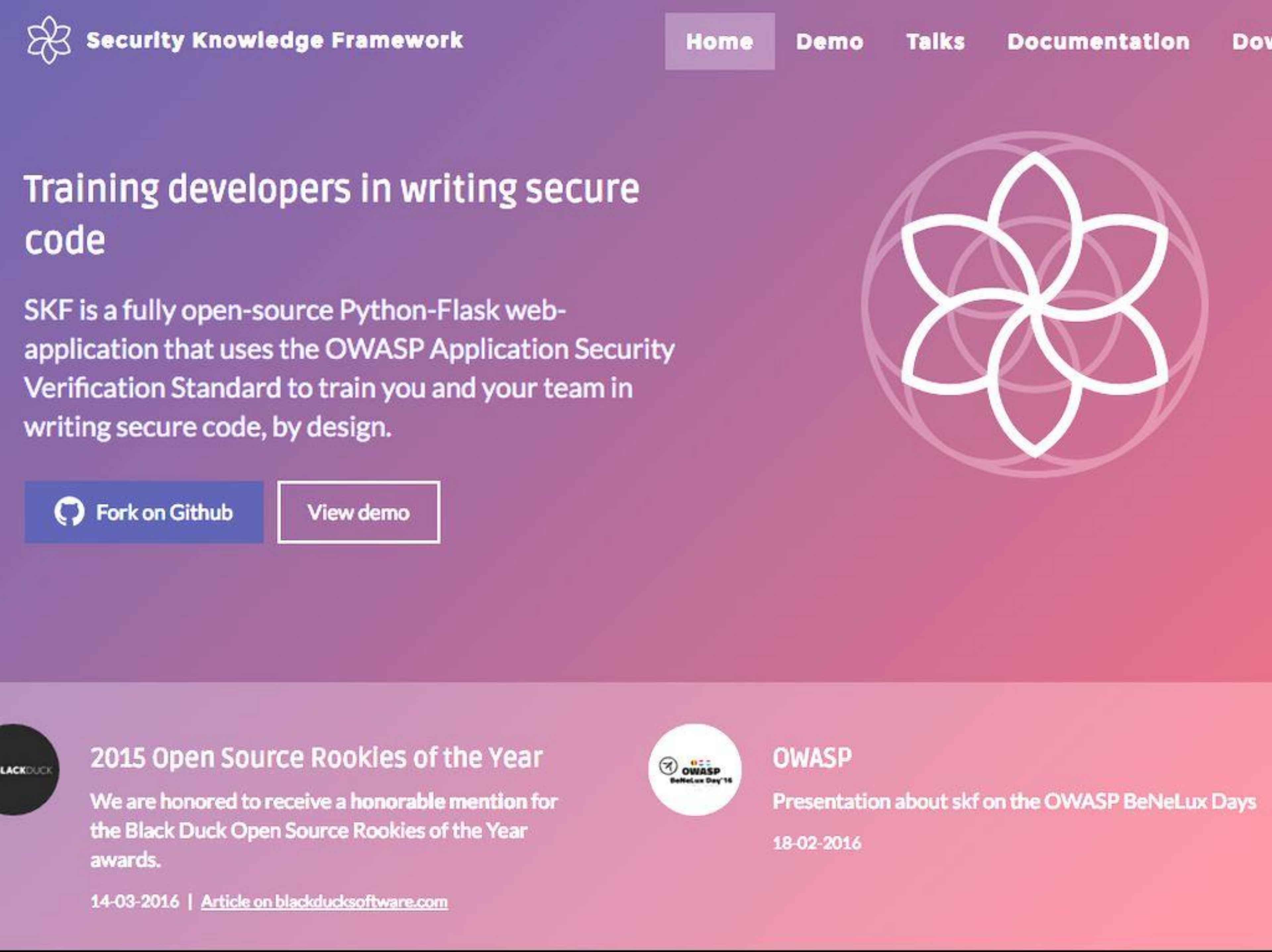
Website Application Vulnerabilities

#1

Frequency: High
Impact: Very High

Vulnerability is a key problem in any system that guards or operates on sensitive user data. Failure to suitably design and implement an application, detect a problem or promptly apply a fix (patch) is likely to result in a privacy breach. This risk also encompasses the OWASP Top 10 List





Security Knowledge Framework

Training developers in writing secure code

SKF is a fully open-source Python-Flask web-application that uses the OWASP Application Security Verification Standard to train you and your team in writing secure code, by design.

2015 Open Source Rookies of the Year

We are honored to receive a honorable mention for the Black Duck Open Source Rookies of the Year awards.

14-03-2016 | Article on blackducksoftware.com

OWASP

Presentation about skf on the OWASP BeNeLux Days

18-02-2016

THANK YOU

PASCAL STEICHEN