

Data Privacy and Security in the Digital Economy

Can Privacy Thrive in the Digital Economy?

Biggest Data Breaches in 2017

EQUIFAX



UBER

YAHOO!

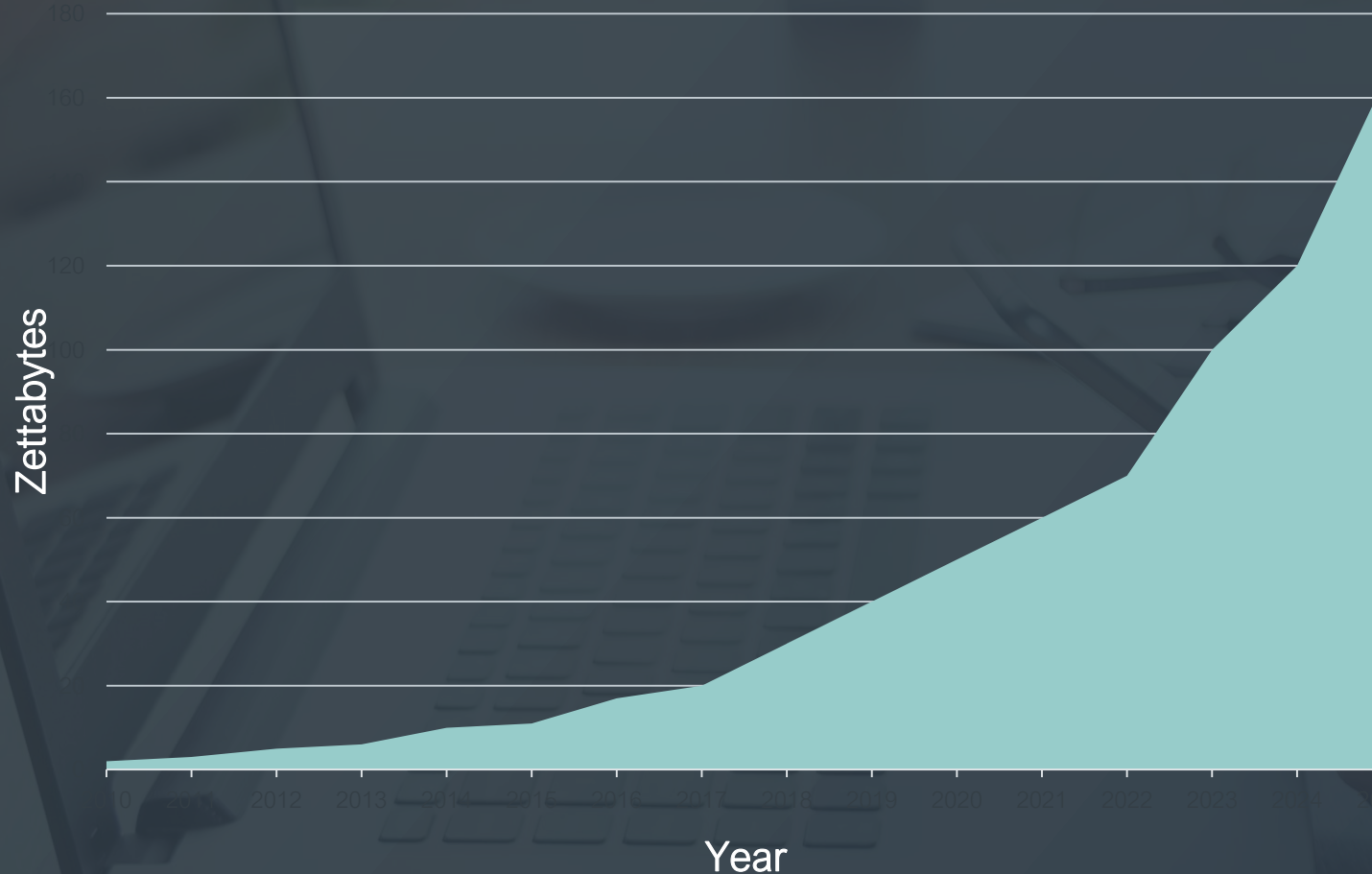
verizon^v



**We are
in the
Data
Age**



Annual Size of Global Datasphere



It is estimated that by 2025 the world's digital data will grow to one hundred and sixty three zettabytes.

DATA CREATED

Source: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

Sponsored by Mariner Innovations



Discussion Topics

Challenges in Safeguarding Privacy Rights
How GDPR Brings Privacy to the 21st Century
Privacy Enhancing Best Practices and
Technologies




Challenges in Safeguarding Privacy Rights

Sponsored by Mariner Innovations

Balancing Free Flow of Information with Privacy and Security Rights





“eCommerce is only possible if consumers are confident that they can transact in a secure manner, laws, regulations and administrative measures for the protection of personal information of users engaged in electronic commerce.”

Source: CETA

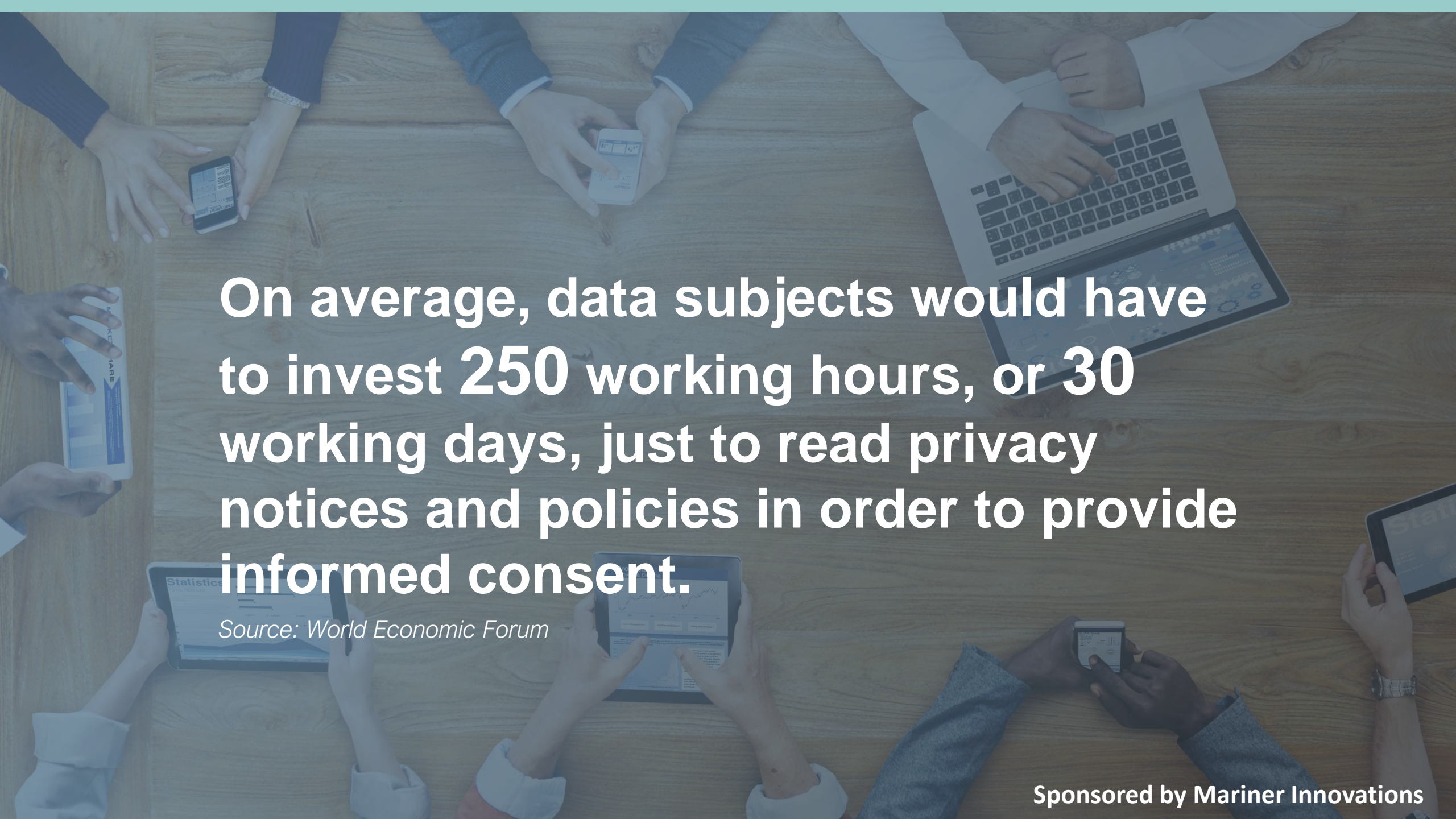


Data Privacy is a Fundamental Human Right

Sponsored by Mariner Innovations

The OECD Fair Information Practices

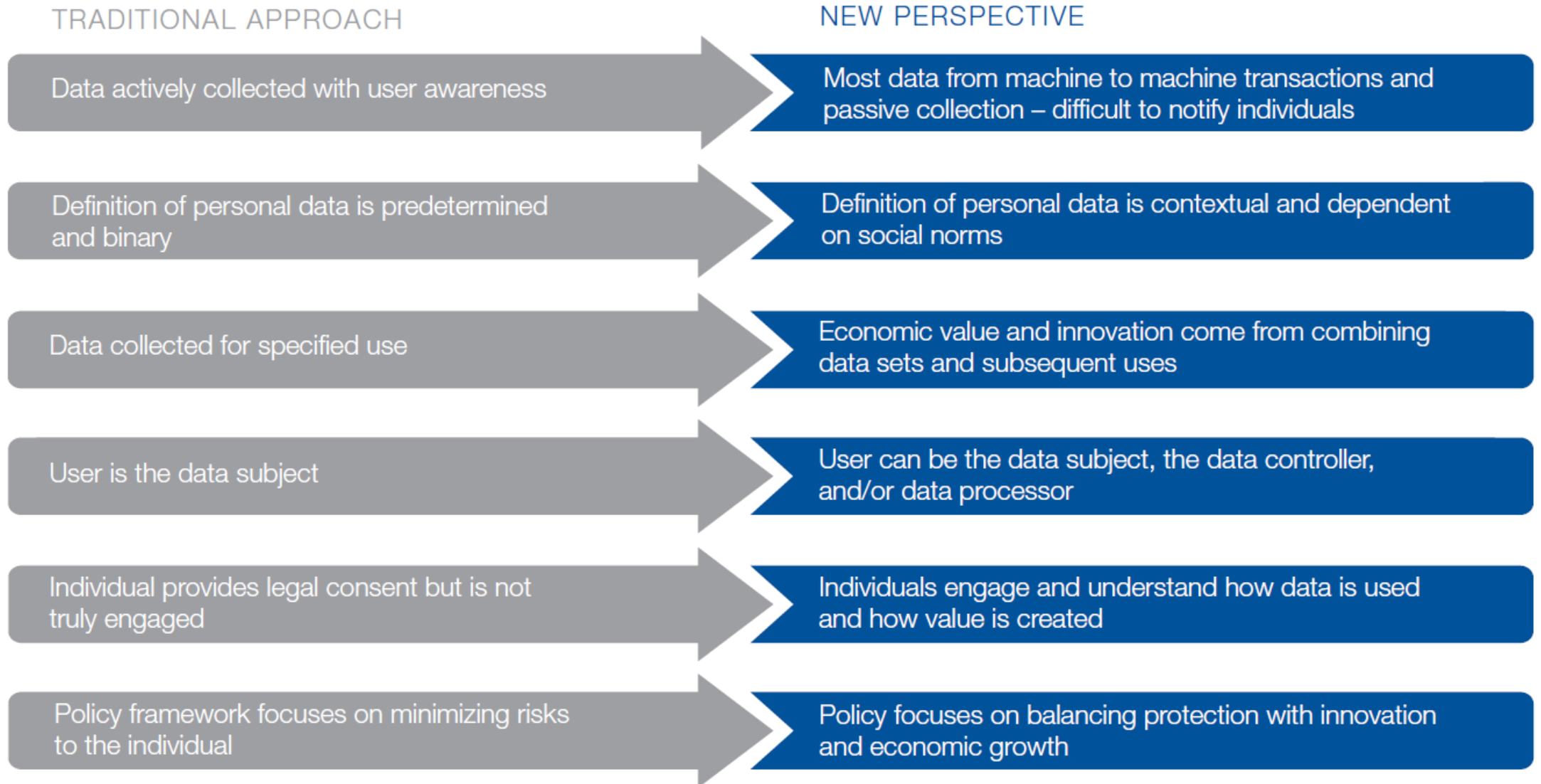
Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate knowledge or consent of the individual
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose
Purpose specification	The purposes for the collection for personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means or learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of person information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.



On average, data subjects would have to invest **250** working hours, or **30** working days, just to read privacy notices and policies in order to provide **informed consent.**

Source: World Economic Forum

Figure 2: New perspectives on the use of data



Study found that it is possible to re-identify 87% of the US population by simply combining three data points – zip code, gender and date of birth.

Source; Carnegie Mellon University

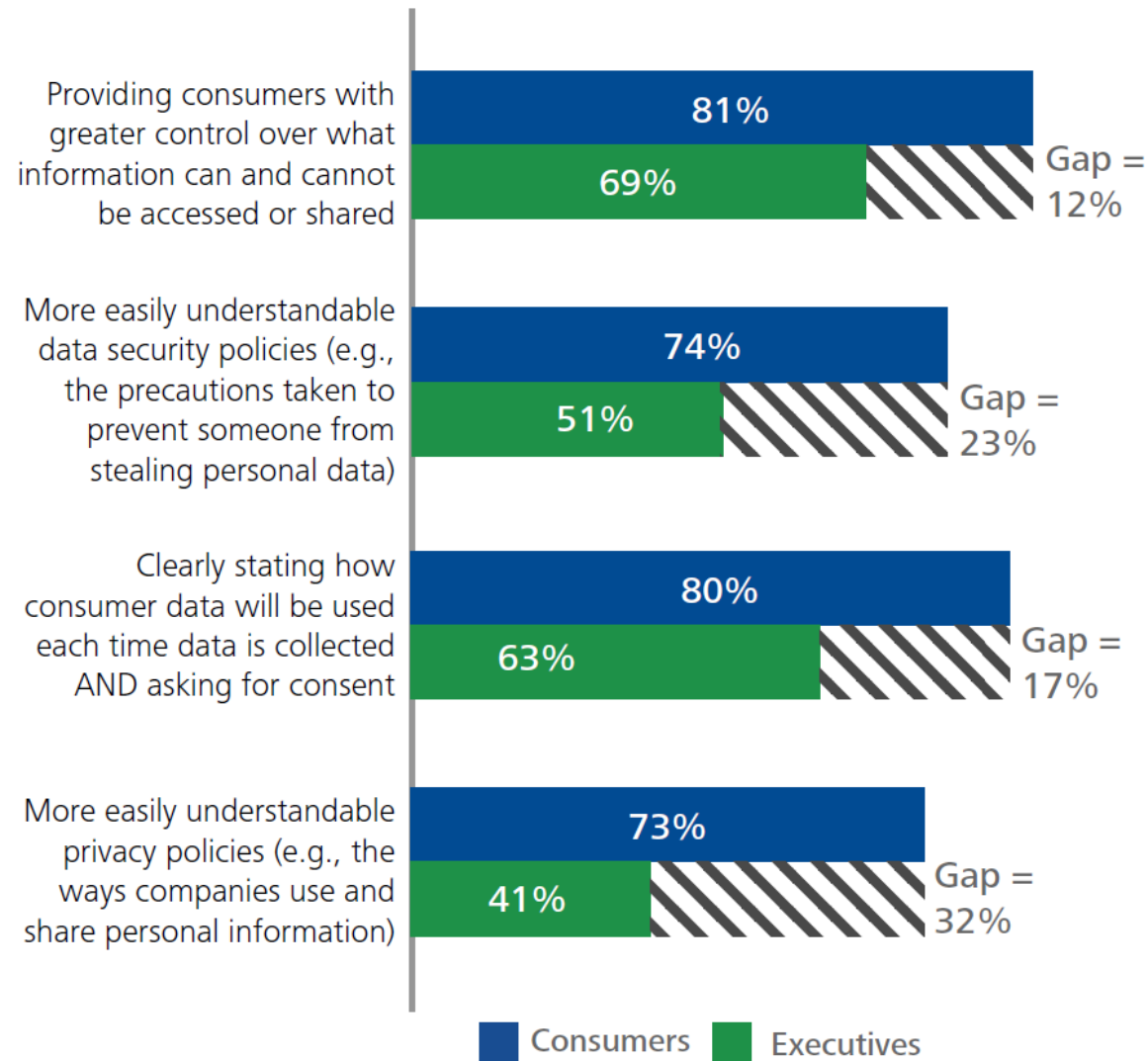
The New York Times were able to identify a single individual in a list of web search queries released by AOL, using the searches that the individual had made over a three month period.

Netflix study researchers were able to individual Netflix users in an anonymized dataset by knowing when and how users rated as few six movies”

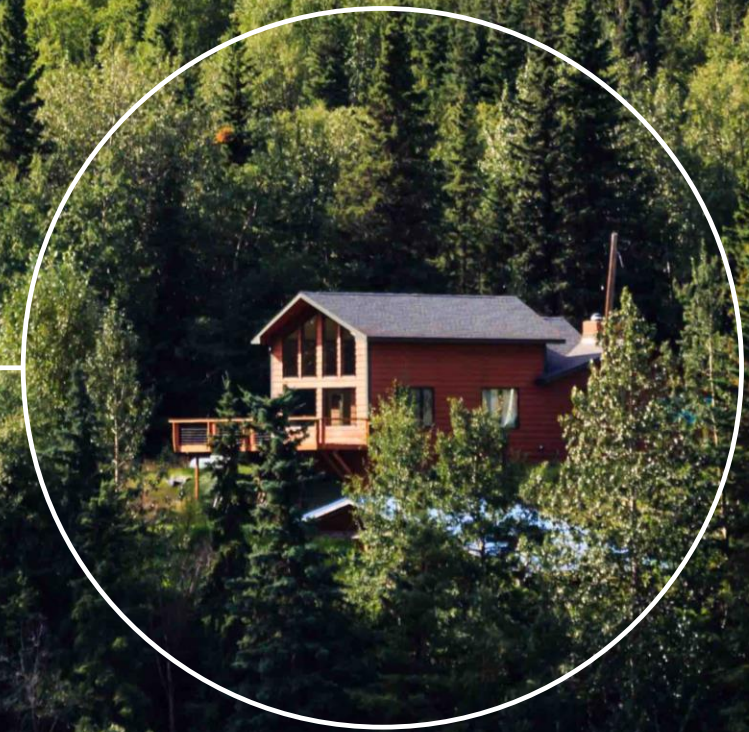
Source: Office of the Canadian Privacy Commission

The New York Times were able to identify a single individual in a list of web search queries released by AOL, using the searches that the individual had made over a three month period.

The Privacy Gap



Living off the Grid?





How GDPR Brings Privacy Rights into the 21st Century

Sponsored by Mariner Innovations

The image shows the acronym 'GDPR' in a large, bold, blue sans-serif font. Each letter is filled with a dark blue color and contains several yellow five-pointed stars, similar to the stars on the European Union flag. The 'G' has three stars, the 'D' has three stars, the 'P' has three stars, and the 'R' has three stars. The stars are positioned at various points within the letters, such as the top, bottom, and sides.

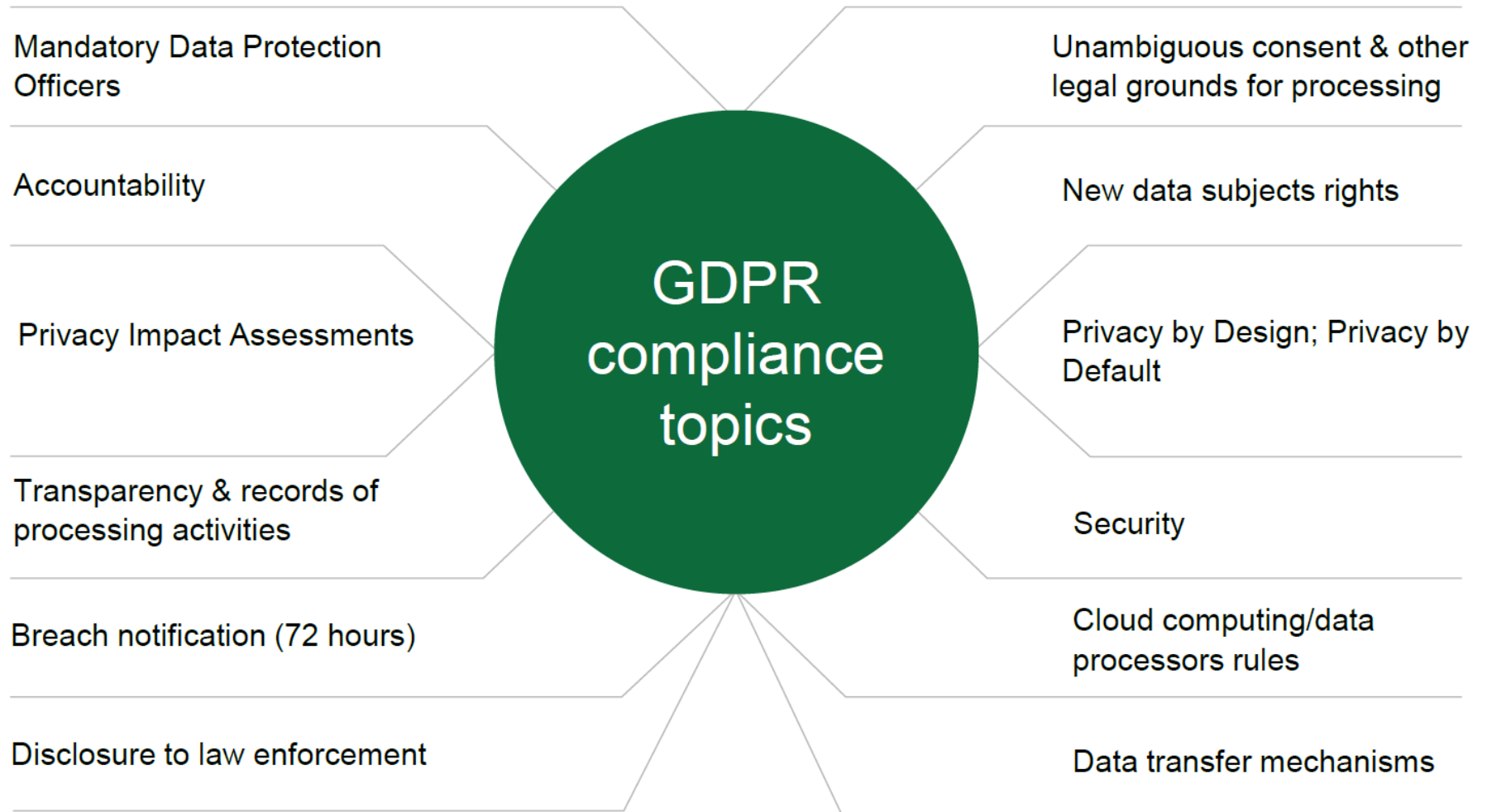
General Data Protection Regulation

Implications

- 1 Expanded jurisdiction
- 2 Higher bar for the protection of privacy rights
- 3 More onerous enforcement mechanisms
- 4 More rigorous accountability and compliance requirements

GDPR overview

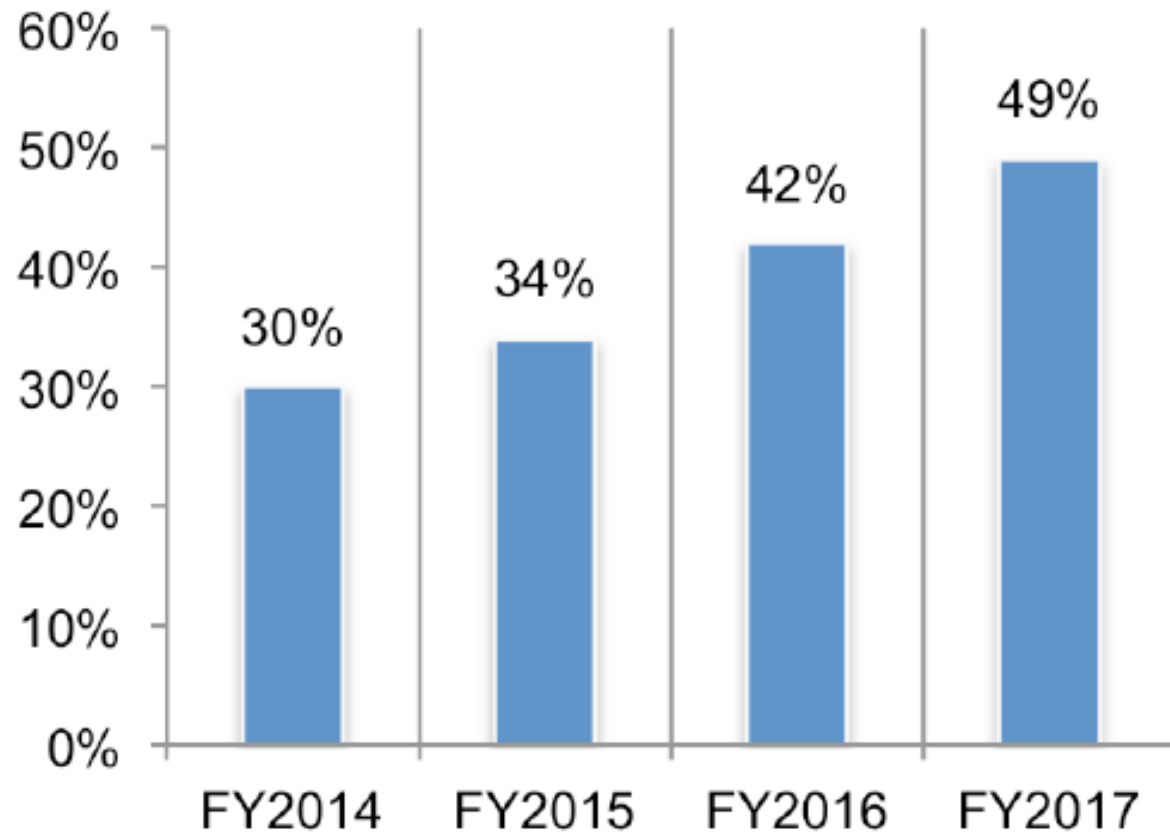
Strictest data protection law in the world...



Breach Response Readiness

Figure 1. How effective is your company's data breach response plan?

Very effective and Effective responses combined



Stringent Enforcement

- 1 Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
- 2 This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.
- 3 There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment.



Privacy Enhancing Best Practices and Technologies

Sponsored by Mariner Innovations



Privacy by Design Principles: A Canadian Innovation

Privacy by Design Foundational Principles



Privacy



Security

Respect and protect personal information

Enable and protect activities and assets
of both people and enterprises

1. Proactive not Reactive; Preventative not Remedial

Anticipate and prevent privacy-invasive events before they happen. Do not wait for privacy risks to materlize

Begin with the end in mind. Leverage enterprise architecture methods to guide the proactive implementation of security

2. Default Setting

Build privacy measures directly into any given ICT system or business practice, by default

Implement “Secure by Default” policies, including least privilege, need-to-know, least trust, mandatory access control and separation of duties.

3. Embedded into Design

Embed privacy into the design and architecture of ICT system and business practices. Do not bolt it on after the fact.

Apply Software Security Assurance practices. Use hardware solutions such as Trusted Platform Module.

4. Positive-Sum

Accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a zero-sum approach involving unnecessary trade-offs.

Accommodate all stakeholders. Resolve conflicts to seek win-win.

5. End-to-End Security

Ensure cradle-to-grave, secure life-cycle management of information end-to-end.

Ensure confidentiality, integrity and availability of all information for all stakeholders.

6. Visibility and Transparency

Keep component parts of IT systems and operations of business practices visible and transparent, to users and providers alike.

Strengthen security through open standards, well-known processes and external validation.

7. Respect for the User

Respect and protect interests of the individual, above all. Keep it user centric

Respect and protect the interests of all information owners. Security must accommodate both individual and enterprise interests.



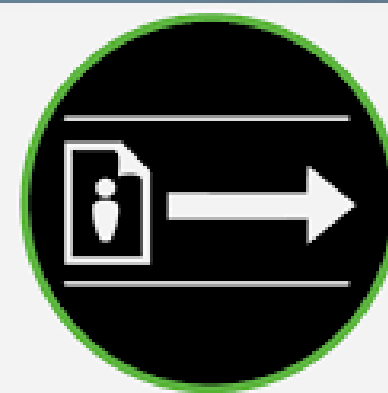
Your data is never bartered or sold.



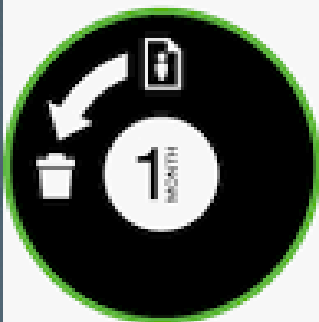
Your data may be bartered or sold.



Your Data May be Used for Purposes You Do Not Intend



Your Data is Used Only for the Intended Use



Your data is kept for less than 1 month.



Your data may be kept indefinitely.

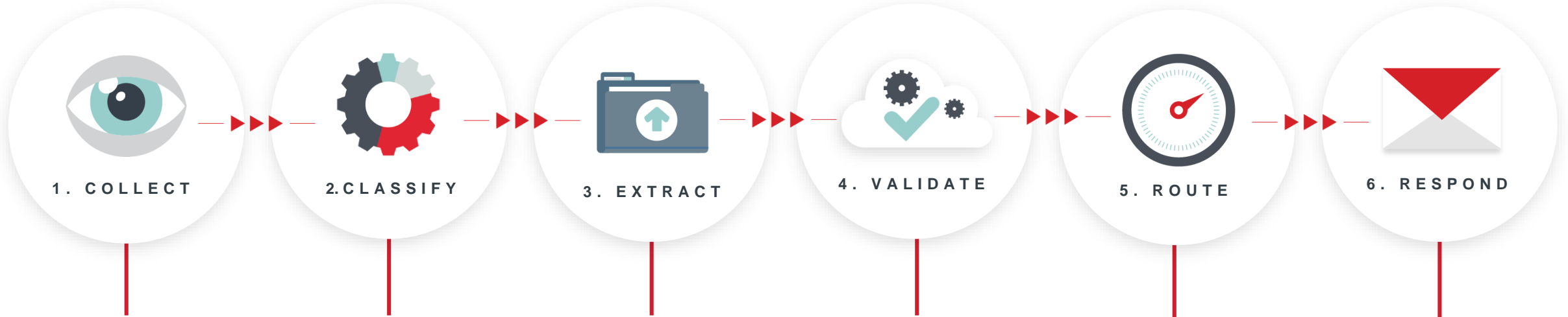


Site gives your data to advertisers.



Your data is never given to advertisers.

Privacy Management System Life Cycle



1. COLLECT

1. Mobile
2. Scanner
3. Email
4. Fax
5. File

2. CLASSIFY

1. Content Classification
2. Automatic Item Prioritization
3. Dynamic Document Processing Routes

3. EXTRACT

1. Date
2. Address Sender
3. Address Receiver
4. Customer/Client No
5. Document Type/Content
6. Signature

4. VALIDATE

Validate :

1. Date
2. Customer/Client No
3. Address
4. Document
5. Signature

5. ROUTE

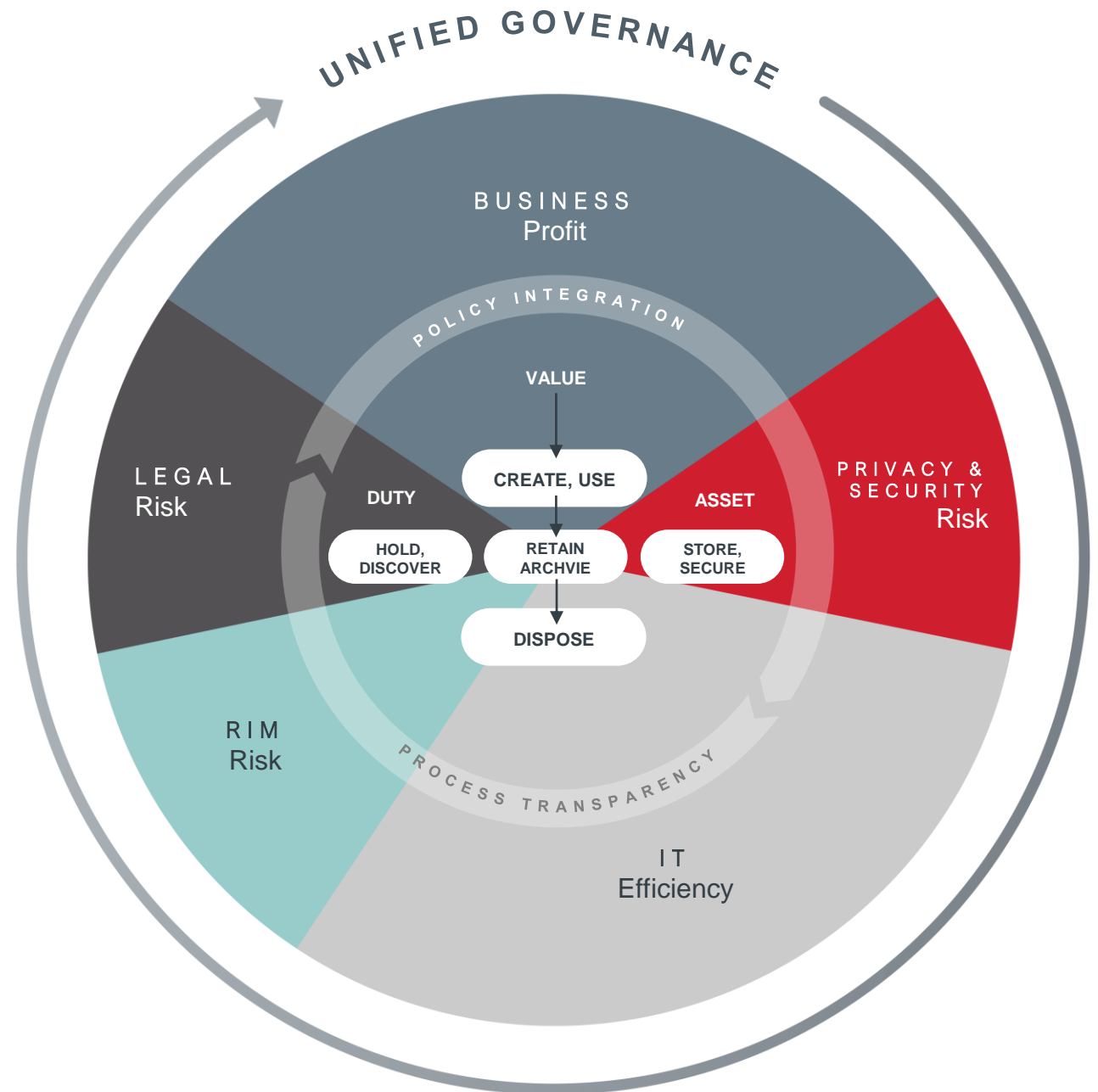
Extracted data:

1. ECM
2. Core Applications
3. CRM
4. Workflow
5. Archive Systems

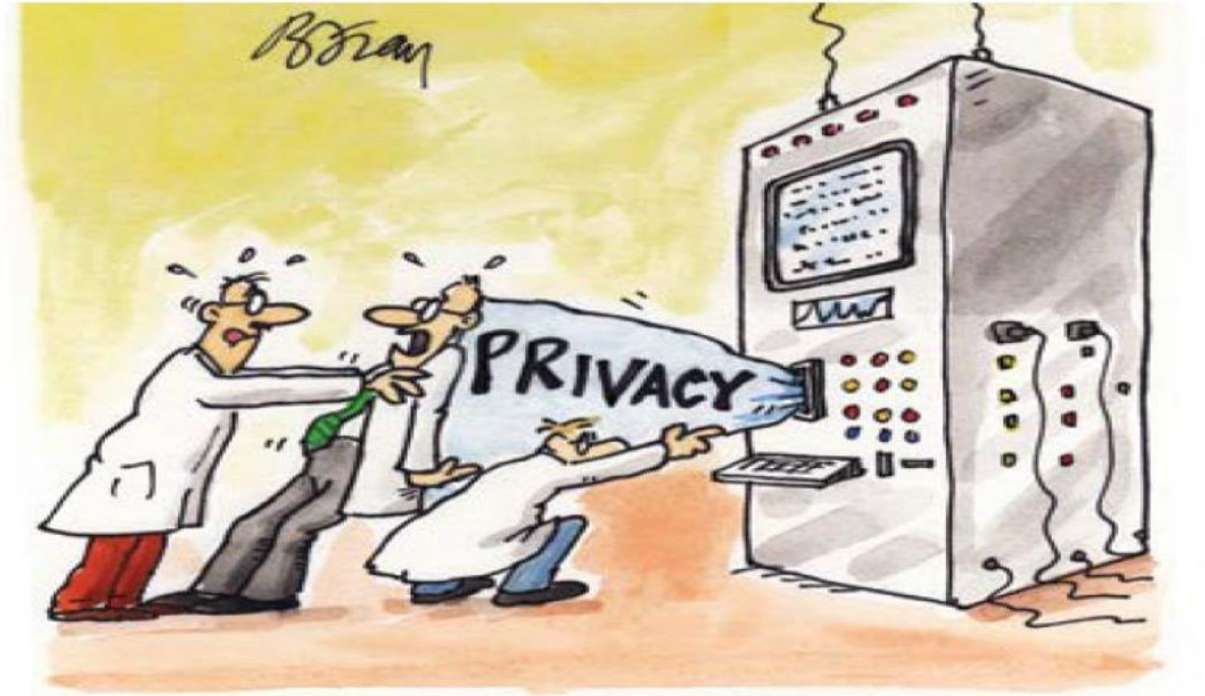
6. RESPOND

1. Queries
2. Automated Response
3. Alerts

Information Governance Reference Model



Key Takeaways



" I SUPPOSE IT WOULD HAVE BEEN EASIER TO
BUILD IT IN AT THE BEGINNING! "

Deloitte.

Resources

Privacy Enhancing Technologies – OPC

https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/

Nimity

<https://www.nymity.com/>

IAPP

<https://iapp.org/>

Data Protection Principles for the 21st Century

https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf

AICPA/CICA Privacy Maturity Model

https://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf

Ponemon Institute

<https://www.ibm.com/security/data-breach>



peryandrew@gmail.com

Sponsored by Mariner Innovations



EVOLVE | 2018

YOUR FUTURE

YOUR CAREER | YOUR COMPANY | **OUR** INDUSTRY

Hope you enjoyed the presentation!

*Please take a moment and complete our
Speaker Survey at: www.pdsummit.ca*

Feedback is a gift and its the only way we can make PDS 2019 even better!