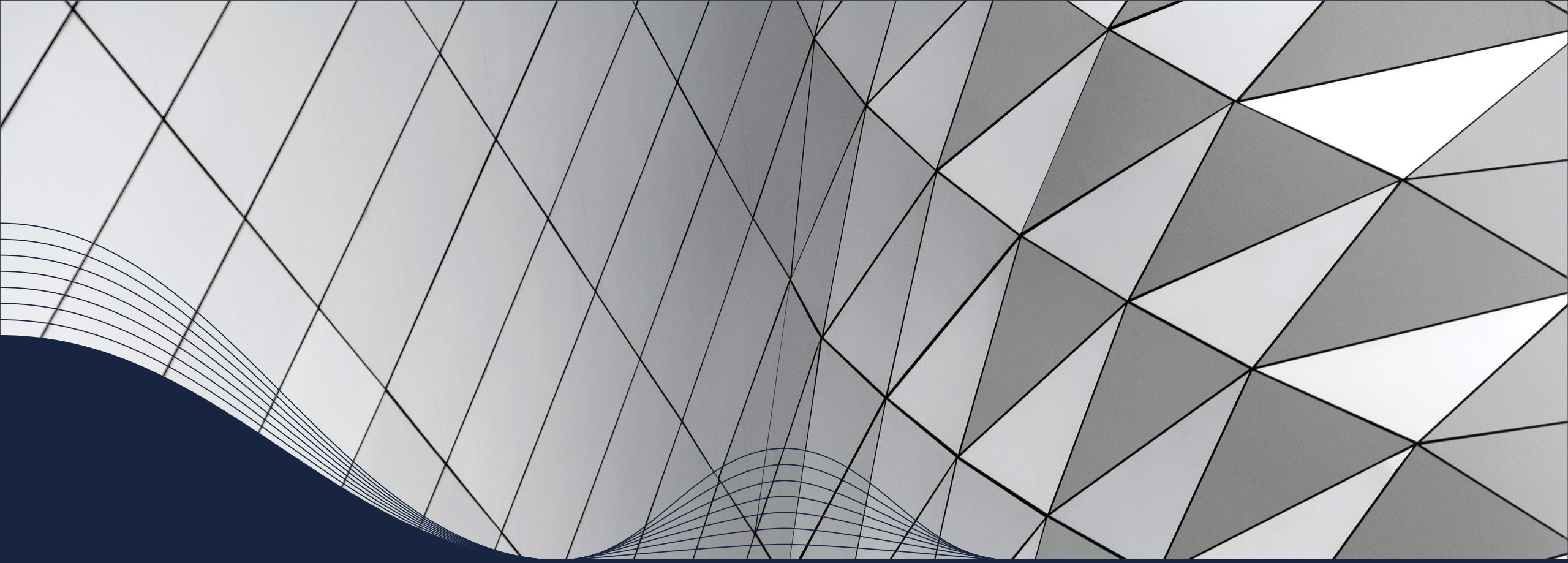


The Changing Face of Privacy Law and Future Costs of Cyber Liabilities

The Future of Cyber Risk Conference

Wednesday 24 July 2019

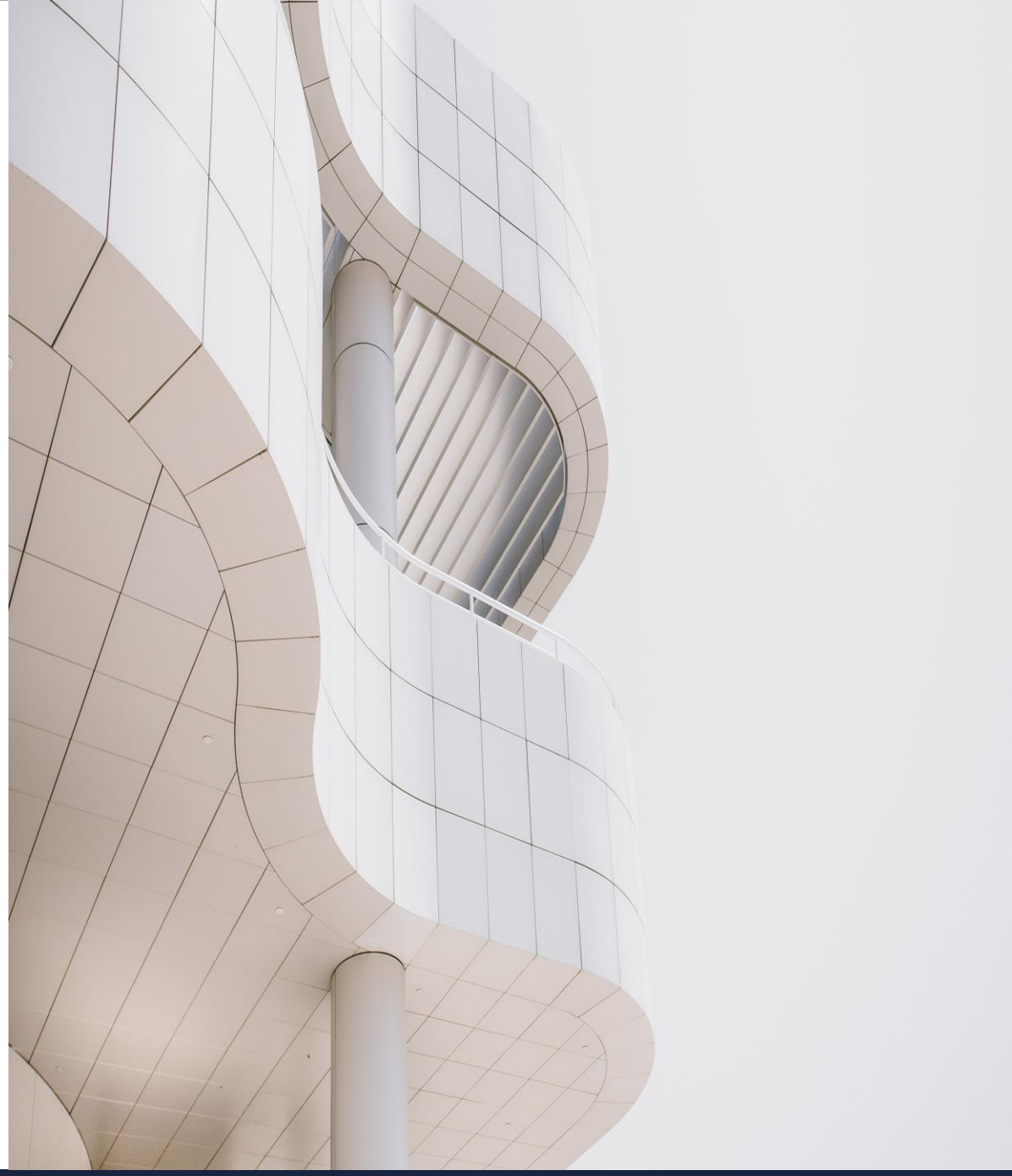
DLA PIPER

Introductions

James Clark
Senior Associate
T: +44 (0) 7885 261792
james.clark@dlapiper.com

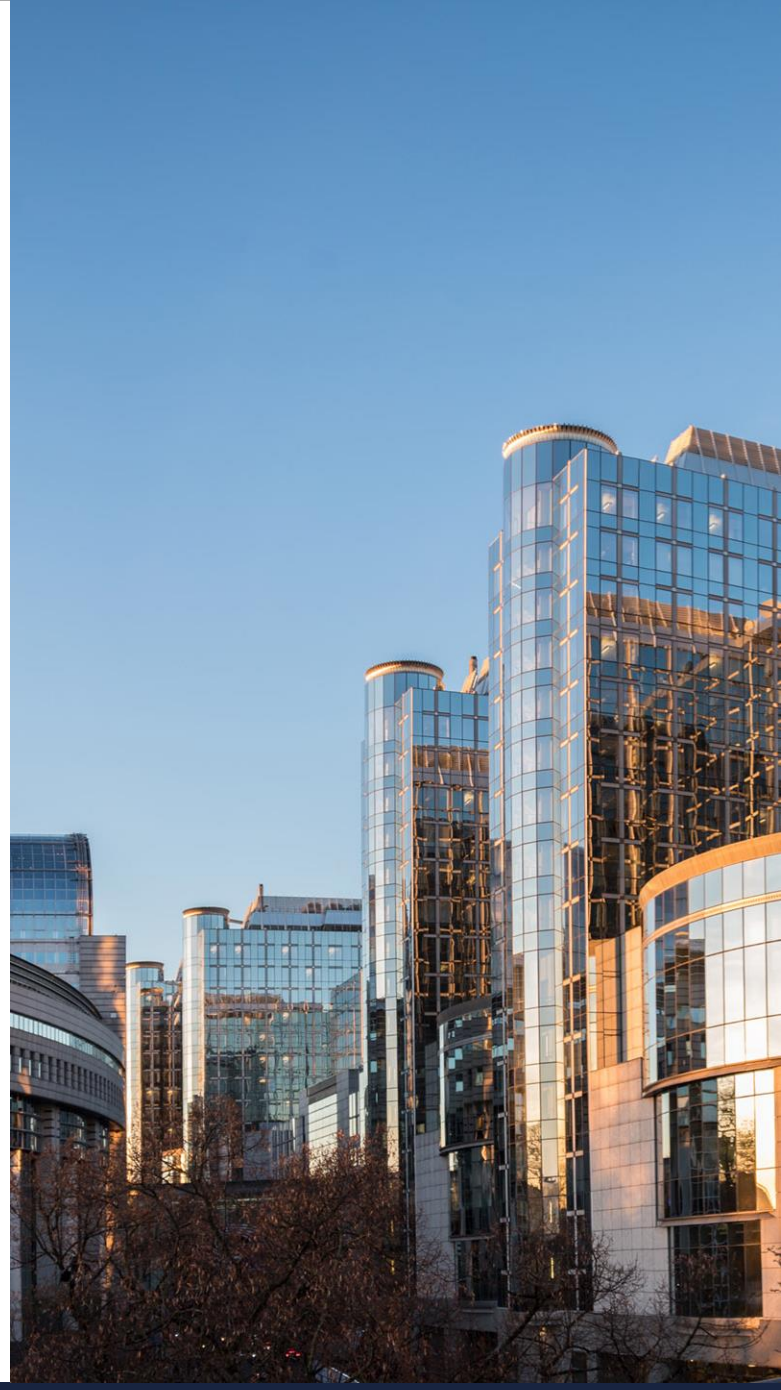
Agenda

- Introduction to three key regimes:
  - Europe (EU)
  - China
  - US
- What is the law looking to achieve?
  - Security requirements
  - Breach notification
  - Remedies
- What is the future direction of travel?
  - Current problems
  - Potential solutions



Europe (EU)

General application	*The General Data Protection Regulation* ("**GDPR**")
Sector specific	*Network and Information Systems Directive* (critical infrastructure and certain digital services providers)
	Privacy and Electronic Communications Directive (telcos and ISPs)
	PSD2; MiFID (financial services)

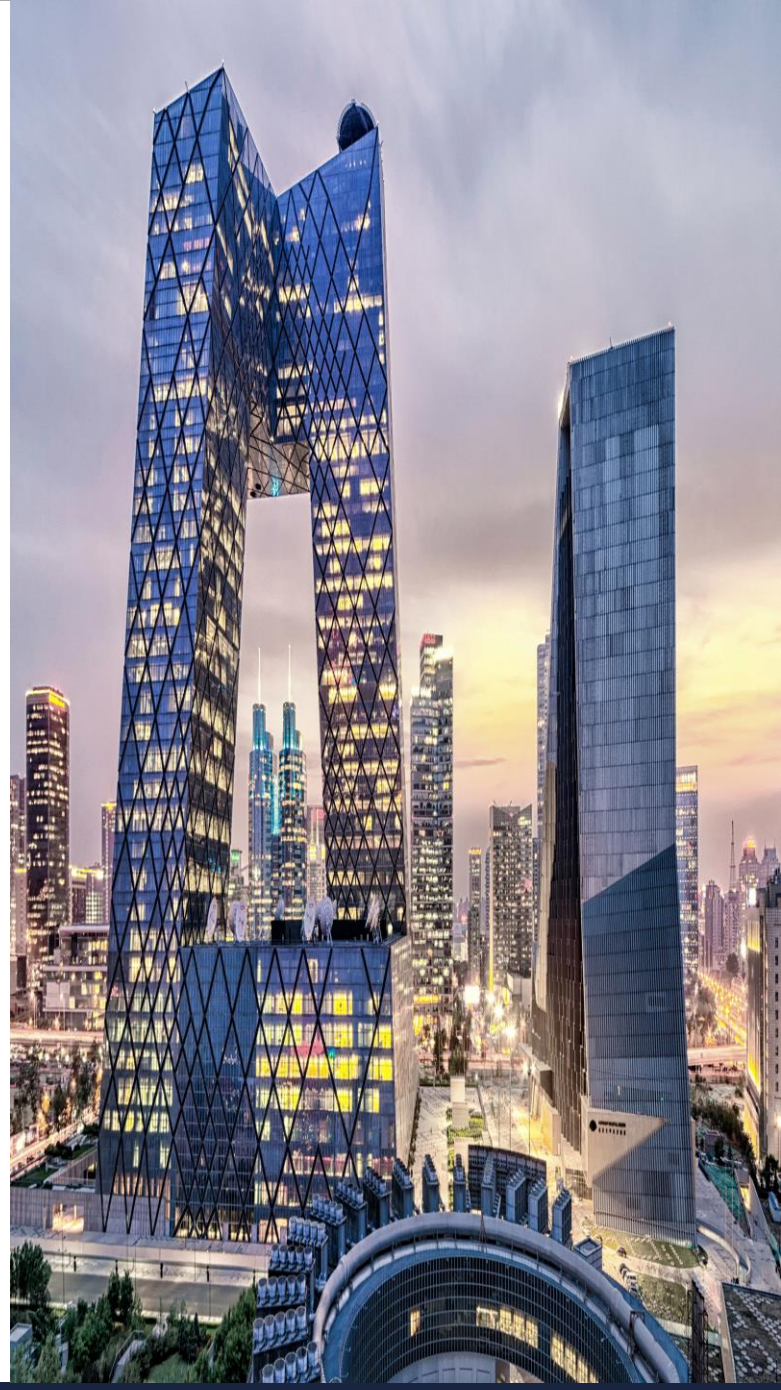


United States of America

General application	*Section 5 of the Federal Trade Commission Act* (FTC has authority to prevent and protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices)
	State specific data breach notification laws in all 50 states
	California Consumer Privacy Act
Sector specific	*HIPAA* (health sector)
	Gramm Leach Bliley Act (financial services)
	State specific and industry specific laws (e.g. *California Insurance Information and Privacy Protection Act*)

China

General application	*The PRC Cybersecurity Law*
	Decision on Strengthening Online Information Protection
Sector specific	*The Guidelines for Data Governance of Banking Financial Institutions* (financial services)
	The Provisions on Telecommunication and Internet User Personal Information Protection (telcos and ISPs)
	The PRC Consumer Rights Protection Law (consumer services)



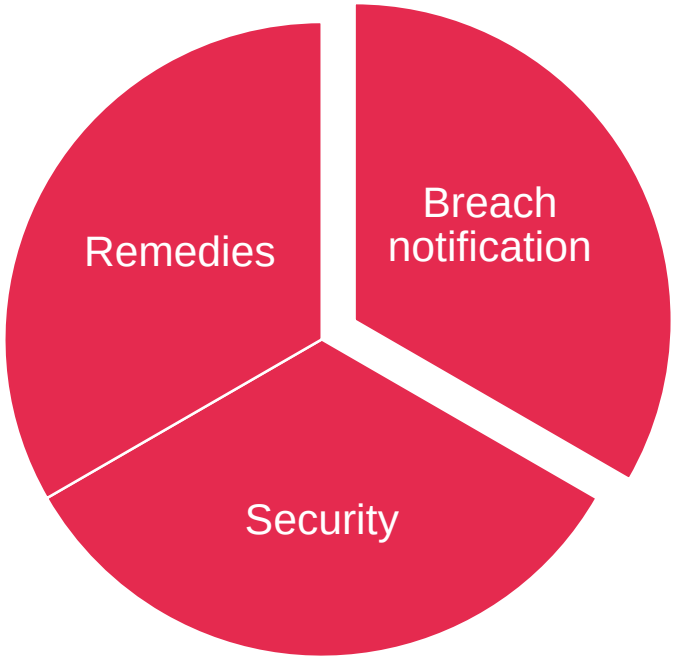
What is the law looking to achieve?
Security

Non-prescriptive; 'reasonable' standard which depends on context of information processing; for the regulated entity to determine; can evolve over time with the state of the art; may be supported by technical certifications (e.g. ISO 27001) – GDPR; FTC; CCPA

vs.

Specific minimum technical standards, tailored to sector / industry and context; require refreshing / updating – Multi-Level Protection Scheme for Information Systems (China); industry guidance under NIS (EU)?

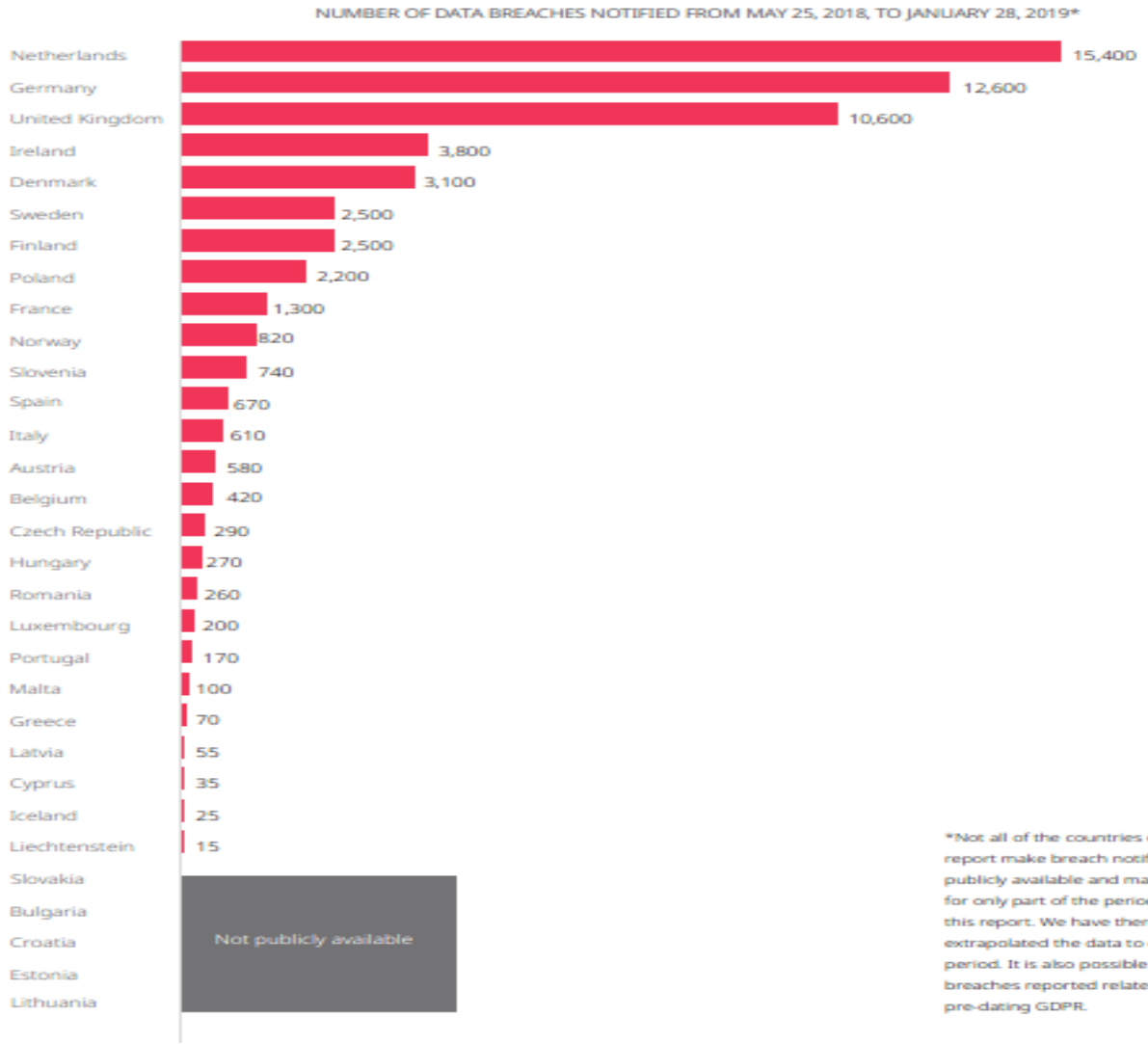
What is the law looking to achieve?
Breach notification



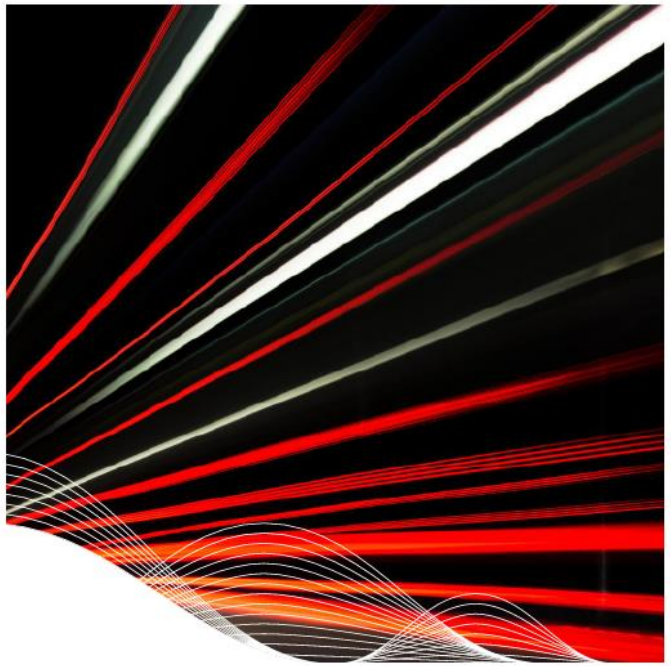
- Time limits, e.g.:
  - 4 hours (!) (PSPs under PSD2);
  - 72 hours (GDPR);
  - 60 days (HIPAA).

- Level of risk/impact triggering breach, e.g.:
  - Notification *unless* risk to rights and freedoms unlikely (GDPR)
  - No risk of harm analysis in many US states
  - No single test, multi-factor analysis (China)

- Regulator vs. impacted individuals
  - Regulator; then individuals (higher threshold);
  - Regulator and individuals simultaneously, same threshold;
  - Individuals only.



*Not all of the countries covered by this report make breach notification statistics publicly available and many provided data for only part of the period covered by this report. We have therefore extrapolated the data to cover the full period. It is also possible that some of the breaches reported relate to the regime pre-dating GDPR.



DLA Piper GDPR Data Breach Survey: February 2019

A report by DLA Piper's cybersecurity team

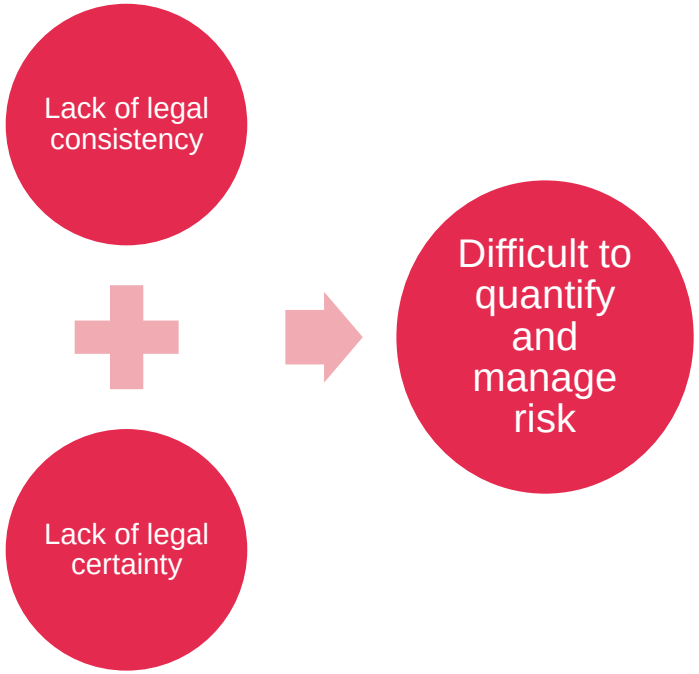
DLA PIPER

What is the law looking to achieve?
Remedies

- Fines
  - Significant fines (GDPR; HIPAA; FTC)
- Civil claims / compensation
  - Broad right of compensation (material and non-material damage) (GDPR)
  - Class action risk (e.g. based on statutory damages in CCPA)
- Criminal penalties
  - Misappropriation of data (GDPR; China)
  - Violation of privacy rule (HIPAA)

Future direction of travel

Three Connected Problems



1. *Lack of consistency between cyber laws globally.*
2. *Lack of certainty about how laws will apply, and how courts and regulators will calculate remedies / damages.*
3. *Difficult to manage risk – which standards to apply where? How much is at stake? What constitutes "reasonable" security etc?*

Future direction of travel

Potential solutions

1. Harmonising of general laws at highest level possible.
2. At the same time, industry specific guidance, codes of practice etc. to crystallise good practice in given contexts.
3. Codifying guideline amounts for damages for certain types of breach, based on data types compromised etc. (compare with personal injury, or with fine tiers under HIPAA).
4. Full acceptance of (i) data mapping; and (ii) privacy (and security) by design.
5. Greater maturity (from companies AND regulators) driving more intelligent, risk-based decisions, and targeted optimising of limited resource.

Questions

Thank you