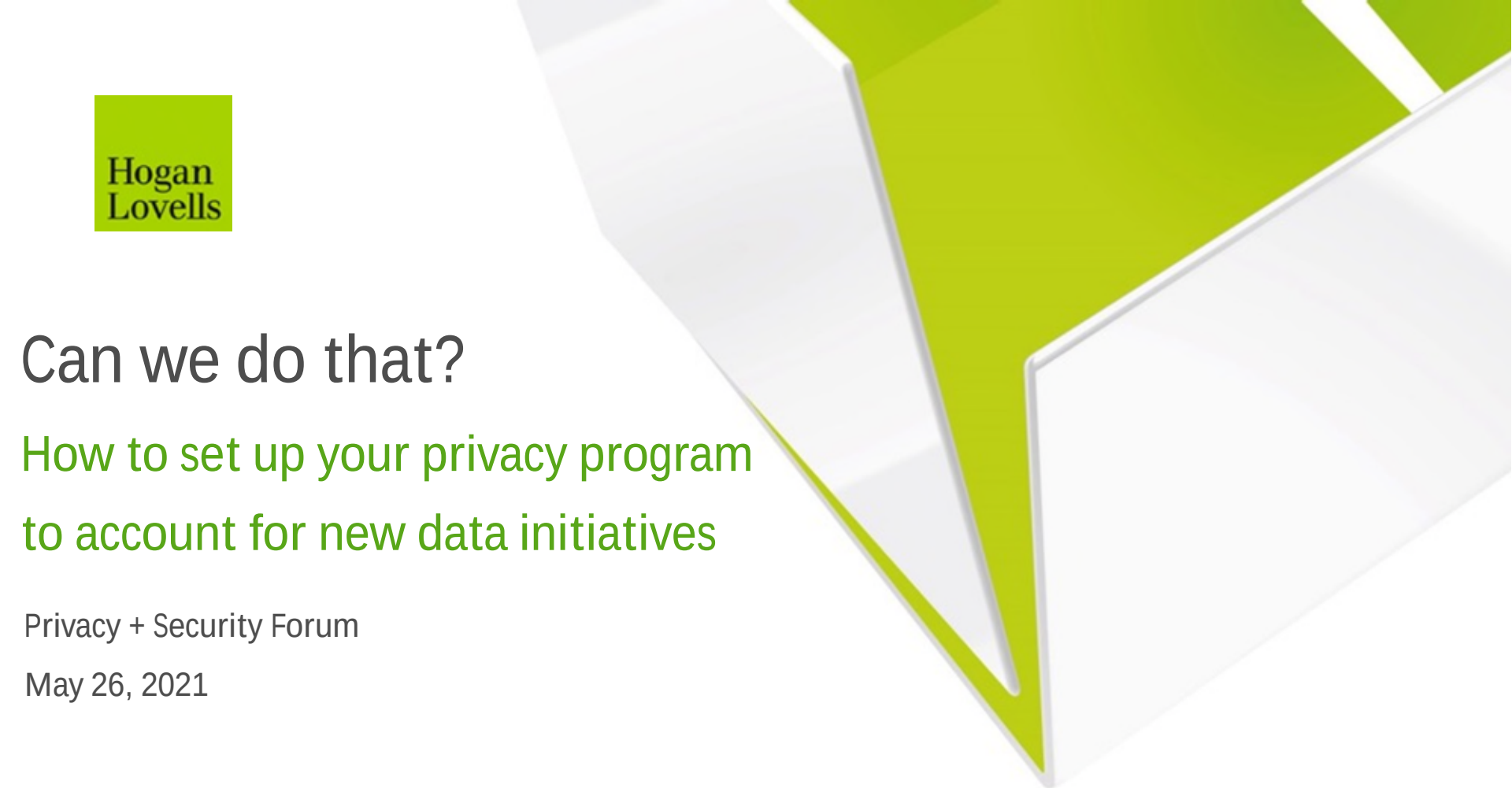

Can we do that?

How to set up your privacy program to account for new data initiatives

Privacy + Security Forum

May 26, 2021

Introductions

Bret Cohen
Partner
Hogan Lovells

Daniel Cunha
VP, Legal
OpenTable

Kelly Gertridge
Head of Privacy
Atlassian

Cristin Morneau
Global Head of Privacy & DPO
Groupon

Can we do that?

- You get a call from your head of marketing at 4pm on a Friday
- “We have a great new opportunity with FilterCo – they have an exciting new AI solution that is going to help us provide an end-to-end view of all of our customer relationships”
- All we need to do is:
  - Click through their terms
  - Upload a list of customer email addresses
    - “Don’t worry, it’ll be hashed”
  - Drop a first-party cookie on our site
  - Incorporate a third-party SDK into the check-out page
  - “Tweak” our privacy policy

GDPR: Focus on compatibility

- "Personal data shall be…collected for specified, explicit and legitimate purposes and not further processed **in a manner that is incompatible with those purposes**…." *(GDPR, Art. 5.1.b)*
- "[T]he legislator chose a double negation: it prohibited incompatibility. By providing that any further processing is authorised as long as it is *not incompatible*…it would appear that the legislators intended to give some flexibility with regard to further use." *(Article 29 Working Party Opinion 03/2013 on purpose limitation, 21)*
  - Different processing not de facto "incompatible"
  - Societal norms or data subjects may change views on compatibility
  - Not all potential purposes are known at time of collection

GDPR: Compatibility factors

- "Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
  - any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
  - the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
  - the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
  - the possible consequences of the intended further processing for data subjects;
  - the existence of appropriate safeguards, which may include encryption or pseudonymization." *(GDPR Art. 6.4)*

Historic U.S. approach: Focus on deception and materiality

- FTC approach: "[U]nfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful" *(FTC Act, Section 5(a))*. A "deceptive" practice is where:
  - there is a representation, omission, or practice that is likely to mislead the consumer;
  - the consumer is acting reasonably under the circumstances; and
  - the representation, omission, or practice is a material one.
- What is "material"? "The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception." *(1983 FTC Policy Statement on Deception)*
  - I.e., consumers were misled in a way that impacted their decisions, rather than constraining data use to a limited set of described purposes

Historic U.S. approach: Focus on deception and materiality

Two primary FTC enforcement paradigms:

- Broken data use promises = material misrepresentation
  - Focus on provably false representations, rather than compatible purposes
- Insufficient notice of sensitive data collection = material omission
  - Closer to incompatible use, but still requires a determination of materiality

CCPA: A materiality approach, constrained by disclosures

- "A business shall not use a consumer's personal information for a purpose materially different than those disclosed in the notice at collection. If the business seeks to use a consumer's previously collected personal information for a purpose materially different than what was previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose." *(CCPA Regulations § 999.305(a)(5))*

Analyzing new data initiatives

- Is it really a change? What is the link between the original purpose specified at the time of collection, and the new purpose?
- What new data rights will third parties have, and will that impact the promises you have made?
- What are the impacts of the change to data subjects? How will it impact your systems? Can those impacts be mitigated?
- Will this change apply retroactively or going forward?
- Is there a way to monitor future changes?

Panel Question

How do you identify new data use cases within the business? How do you make sure that the business comes to you?

Panel Question

Once the business comes to you, how do you determine what legal/privacy standard to apply?

Panel Question

You've determined that notices need to be updated. How do you notify?

Panel Question

You've approved the project. What's next? How do you make sure that the business complies with controls?

Back to FilterCo…

- "We have a great new opportunity with FilterCo – they have an exciting new AI solution that is going to help us provide an end-to-end view of all of our customer relationships"
- All we need to do is:
  - Click through their terms
  - Upload a list of customer email addresses
    - "Don't worry, it'll be hashed"
  - Drop a first-party cookie on our site
  - Incorporate a third-party SDK into the check-out page
  - "Tweak" our privacy policy

What do you do?