

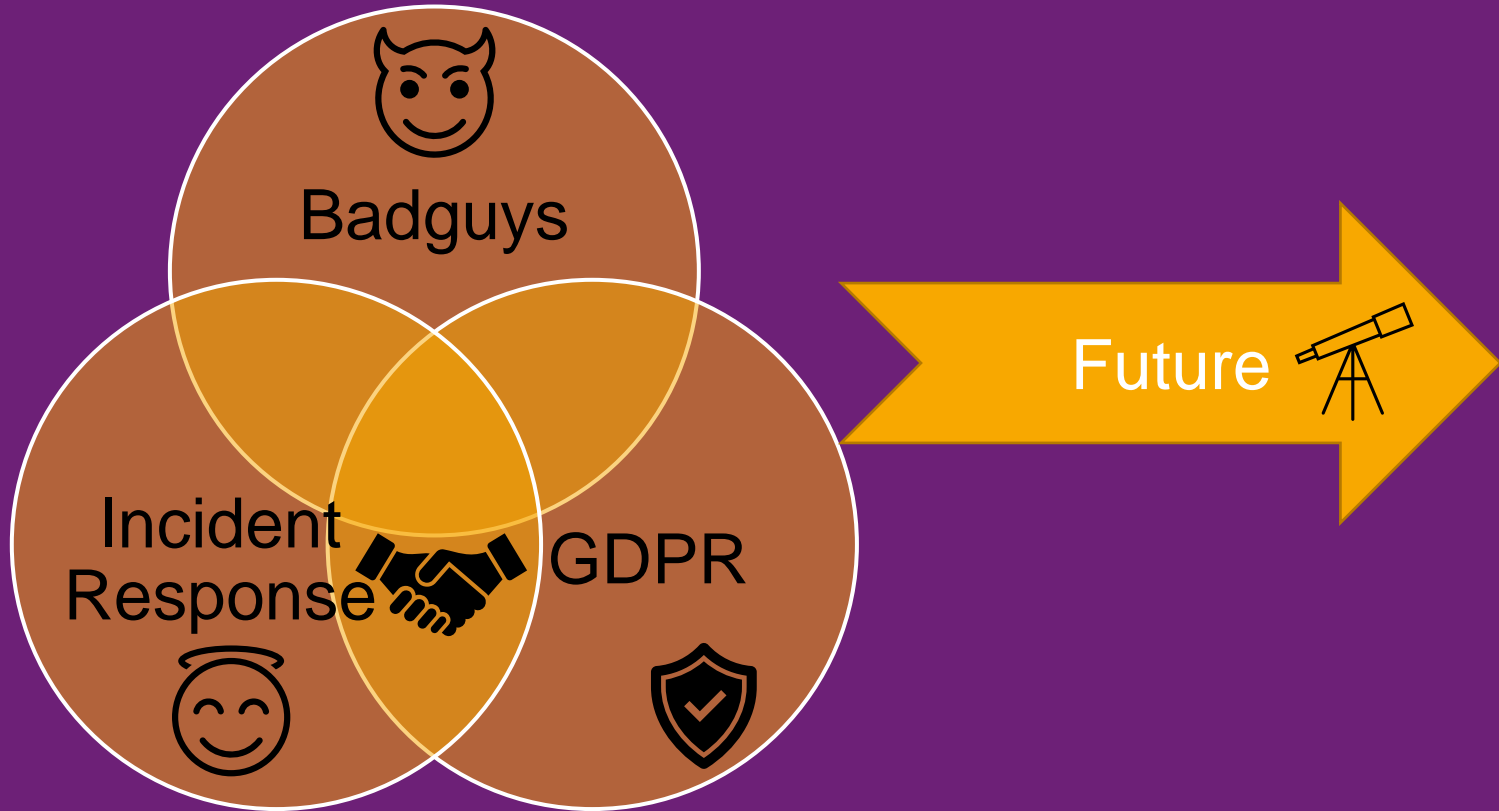
The background of the slide is a photograph of a red wooden lifeguard hut on a sandy beach. The hut has a green roof and is elevated on wooden stilts. A wooden ramp leads up to the hut. In the background, the ocean is visible with some people walking on the beach.

# Data Protection and Incident Response

... from contradiction to cuddle-buddies

Andrew Cormack, Chief Regulatory Adviser, Jisc

# Outline of talk



# What do badguys want?

(in most cases)

## MONEY

- Credit Card theft  
+ other identifying data
- Bank payment modification
- Ransomware

a.k.a.  
Unauthorised/  
Uncontrolled

- Viewing
- Sale
- Modification
- Destruction



# What do badguys need

(in most cases)

Invisibility

+

Scale

=

Time

- Data loses value once loss is known
- Opportunity for profit/harm may be lost

- Most attacks are not targeted
- Low success rate/low value
- High volume needed

- To build up scale while remaining invisible

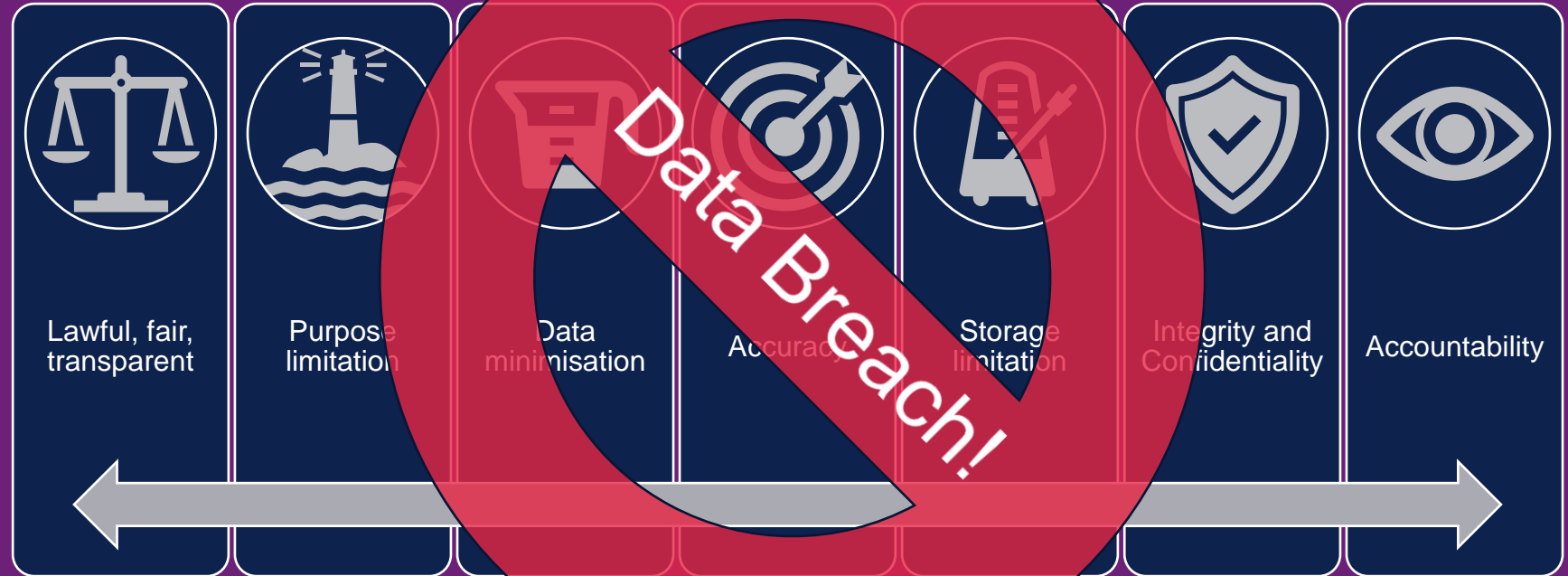
# What does data protection (law) need

## GDPR Principles

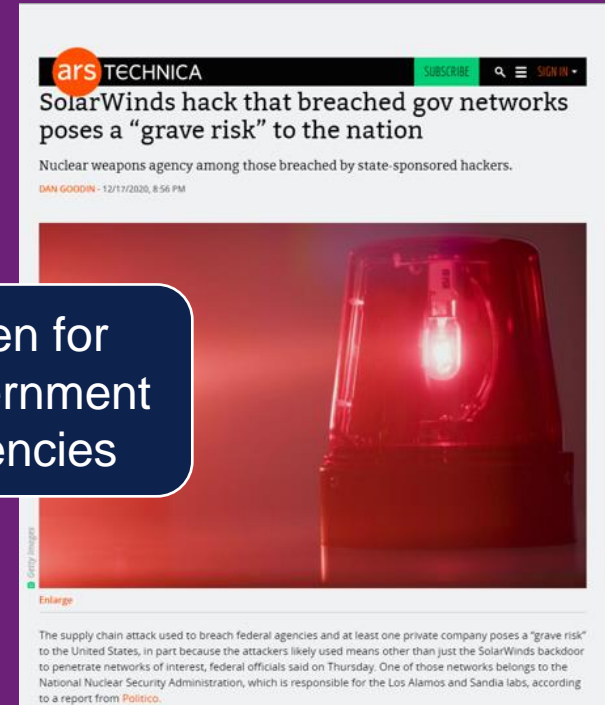


# What does data protection (law) need

## GDPR Principles



# Why do we need Incident Response (IR)?





# Why might Incident Response work?

## Badguy Needs => IR Opportunity

Invisibility => victims won't know till too late

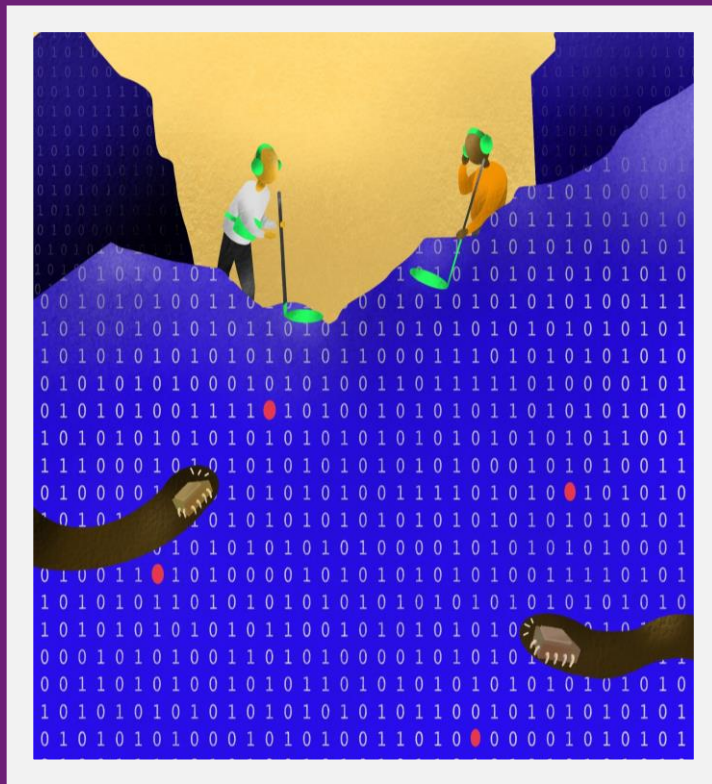
- Someone external might spot signs

Scale => large-scale patterns

- Wide perspective may detect these

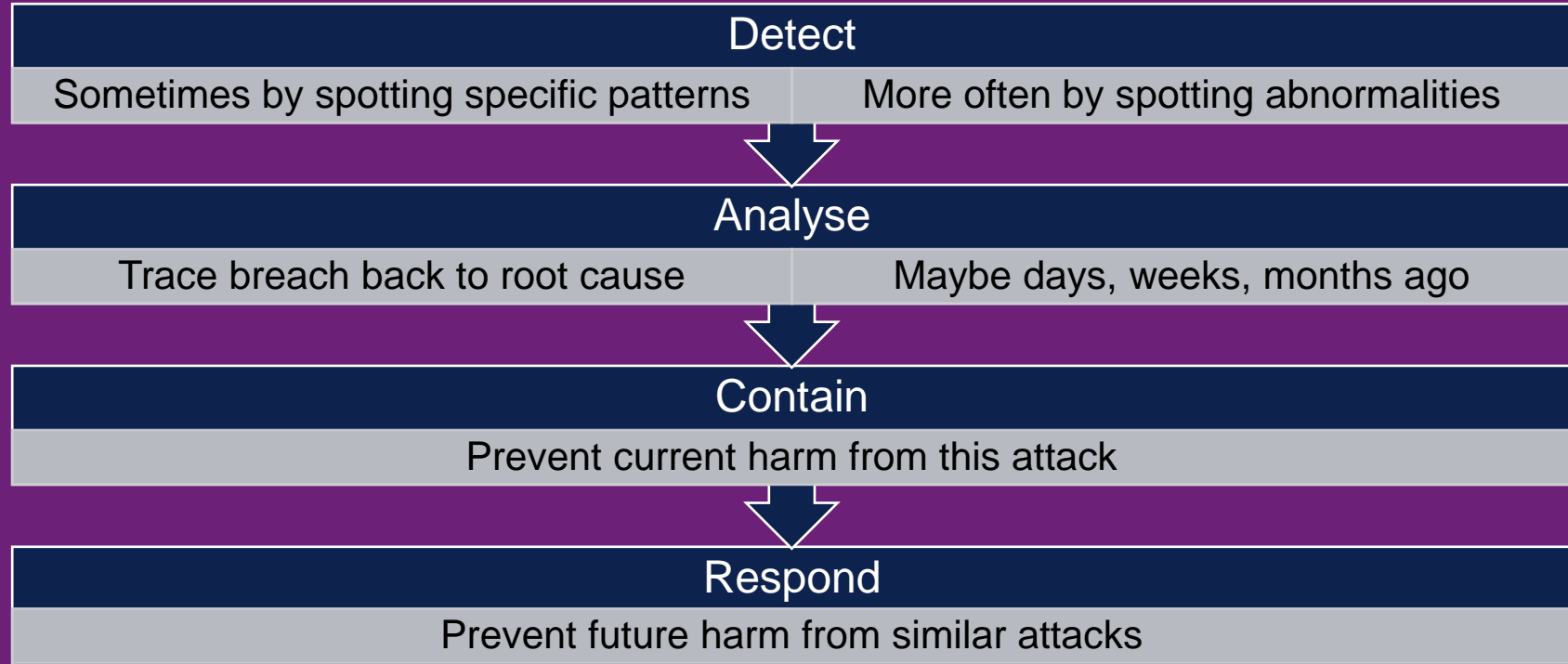
Time => opportunity window

- To detect/mitigate before major harm





# What does IR look like?



# What does IR need?

## Data

- To spot patterns and abnormalities
- Flows, activity, logs
  - Network/email, website visits, file/process creation/deletion...
- Lots of personal data
- Normal & abnormal



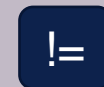
## History

- To understand how breach happened
- To mitigate current harm
- To prevent future harm










## Care

- To be (much) less threat than the badguys...



# DP + IR?

## Conflict, or compatible?

	DP Principle	IR Purpose?
	Lawful, fair, transparent	Yes: otherwise we're no better than badguys
	Purpose limitation	Yes: "ensuring network and information security"
	Data minimisation	Yes: the haystack is big enough already
	Accuracy	Yes: we need to see through badguy attempts at concealment
	Storage limitation	Yes: there's a point where all damage will have been done
	Integrity and Confidentiality	Yes: if badguys can access our data/knowledge we're helping them
	Accountability	Yes: well-designed processes are essential to operate IR

# How to (formally) align law and IR?

Not personal data?

- Maybe technically true, but uninformative and untrustworthy

Consent (by using service)?

- Just, no...

(Part of) Contract?

- Maybe, but doesn't work for non-customer logs

Public interest?

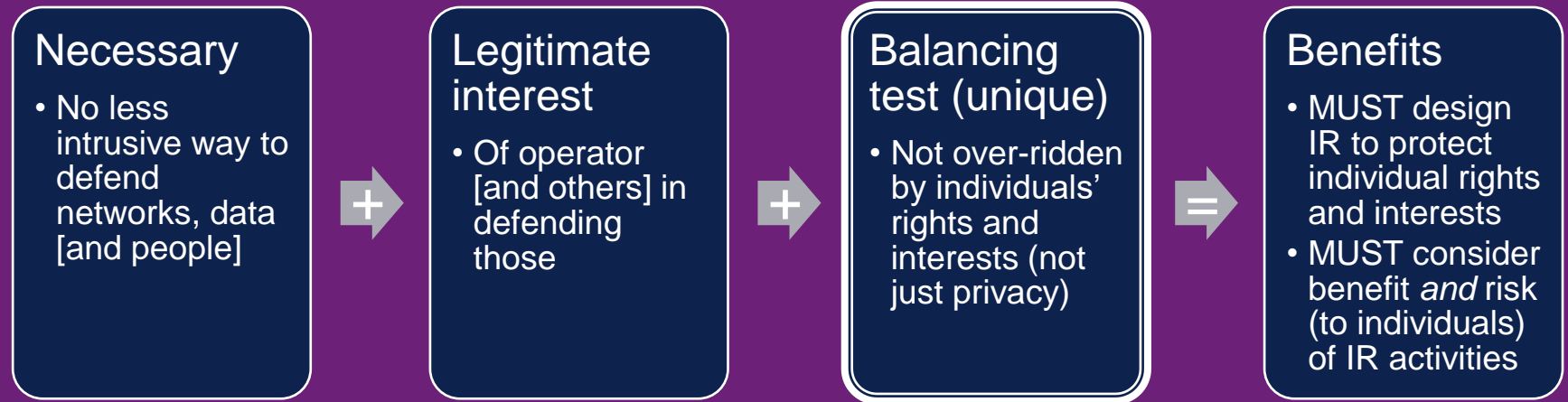
- If you're a public body, with IR as legally-defined task
- Balancing test is good practice, rather than legal requirement

Legitimate interest?

- Yes! leads to good data protection **and** good incident response!

# Legitimate Interest Rec.49/Art 6(1)(f)

“Most protective lawful basis in GDPR” [ANC]



# How does this help IR?

Builds Trust

- More trustworthy to embrace legal framework than quibble it away

Helps think about...

- Data minimisation (start from process and work back)
- Retention periods (look realistically at when IR becomes irrelevant)
- Prioritisation/sharing (via balancing test)
- And more...

# For example: information sharing (0)

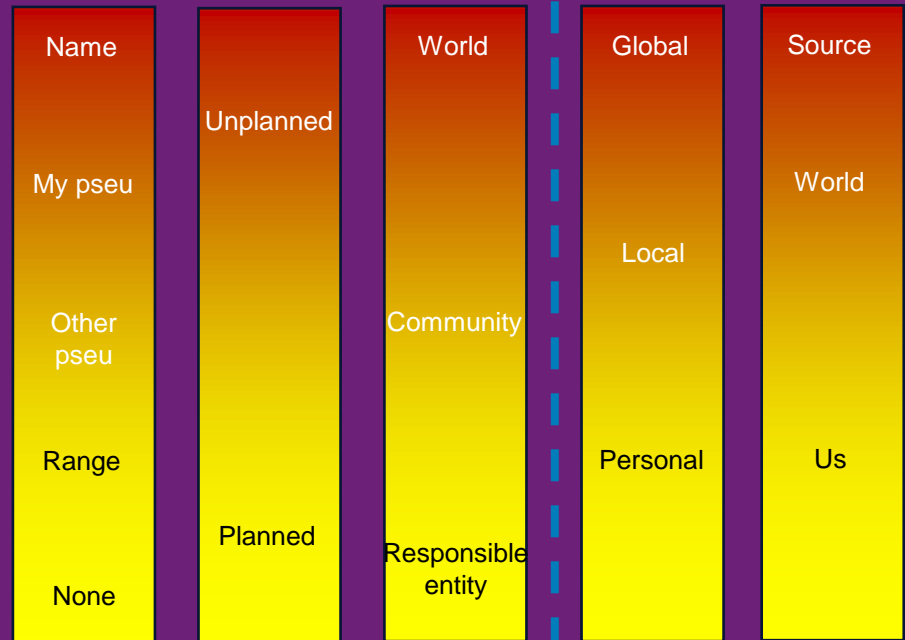
## Art.6(1)(f) balancing test

### Harm factors

- What identifier
- How collected
- Extent of disclosure

### Benefit factors

- Severity of (potential) incident
- Extent of benefit





# For example: information sharing (1)

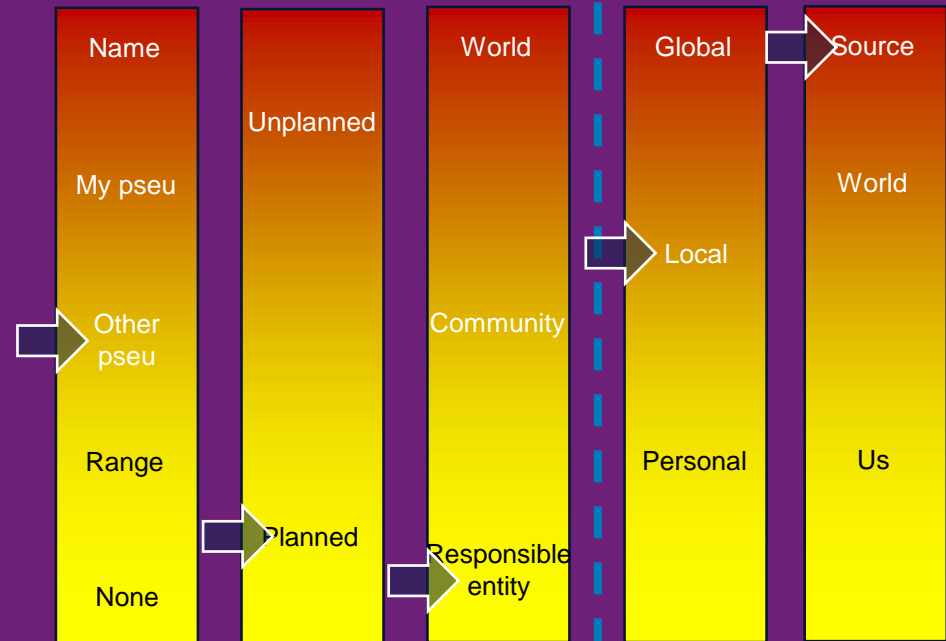
## Harm factors

- What identifier
- How collected
- Extent of disclosure

## Benefit factors

- Severity of (potential) incident
- Extent of benefit

## Reporting compromised PC to home ISP



Based on Cormack (2016)

# For example: information sharing (2)

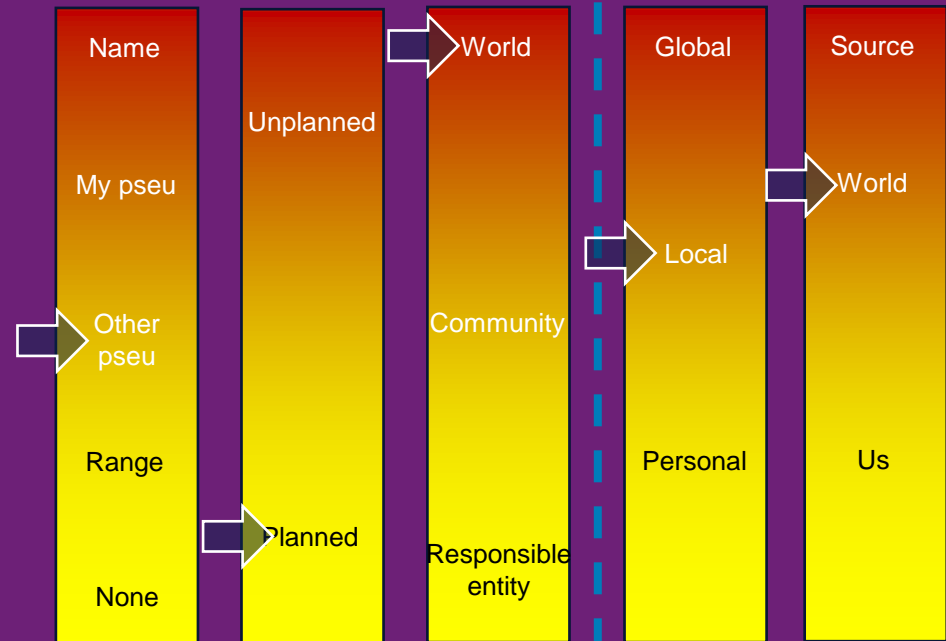
## Harm factors

- What identifier
- How collected
- Extent of disclosure

## Benefit factors

- Severity of (potential) incident
- Extent of benefit

## Publishing list of SSH scanning IPs



Based on Cormack (2016)

# History of co-existence (2009-2016)

It's allowed...

## ePrivacy Directive (2009 revision)

- First mentions “legitimate interest” in protecting networks

## GDPR

- Confirms legitimate interest, expands scope of those covered

## Breyer v Germany (ECJ case)

- Confirms legitimate interest, even under DP Directive, and that website operators are in scope

# History of co-existence (2017-2020)

It's required...

Art29 Guidelines on Breach Notification (WP250)

- Threat of (additional) fine for not doing IR

Ticketmaster (UK ICO penalty notice)

- £1.25M for – among other things – not doing good IR

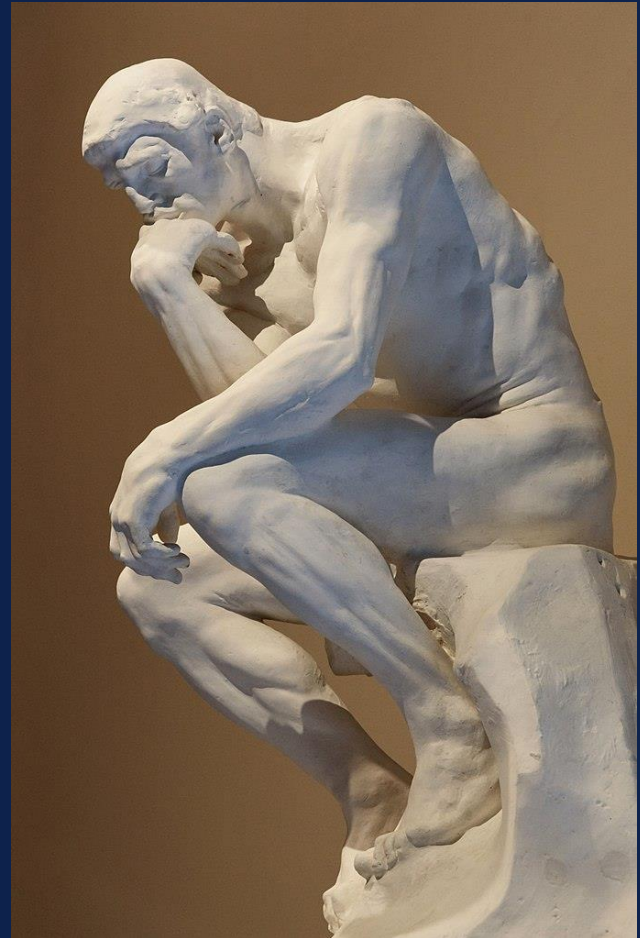
Not just compatible: mutually dependent 😊

# I wish I'd said this...

**"We are not protecting the data, we are protecting the individual human being and sometimes to protect the human being you need to use data."**

EDPS, Wojciech Wiewiórowski (reported by Gabriela Zanfir-Fortuna)  
at Brussels Privacy Forum on Personal Data in Research, 2<sup>nd</sup> Dec 2020

**PAUSE**



"Rodin's Thinker" by Mustang Joe is available  
under [CC0 Universal Public Domain Dedication](#)

# Is this (really) necessary?

## Lessons from *Watson/Tele II* (case that cancelled the Data Retention Directive)

### Purpose

- Define/distinguish: Defence (IR) vs offence/attribution (LEO)
- We're trying to help (many) victims, not punish (few) terrorists

### Pseudonyms

- Covers most IR data (e.g. IP addresses): good for DP
- Identify as late as possible (When you know you have a victim)

### Automated Processing

- Arguably a requirement (legal & practical) of minimisation...
- At least for initial data => alert reduction stage

### Automated *Prevention*

- Even better than incident response (when possible & accurate)
- Don't ban it via automated decision-making rules, please



# Information Sharing (1)

## How law could help (more)

Why

Effective...

- Tell victims
- Tell other teams
- Collaborate to fix

How

Trustworthy...

- Within DP law
- Simple process
- Global benefits

## Inter-sector

### Between (legal) regimes

- If I can't lawfully do something, but you can...
- My data subjects may worry if I share with you

### Risk of such bumps between

- CSIRT => Law Enforcement/National Security
  - If latter has additional powers
- CSIRT => Public Body?
- CSIRT => Network Operator?
  - If future ePrivacy Regulation reduces restrictions on latter
- Not-NIS => NIS?

### Self-denying ordinances?

- e.g. NCSC-NL is a CSIRT, not a security service
- e.g. Public bodies should also balance IR against rights

# Information Sharing (2)

## How law could help (more)

Why

Effective...

- Tell victims
- Tell other teams
- Collaborate to fix

How

Trustworthy...

- Within DP law
- Simple process
- Global benefits

## International

### Within EU

- Legitimate interests (of many parties) looks OK

### Exports (incidents often global)

- DP Directive: self-assess benefit/risk
- GDPR: removes self-assessment option, so
  - Legitimate interest (Art.49) for ad hoc, but
    - Limited to exporter's "compelling" interest
    - Formalities? ("inform supervisory authority"?)
- Contracts for regular sharing/platforms?

# This isn't an essay question...



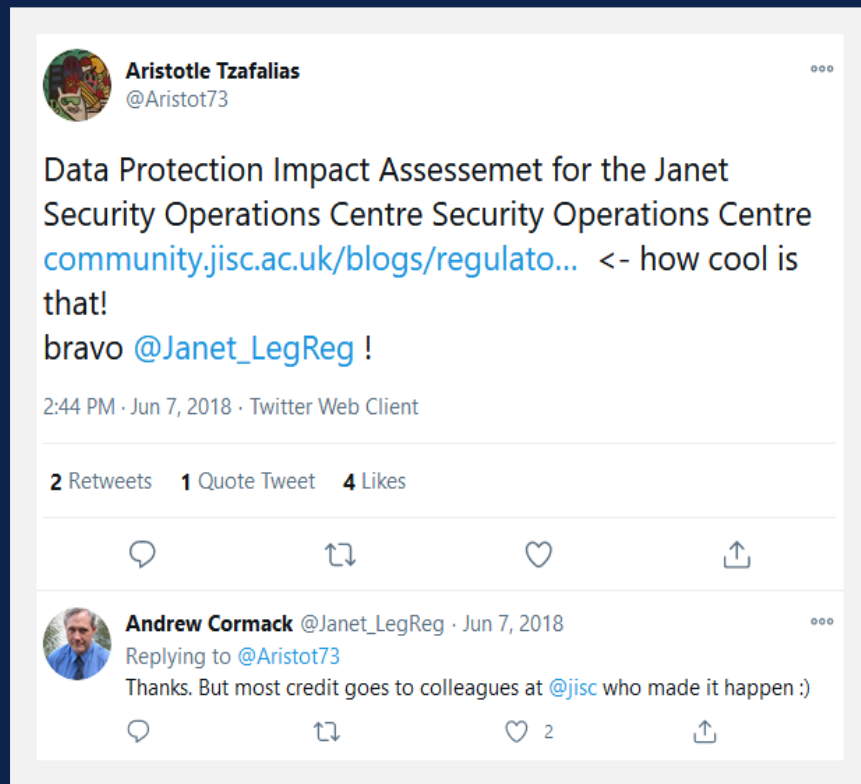
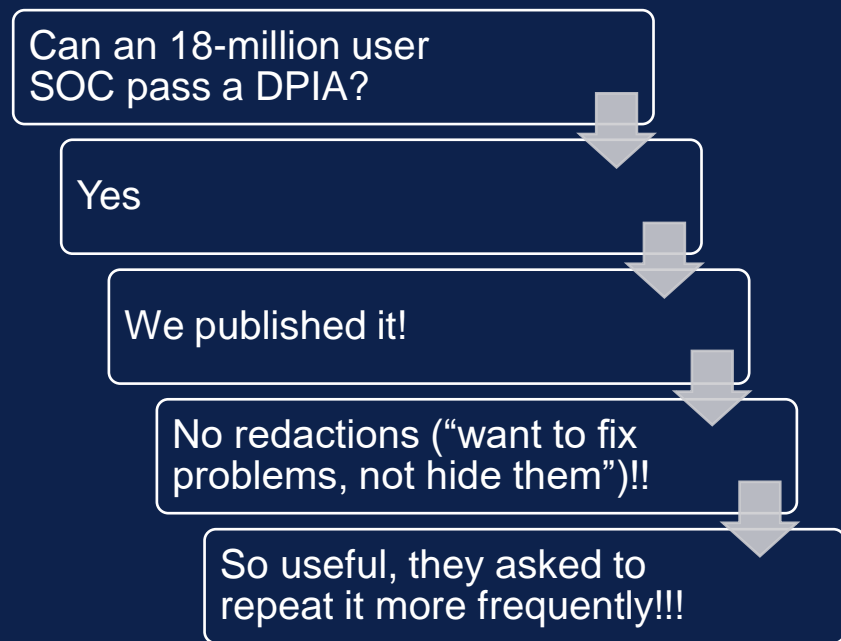


# The online equivalent shouldn't be, either



# Security Operations Centre DPIA

## The ultimate test...



# References

- Videos
  - <https://regulatorydevelopments.jiscinvolve.org/wp/2020/10/15/incident-response-and-law/> (5 min)
  - <https://regulatorydevelopments.jiscinvolve.org/wp/2020/10/28/assessing-our-security-services/> (1 min)
- Law Papers
  - Incident Response (2016) <https://doi.org/10.2966/scip.130316.258>
  - Incident Detection (2020): <https://doi.org/10.2966/scip.170220.197>
  - History of the IR “permission” (2018): <http://ejlt.org/index.php/ejlt/article/view/617>
- SOC DPIA: <https://repository.jisc.ac.uk/8063/1/jisc-security-operations-centre-dpia-august-2020.pdf>
- PenTest LIA: <https://regulatorydevelopments.jiscinvolve.org/wp/2018/09/12/penetration-testing-legitimate-interests-assessment/>
- Blog: <https://regulatorydevelopments.jiscinvolve.org/wp/tag/incident-response/>



**Andrew Cormack**  
**Chief Regulatory Adviser**  
**@Janet\_LegReg**

---

Lumen House, Library Avenue, Didcot

OX11 0SG UK

[Andrew.Cormack@jisc.ac.uk](mailto:Andrew.Cormack@jisc.ac.uk)

[jisc.ac.uk](http://jisc.ac.uk)

