actlaw society

MARCH MASTERY

a month of intensive cpd learning

Into The Data Breach: Navigating cyber breaches and cyber protections in contracting

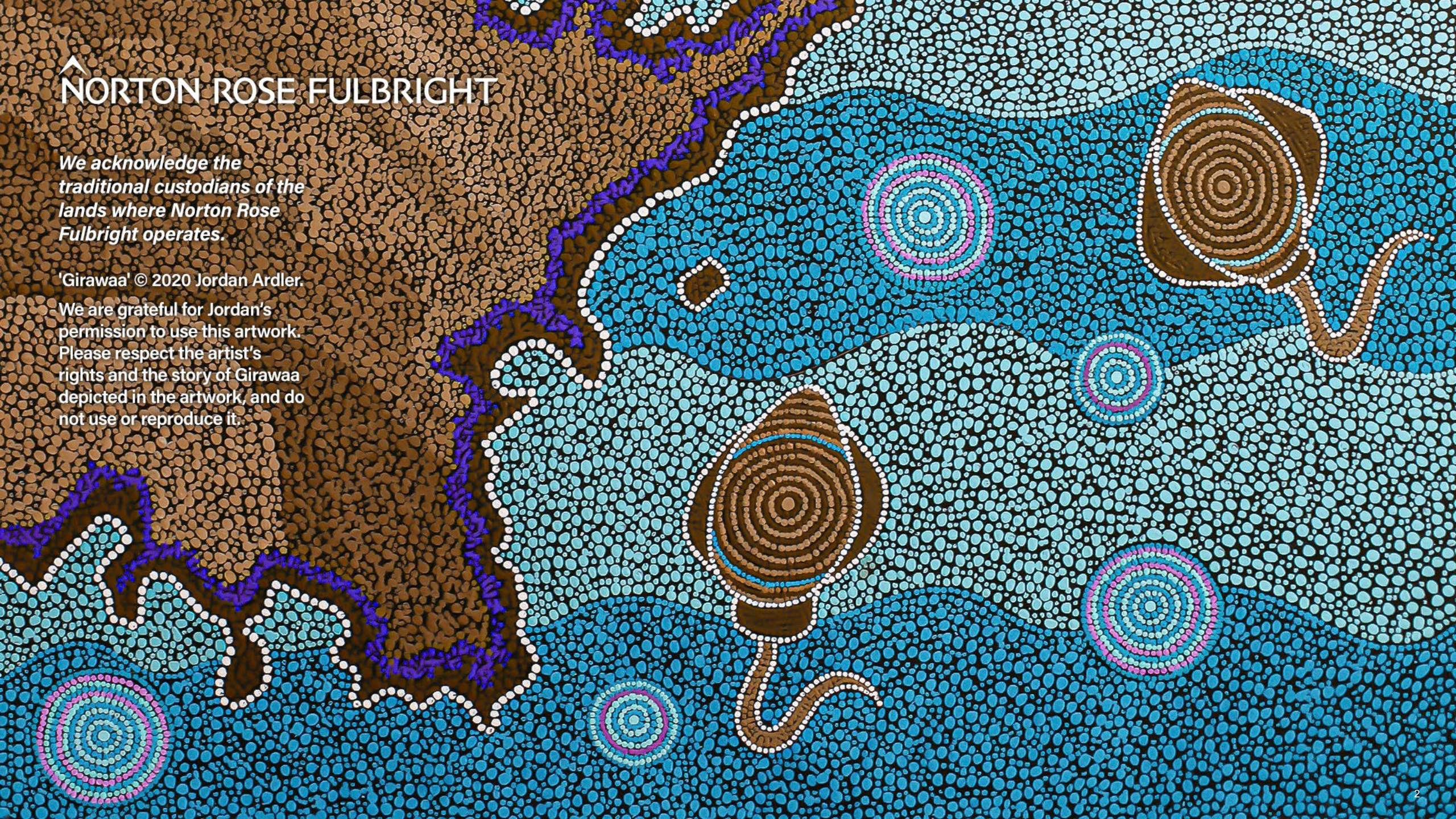
PRESENTED BY ANNIE HAGGAR & AMANDA WESCOMBE

NORTON ROSE FULBRIGHT

GOVERNMENT LAWYERS MORNING: THURSDAY 13 MARCH 2025

Lawcover

OPTEON


NORTON ROSE FULBRIGHT
We acknowledge the traditional custodians of the lands where Norton Rose Fulbright operates.
'Girawaa' © 2020 Jordan Ardler.
We are grateful for Jordan's permission to use this artwork. Please respect the artist's rights and the story of Girawaa depicted in the artwork, and do not use or reproduce it.

Your presenters

Annie Haggar

About Annie

Partner, Head of Cyber Security, Australia
– Norton Rose Fulbright Australia

Annie is a multi-award-winning cyber security lawyer who has spent 12 years as legal counsel for Accenture, including 6 years as a global legal lead for its managed security business. Annie has spent over 20 years advising government and private sector clients alike in navigating technology law, security risks, procurements, and regulations.

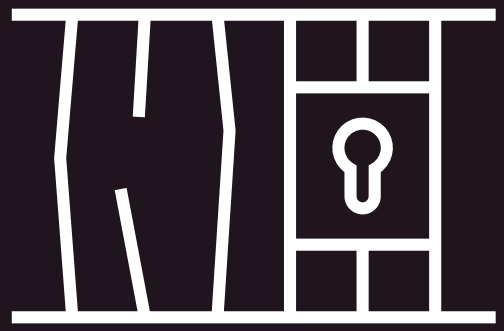
Amanda Wescombe

About Amanda

Special Counsel, Australia
– Norton Rose Fulbright Australia

Amanda is a senior cyber security lawyer and a trusted advisor to private sector and government clients. At Norton Rose Fulbright, Amanda's practice combines her legal, commercial, and governance experience to advise clients how to understand, prepare for, defend against, and recover from cyber attacks.

1. Security breaches and their impact



Types of breach

Breaches may include:
Phishing
Malware
Distributed denial of service (DDoS) attacks
Ransomware
Brute force attacks
Structured query language (SQL) injections
Supply chain attacks
Deepfakes
Business email compromise (BEC)
Advanced persistent threats (APT)

Types of impact

Impacts of a breach may include:
Data access
Data theft
Data alteration or manipulation
Data encryption
Compromised personal information
Compromised commercially sensitive information
Compromised classified information
National security threats
Loss of public trust in government
Financial loss
Corruption and bribery
Infiltrated telecommunications
Third party breaches

2. Role of government legal teams during a breach

Direct

What kind of breach?

Indirect

CISO calls

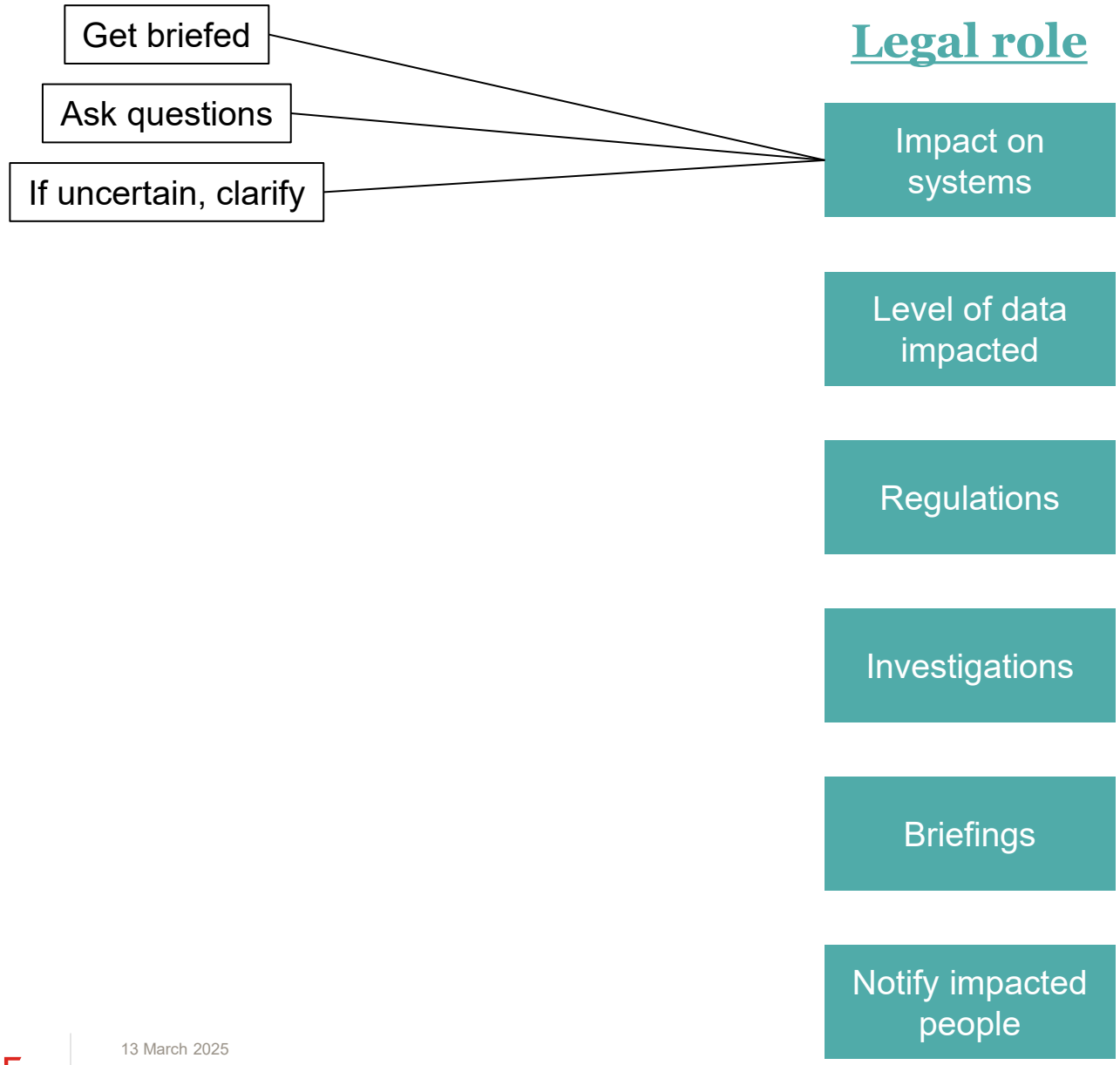
- Impact on systems
- Level of data impacted
- Regulations
- Investigations
- Briefings
- Notify impacted people

Direct What role does legal play? Indirect

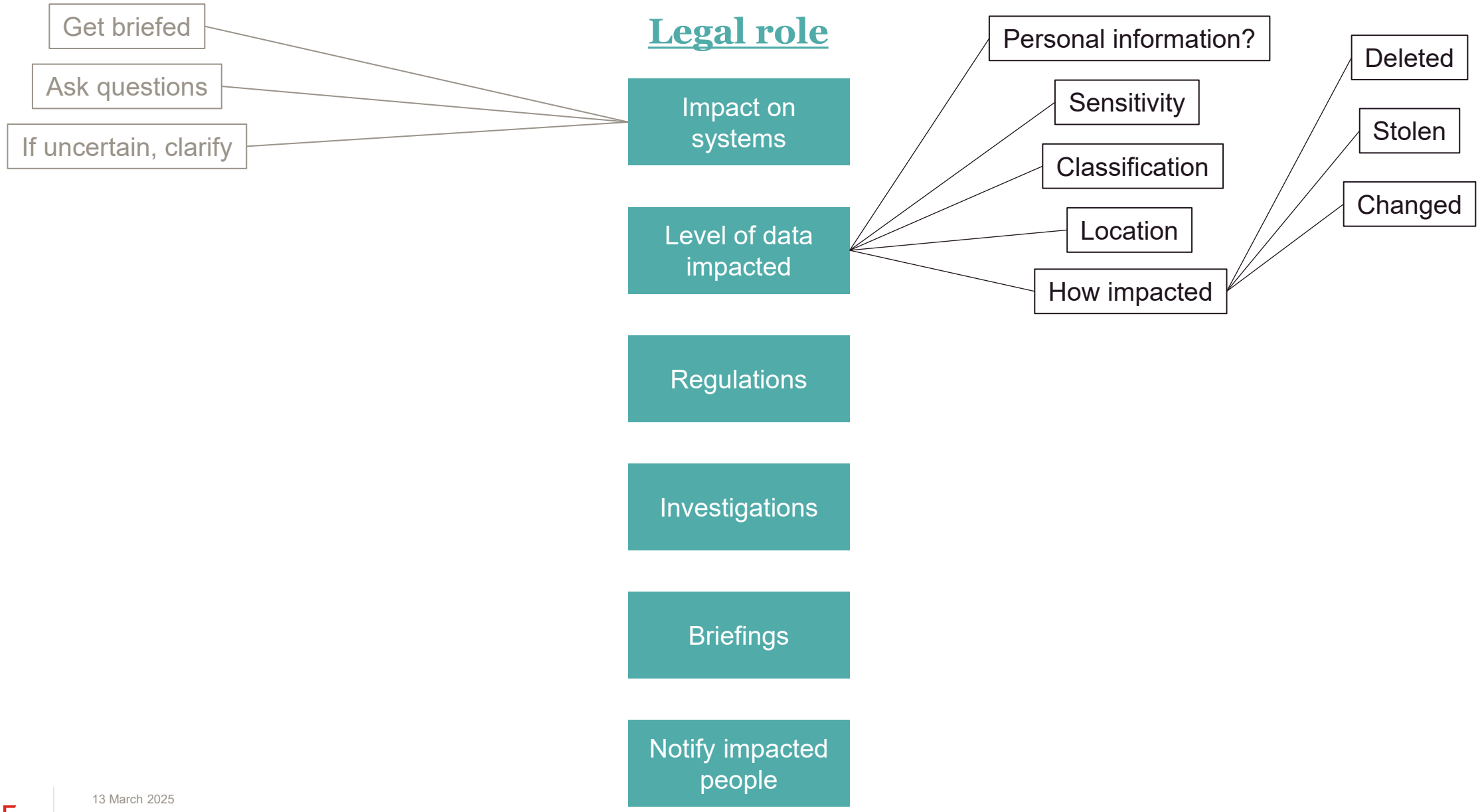
Legal role

- Impact on systems
- Level of data impacted
- Regulations
- Investigations
- Briefings
- Notify impacted people

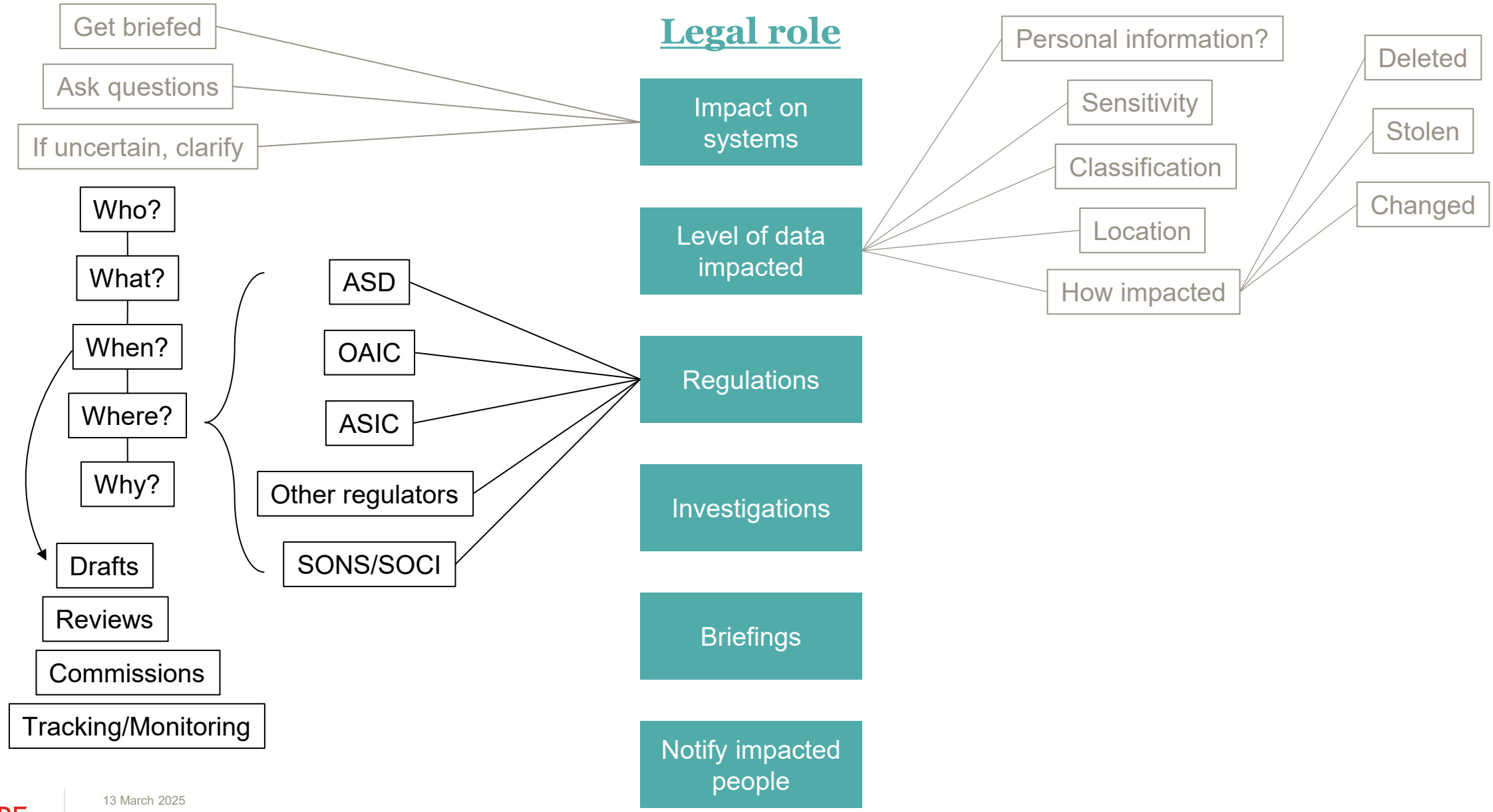
Direct What role does legal play? Indirect



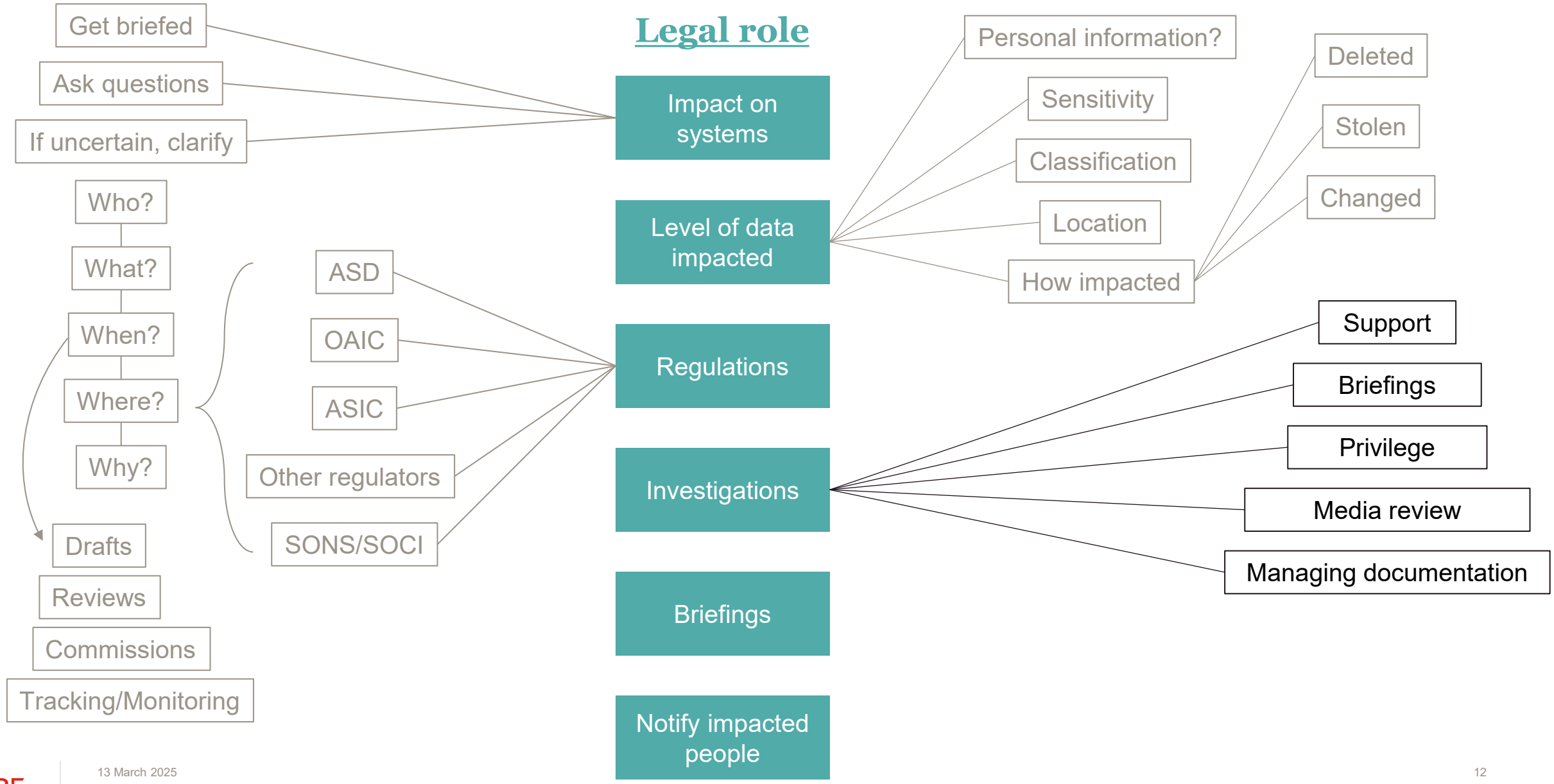
Direct What role does legal play? Indirect



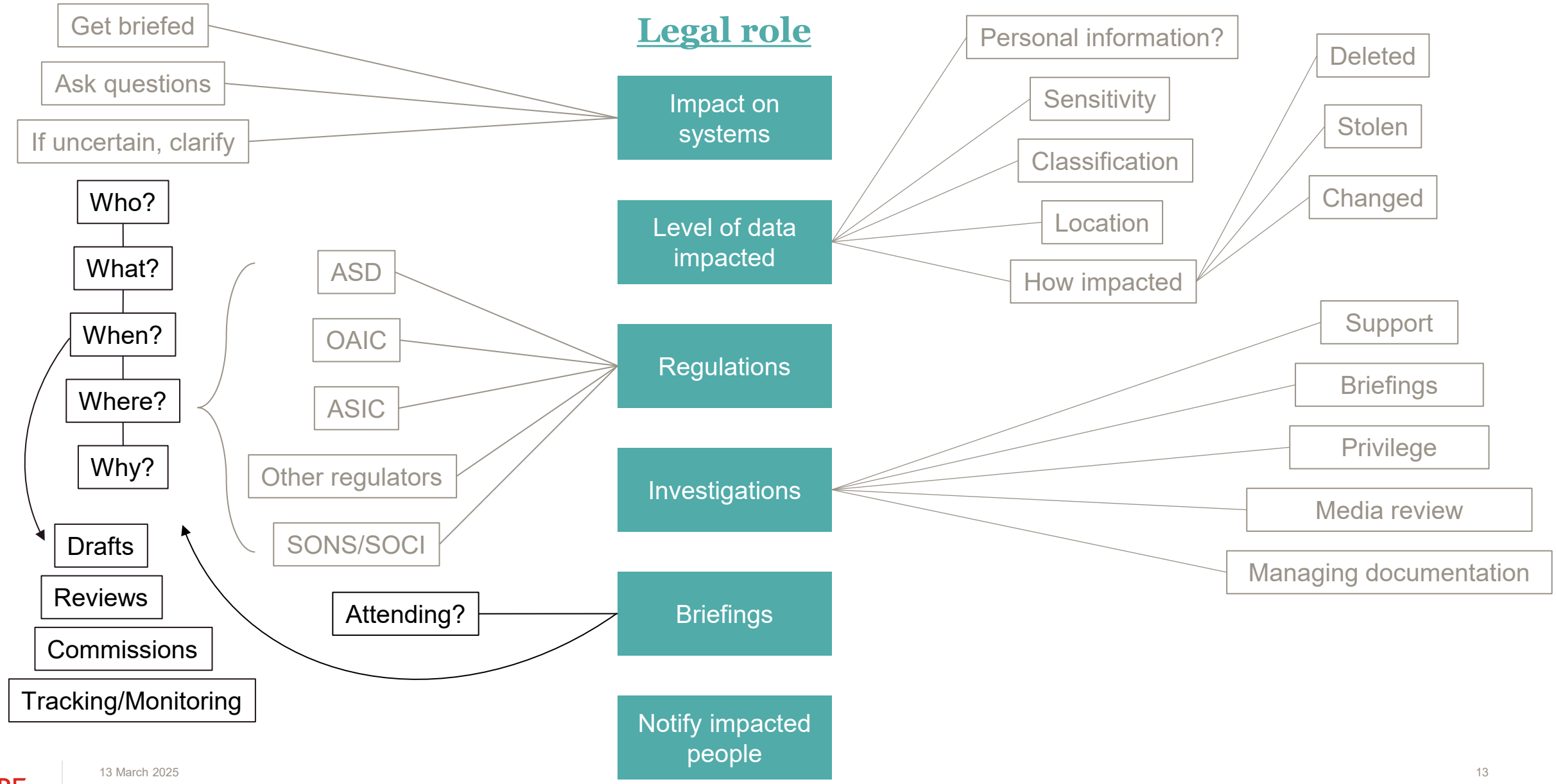
Direct What role does legal play? Indirect



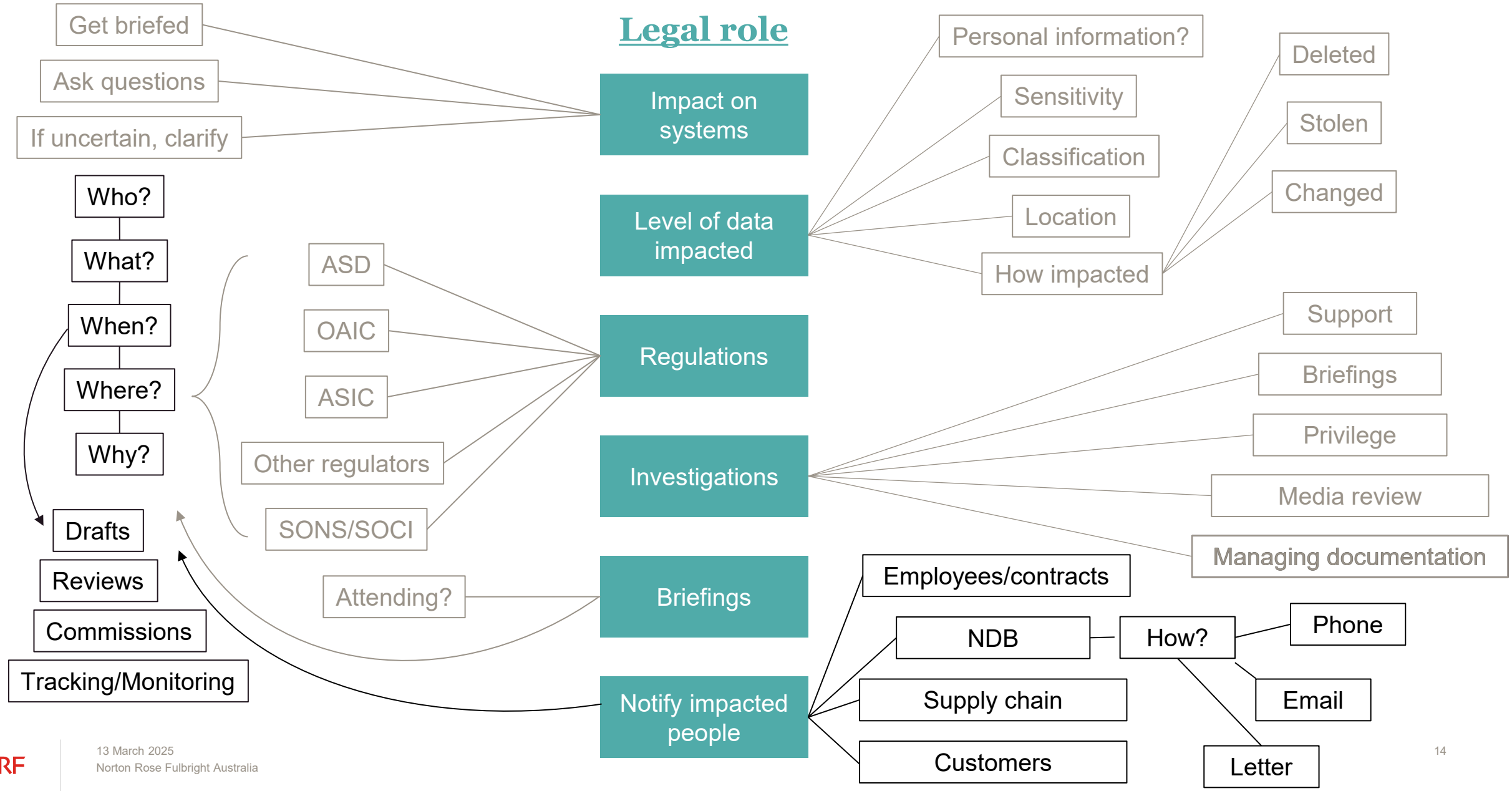
Direct What role does legal play? Indirect



Direct What role does legal play? Indirect



Direct What role does legal play? Indirect



Incident response (IR) plan for entity

- Each entity will (or should) have an IR plan and a data breach response plan
- You may wish to have a legal IR plan for how the legal team needs to respond
- Legal's IR plan needs:
  - ✓ Is there one? Where is it stored? When was it last updated?
  - ✓ Who / where are your key delegates? Where is the list? Where are their contact details stored?
  - ✓ Have you pre-drafted any regulatory communication? Are you working with the comms team?
  - ✓ Where is your contact database for all Notifiable Data Breach (NDB) recipients/supply chain contacts?
  - ✓ Has the legal team got expertise across cyber, tech and privacy areas?
  - ✓ Have your legal + technical experts been retained and cleared?
  - ✓ Have your key supply contracts got requirements to assist?
  - ✓ Who are your key decision makers for reporting a data breach?
  - ✓ Do you have a plan for responding to ransom payment demands?
  - ✓ What level of disclosure or authority has been granted to your key decision makers?
  - ✓ Will privilege attach? If so, how will you protect privilege?
  - ✓ Is there a media plan or response incorporated into the IR plan?

3. Managing the breach

What does legal do in the first 24 hours?

01

Initial notification

Legal receives a call from the technical team of a potential or actual breach

02

Fact-finding call

Legal will conduct an initial call within an hour of initial notification to gain an understanding of known facts of the incident

03

Engagement of relevant teams and onward coordination

After gaining an understanding of the incident, legal will coordinate the initial incident response

This could include:

- Involving relevant teams and counsel to advise on jurisdiction-specific issues
- Engaging service providers or external counsel as required (legal, forensics, PR, etc.)
- Providing updates to third parties as required including Notifiable Data Breach recipients/Supply chain contacts
- Obtaining threat intelligence and advise on engagement and negotiation, including any risks which may arise
- Arranging an all-parties conference call

04

Conference call

Within a few hours, all involved parties will attend a call, align on next steps, confirm what resources are required, and develop an action plan to respond to the incident

05

Contacts list

Following the conference call, legal will circulate a list of all parties involved in an incident and the contact details of each to allow for ease of communication and coordination

06

Further conference calls

The exact nature of further conference calls will be dependent on the specific facts of the incident

First 48 hours

Cyber workstreams

These are the most common workstreams needed in a cyber incident response that the legal team must be aware of when responding to a breach. Where possible, each stream is established under privilege to protect findings and advice*

FORENSICS	Engagement with the forensics team (DFIR) to gather analysis, earliest date of activity, most recent date of activity, visibility coverage, tactics, techniques and procedures (TTPS), information for establishing chronology (for later legal activities), and containment options and certainty level
THREAT ACTOR NEGS	Not always required – dependent on attack type. Working with Threat Actor Negotiator in accordance with department-endorsed policy, supporting negotiation strategy, legal risk and due diligence assessment and engagement with senior staff responsible for ransom payment policies (where applicable)
LEGAL	Law enforcement/security agency engagement, contractual and regulatory notices. Protection of communications (privilege), strategy and coordination for inter-department breaches (multiple law enforcement and regulatory engagements), protection and containment of incident evidence, notification to impacted parties (see separate stream). Advice on department's legal obligations including obligations to meet payroll, contractual delivery, notification and impacts (criminal liability, fines, etc) of not being able to meet obligations due to incident. Data breach assessment and advice
RECOVERY & REMEDIATION	'Path to green' advice and support Capturing for future legal/regulatory purposes all actions taken in recovery and remediation. Recovery chronology for legal claims and defence purposes
COMMUNICATIONS	Internal and external communications legal oversight. Working with Crisis communication team, advising on communication strategy, clearing communications, supporting key communications activities (press releases, media appearances etc)
POST INCIDENT	Closure documentation and reporting. Coordination of lessons learned under privilege, including call with all key stakeholders. Review of all forensic recommendations and 'lessons learned' documentation
E-DISCOVERY	Protection of evidence. Analysis of forensic reporting on data for regulatory reporting and notification obligations. Analysis of impact on contractual and other obligations. Other activities depending on scope and nature of cyber incident
NOTIFICATION	Notification strategy including management of multiple jurisdictions and regulators. Analysis of impacted data and groups for notification based on regulatory obligations. Preparation of template notices to impacted groups (customer entities, individuals, suppliers). Coordination of notification and management of incoming queries and responses

*Privilege may not be established and may be lost depending on how the communications and documents are managed and the conduct of the parties

Cyber legal activities

Pre-incident	During incident	Ongoing Regulator engagement	Third party exposure
Cyber readiness materials **[1]**	Investigation terms of reference (ToR)	Advice on department strategy	Advice on government strategy (including inter-department privilege)
Regulatory response pack **[2]**	Engagement of vendors	Responding to information requests	Triage / responding to pre-action correspondence
Pen-tests / audits **[3]**	Negotiation and payment	Managing reporting	Representation in formal claims / class actions
Training **[4]**	Forensic oversight	Representations in response to proposed / actual enforcement action	Advising on actions against service providers
Tabletops / scenarios **[5]**	Fact finding		
Feedback loop **[6]**	Advice on forensic reporting		
	Intelligence services engagement		
	Strategic advice on containment		
	Documenting containment		
	Cyber review and analysis		
	Comms / PR engagement		
	Notification strategy		
	Regulatory notifications		
	Data subject notifications		

Key:

- Privilege protections recommended*
- External / internal teams to feed-in technical / factual info (critical)
- External / internal legal

Notes:

[1] Review/Preparation of Cyber Policies, Incident Response Manuals and Ransom Response Plans
[2] Undertake a regulatory response readiness assessment under privilege
[3] Avoiding problematic audit trails in anticipation of post-incident regulatory investigations / follow-on litigation
[4] Training for core response team and other key stakeholders
[5] Preparation of tabletops and scenarios and delivering alongside other stakeholders. Legal team to deliver specific scenarios tailored to jurisdiction
[6] Regular feedback loop of lessons learned from other incidents

***Privilege**

It may not be possible to establish and maintain privilege over all elements of the incident. However, if correct protocols are implemented and maintained, arguments can be made that privilege should apply

4. Cyber breaches and privilege

Cyber incidents and privilege in Australia

Why is it important to protect privilege?

- Protection from disclosure
- Supports defence of proceedings (not discoverable)

Why is it important to protect privilege?

- Legal professional privilege (or client legal privilege) attaches to confidential communications for the ***dominant purpose of legal advice / for use in existing or anticipated litigation***
- Without prejudice privilege
- Common interest privilege
- Self-incrimination privilege

What are the elements of legal professional privilege?

1. **Confidential communications:** The communication must be confidential
2. **Legal advice:** The communication must be for the dominant purpose of seeking or providing legal advice
3. **Between lawyer and client:** The communication must be between a lawyer and their client, or between the client and a third party, if the third party is acting as an agent of the lawyer or client

Challenges to establishing privilege in Australia over cyber investigations

- **Singtel Optus Pty Ltd v Robertson [2024] FCAFC 58**
- **Robertson v Singtel Optus Pty Ltd [2023] FCA 1392**
- Federal Court of Australia on appeal confirmed original court decision that the forensic report was not protected by legal professional privilege
- Beach J (primary judgement [120]-[123]) noted there were multiple purposes for procuring the report, including:
    I. providing legal, litigation, or regulatory advice for a proceeding;
    II. identification of the circumstances and root causes of the cyber attack for management; and
    III. review of Optus management's policies and processes in relation to cyber risk

- Beach J stated ***privilege may attach*** to factual investigations carried out by lawyers as well as to reports prepared by non-lawyers
- However, the investigation and reports must have the ***dominant purpose of providing legal advice*** to the client

Singtel Optus Pty Ltd v Robertson [2024] FCAFC 58

> *"Channeling material through lawyers or having lawyers make the retainer,* ***belatedly, cannot cloak material with any privilege that it did not otherwise have****. And the fact that the SOPL Board's objectives as set out in the circular resolution of 11 October 2022 are replicated in the main retainer letter* ***does not change the reality of the Board's or the CEO's purpose(s)*** *for engaging Deloitte to undertake an external review, which I am not satisfied was a dominant legal purpose" (at [161])*

Other reasons the claim of privilege was denied:

- Justice Beach did not accept that the General Counsel (and Company Secretary) Mr Kusalic was always acting with a legal purpose in mind, as he considered that Mr Kusalic was communicating with the Board in both his capacity as company secretary and as general counsel
- Justice Beach considered there were multiple purposes for which the Deloitte Report was commissioned, and that the evidence did not establish that it was procured for the dominant purpose of Optus obtaining legal advice or for use in litigation or regulatory proceedings [83]
- Deloitte was engaged to commence the investigation prior to the engagement of the legal advisors, or their coverage of the investigation with privilege

How best to protect privilege?

- **Mark communications as confidential:** Clearly label communications as "confidential" and "privileged"
- **Limit distribution:** Restrict the distribution of privileged communications to those who need to know
- **Maintain confidentiality:** Ensure that the confidentiality of the communication is maintained at all times
- **Legal advice only:** Ensure that the communication is strictly for the purpose of legal advice and not for other purposes
- **Privileged communication channels** – email chains started by the legal advisors
- **Separate, outside, legal counsel** – using in-house teams can put privilege at risk, especially where legal counsel performs multiple roles
- **Engagement of experts by legal counsel** – using tripartite agreements, external legal counsel engage and instruct the experts. Clients provide payment directly
- **Instruction of the experts by legal counsel** for the purposes of legal advice – instructions are provided to the experts by legal counsel, following instructions from the client

5. Notifying Third Parties

Who needs to be notified?

Australian Cyber Security Centre (ACSC)

- Commonwealth's lead agency for cyber security under the Australian Signals Directorate (ASD)
- Services include:
  - Australian Cyber Security Hotline (24/7)
  - Publishing alerts, technical advice, and notifications on significant cyber security threats
  - Cyber threat monitoring and intelligence sharing with partners
  - Technical advice and assistance to help Australian entities respond to cyber security incidents
- Critical infrastructure – report within 12 hours of becoming aware of an incident with a 'significant impact', 72 hours for an incident with a 'relevant impact'
- Report a cyber security incident | Cyber.gov.au

Office of the Australian Information Commissioner (OAIC)

- Australia's national privacy and information access regulator
- Performs:
  - Investigations
  - Handling of complaints
  - Monitoring of agency administration
  - Education to the public, organisations and agencies
- Responsible for the Notifiable Data Breaches (NDB) scheme – entities subject to the scheme must report 'as soon as practicable' any eligible data breach
- Report a data breach | OAIC

ACT Government Cyber Security Centre (ACT CSC)

- Sits under the Chief Minister, Treasury and Economic Development Directorate (CMTEDD)
- Responsible for developing ACT ICT security policy, standards, strategies and protecting ACT ICT infrastructure
- Reported to for:
  - Inappropriate or prohibited uses of ICT
  - Data spills, breaches or leaks
  - Observed ICT system vulnerabilities
  - Major ICT incidents including outage or vandalism of a website
- Report 'as soon as possible' after becoming aware of a security incident
- Contact - cyber.security@act.gov.au

Source: *ACT Government Cyber Security Policy; Report a data breach | OAIC; Report a cyber security incident | ACSC; ACT CSC Acceptable ICT Use Policy 2024*

Notifiable data breaches – key concepts

- What is a data breach? → unauthorised access, unauthorised disclosure or loss of personal information
- What is an eligible data breach? → a data breach that is likely to result in serious harm to an individual
- What is serious harm? → includes physical, psychological, emotional, financial or reputational harm
- Relevant matters in assessing “serious harm” include:
  - the kind of information
  - the sensitivity of the information
  - whether the information is protected by security measures and the likelihood of overcoming them
  - the persons who have or could obtain access to the personal information
  - the nature of the harm

Source: *Federal Register of Legislation - Privacy Act 1988*

What must you do if there is an eligible data breach?

- Are there reasonable grounds to *suspect* there may have been an EDB?
  - If so, carry out a reasonable and expeditious assessment of whether there are reasonable grounds to *believe* there is an EDB and take all reasonable steps to complete this within 30 days
- If there are reasonable grounds to *believe* there has been an EDB, the entity must, as soon as practicable, prepare a *statement* which is given to the Commissioner that sets out:
  - identity and contact details of the entity
  - description of the EDB
  - particular kinds of information concerned
  - recommended steps that individuals should take in response to the EDB
- Following notification to the Commissioner, the entity must as soon as practicable:
  - if possible to notify the contents of the statement to all individuals to whom the information relates, take reasonable steps to do so
  - if possible to notify the contents of the statement to all at-risk individuals, take reasonable steps to do so
  - publish the contents of the statement on the entity's website and take reasonable steps to publicise it

Source: *Federal Register of Legislation - Privacy Act 1988*

What exceptions apply?

- Have you taken remedial action in time?
  - If there is a data breach that is likely to result in serious harm, but the entity takes action before the harm is suffered, the data breach is taken to never have been an EDB
- Are 2 or more entities involved in the EDB?
  - If more than one entity holds personal information that was compromised in an EDB, only one entity needs to prepare a statement and notify individuals about the data breach
- Is the entity an enforcement body and would notification prejudice enforcement-related activities?
  - An enforcement body does not need to notify individuals about an EDB if its CEO believes on reasonable grounds that notification would be likely to prejudice an enforcement-related activity
- Is notification inconsistent with secrecy provisions?
  - If another Commonwealth law prohibits or regulates the use or disclosure of information, then an agency needs to consider whether notification of the EDB would be inconsistent with the secrecy provision

Source: *Federal Register of Legislation - Privacy Act 1988*

Questions

nortonrosefulbright.com

Law Society of the Australian Capital Territory
Phone 02 6274 0333 | memberconnect@actlawsociety.asn.au

actlawsociety.asn.au