Privacy Act 2.0

ALGIM Autumn Conference: "Unlocking the Potential"
7 May 2019

Daimhin Warner
Director (Auckland), Simply Privacy Ltd

Simply Privacy.

What’s privacy really?

Simply Privacy.

Privacy's **about people**

Remember the people behind the data

- preserving individual **control**
- protecting **autonomy** and dignity
- giving people **meaningful choices**

Simply Privacy.

Privacy's about **unlocking the potential**

If data security creates the **padlocks**

data privacy provides the **keys**

to **unlock the potential** of personal information,
within a lawful, responsible and ethical framework

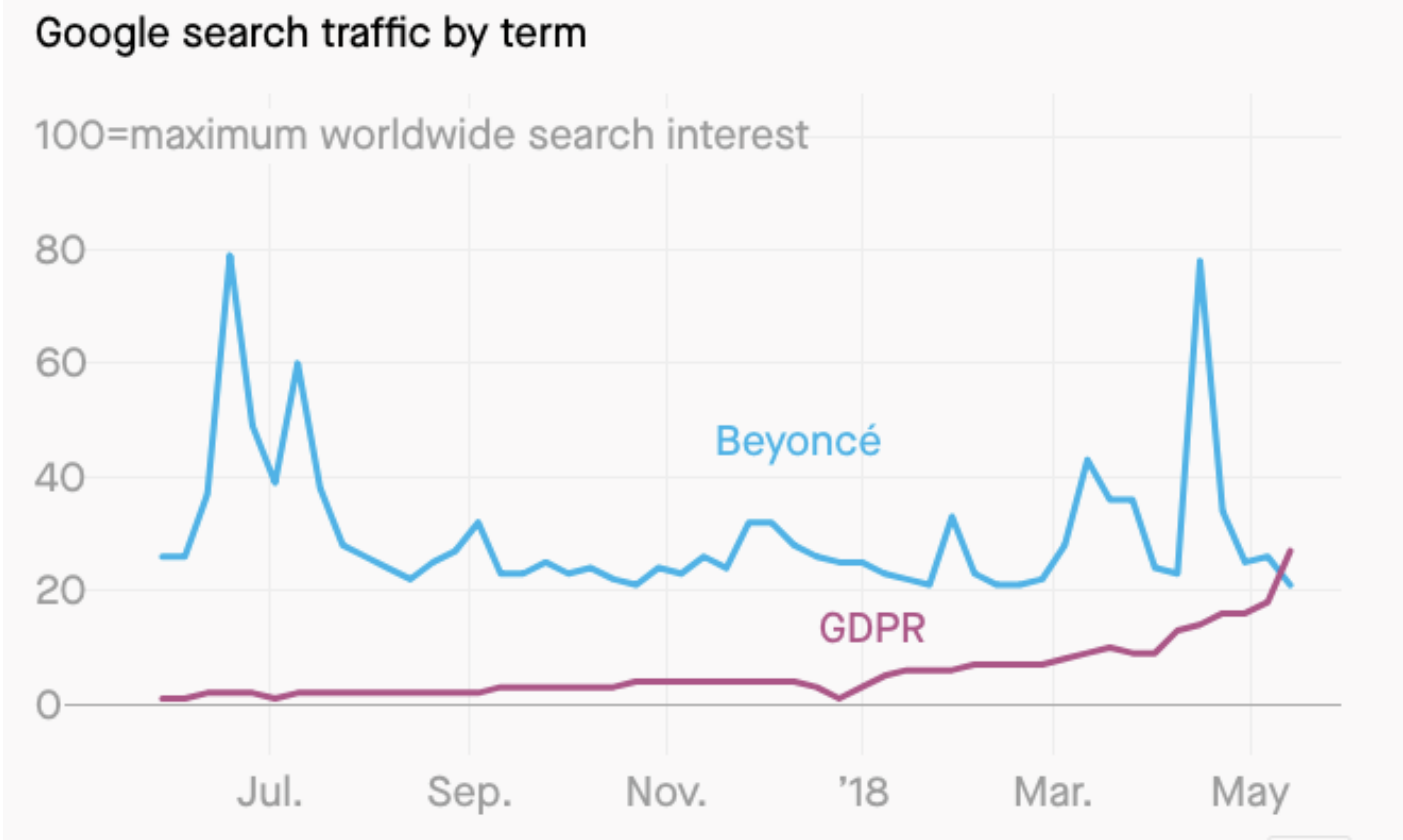
Privacy is an enabler, not a barrier

Simply Privacy.

We’re heading into a new privacy era

Simply Privacy.

Privacy's **bigger than Beyoncé**



Simply Privacy.

Privacy's **getting real**

Privacy laws are being reformed

- GDPR and GDPR-isation
- Australia
- USA – CCPA/ Federal privacy law
- NZ Privacy Act reform

In response to

- Rapid technological change – AI; big data; IOT; surveillance technology
- Concern about major data breaches; invisible processing; online harms
- Renewed focus on more fundamental ideas - ethics, human rights and social licence
- Evolving public expectations – "post-peak apathy"

Simply Privacy.

From privacy is dead (peak apathy)…

Privacy no longer a social norm, says Facebook founder

▲ People have become more comfortable sharing private information online, says Facebook founder Mark Zuckerberg. Photograph: Eric Risberg/AP

"You have zero privacy anyway, get over it",
Scott McNealy, CEO of Sun Microsystems, January 1999

Simply Privacy.

To privacy as a differentiator (post-peak apathy)…

Simply Privacy.

Privacy Bill 2019 – Shifting the goalposts

- Retains flexible principles-based approach, but…
- Creates mandatory privacy breach notification regime
- Gives Privacy Commissioner the power to issue **[public]** compliance notices
- Gives Privacy Commissioner the power to make binding access determinations
- Strengthens accountability for cross-border information sharing
- Has extraterritorial effect
- Creates new criminal offences

*might still change

Simply Privacy.

Key updates to the Privacy Bill

- Increases threshold for mandatory privacy breach notification (more later on this)
- Requires the Privacy Commissioner to make compliance notices public
- Outsourcing agency deemed to know of a breach by supplier = civil liability
- Prohibits collection of personal identifiers where they're not necessary to provide a service
- Places limitations on the collection of personal information about children
- Requires agencies to take steps to minimise the risk of misuse of a unique identifier
- Permits agencies to refuse a Privacy Act request where it was made under duress

- New Privacy Act scheduled to commence **1 March 2020**

Simply Privacy.

Key Select Committee omissions

- Right to be forgotten (though, note its limitations)
- Big fines (or any fine at all for a breach of the privacy principles)
- Data portability
- Restriction on automated processing
- Mandatory Privacy Impact Assessments

A law fit for 2011… What will this mean for EU adequacy?

Simply Privacy.

GDPR – Re-setting best practice

- Extraterritorial effect:
  - Established in EU?
  - Offering goods and services or tracking behavior?
  - Subjects must be in EU at time of collection
  - Requires an **element of targeting**
- For local government, could apply to engaging with EU employees, suppliers or property buyers
- Must have data protection officer
- Must maintain record of processing
- Much more prescriptive (rights and obligations)
- Fines up to higher of 4% annual global revenue or 20 million euros

Simply Privacy.


mandatory breach notification
~~WINTER~~ IS COMING
GAME OF THRONES

Mandatory breach notification – **mea culpa**

- From March 2020 data breaches must be notified
- If reasonable to believe they've caused, or are likely to cause, serious harm
- Notify to Privacy Commissioner and affected people
- Failure = criminal offence and $10,000 fine
- Failure = interference with privacy of affected people
- Failure = irreparable reputation damage (impact on trust)
- Put a plan in place to meet this new obligation
  - **Catch them**
  - Investigate them
  - Notify them
  - Prevent them

Simply Privacy.

The fallout is worse… but not much

Simply Privacy.

Commissioner's new ~~clothes~~ powers

Compliance notices

- Require an agency to do something
- Require an agency to stop doing something
- Enforceable, and appealable, to the HRRT
- Must be publicised, unless

Binding access determinations

- Direct an agency to release personal information requested by data subject
- Appealable to the HRRT

Simply Privacy.

New criminal offences

It will be an offence for a person to:

- Impersonate a person to access, use or alter personal information
- Knowingly destroy personal information subject to a request
- Fail to notify the Privacy Commissioner of a privacy breach
- Fail to comply with a compliance notice

Liable to a **fine of up to $10,000** (up from $2,000)

Note - limits on personal liability!


Thanks
Any questions?
Simply Privacy.