IAB Canada Privacy Policy Member Update

April 10, 2019

iab.canada

Today's Agenda

1. Update on US Privacy Developments
2. IAB Europe – Transparency & Consent Framework (TCF)
3. PIPEDA – Canada Privacy Update
4. Questions & Next Steps

IAB US Update (Abr.)

Sonia Carreno, IAB Canada

April 10, 2019

iab.canada

10 Things to Know About Privacy Discussions in Congress

1. Multiple hearings were held in 2018, including many with top executives from platforms and other companies
2. The “creepiness” factor has grabbed the attention of House and Senate members, but issue conflation and demagoguery are rampant
3. Members have introduced sectoral bills with privacy-centric language, but none are expected to gain traction
4. All eyes are on four specific Senate offices, that are working together to circulate a “discussion draft” this spring. That bill will be seen as the main congressional product on privacy, and will provoke sustained industry advocacy through 2020
5. A Federal bill is likely to include enhanced rule-making authority for the FTC and required mechanisms that companies must implement
6. Duties of “care” and “loyalty” with respect to the handling of consumer data are expected to be included
7. The “New Paradigm,” which IAB has helped draft with a cross-industry coalition, will be a main driver for congressional consideration
8. Republican Members of Congress have stated that Federal preemption must be included for any bill to pass the House and Senate
9. Democrats insist that CCPA-like language must be the “floor” for any piece of draft legislation
10. More hearings on privacy will commence throughout the summer

iab.canada

Broad Consensus Among Reps & Dems

Sen. Wicker (R): *A national framework does not mean a weaker framework, but a preemptive framework that ensures consumers will have the same level of protection across the United States.*

Sen. Cantwell (D): *I find this effort somewhat disturbing, that as our country is grappling with all the privacy violations we've seen, the first thing people want to organize is a preemption effort.*

Rep. Walden (R): *We can improve the security and privacy of consumers' data without adding to the confusion or harming small businesses and entrepreneurs – so Congress should thoughtfully consider what various states are proposing so we deliver that certainty with a national standard.*

Sen. Schatz (D): *I understand that from the standpoint of some of the companies, the holy grail is preemption. And I want you to understand that you're only going to get there if this is meaningfully done.*

Rep. Schakowsky (D): *Data collection industry had become an economic powerhouse "gobbling up every piece of consumer data it can.*

Sen. Moran (R): *We need to provide clear-and-measurable requirements in statutory text for the FTC to utilize while also creating appropriate flexibility in narrow rulemaking authority*

Sen. Blumenthal (D): *We have a trust gap that we need to bridge*

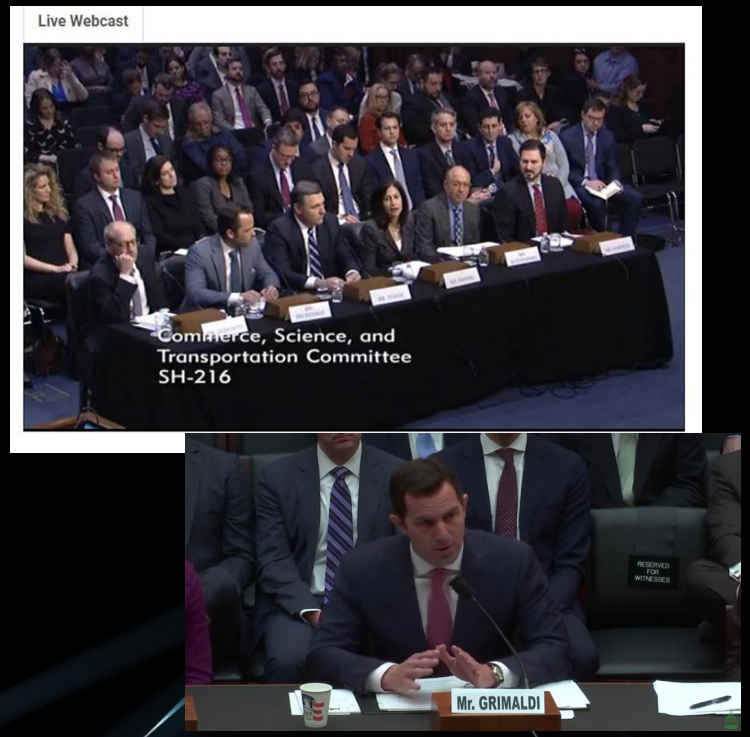
iab. canada

Cross-Industry “Privacy for America” Regulatory Framework

Privacy for America

Mission
Privacy for America will work with Congress to support enactment of comprehensive federal consumer data privacy and security legislation. We have outlined a bold new paradigm for a national law that would make personal data less vulnerable to breach or misuse and set forth clear, enforceable and nationwide consumer privacy protections for the first time.

Steering Committee Members
- IAB
- 4 A’s
- ANA
- DAA
- NAI



The Cross-Industry “Privacy for America” Regulatory Framework

- Provide strong and comprehensive privacy and security protections for consumers
- Provide clear rules of the road for consumers, businesses, and law enforcement
- Stop harmful and unexpected uses of data while allowing beneficial data practices and market innovation to flourish
- Prohibits “unreasonable” data practices as defined under the law; identifies certain practices as “per se unreasonable”
- Enacted as standalone law with FTC as primary enforcer (creates Data Protection Bureau in FTC)
  - Creates new Data Protection Bureau within FTC.
  - Creates defined process for FTC to designate additional practices as unreasonable through rulemaking or enforcement
- Establishes rules governing data collection and use for advertising
- Creates rigorous safe harbor program, to be overseen and approved by FTC
- Preempts certain state privacy laws but authorizes State AGs to enforce key provisions of new law

IAB Europe Update (Abr.)

Townsend Feehan, CEO IAB Europe

April 10, 2019

iab.canada

Transparency Consent Framework Recent Developments

Version 2.0 Released for Commentary & Adoption

TCF Recent developments – Registration, Market update

- 495 registered vendors, 199 CMPs
- TCF implemented on 100.000+ websites
- Roughly 20% of programmatic ad calls from EU sites carry TCF strings
- Vendor and CMP renewal for 2019 registration starts May 1st - rolling monthly renewal process and first 'batch' of renewals were distributed April 2nd;
- Registration fee for Vendor renewal remains Euro 1200
- Administration fee for CMP renewal has increased from Euro 350 to Euro 1200

iab.canada

Finalizing Transparency Consent Framework Version 2.0

Addressing Legitimate Interest and Consumers' Right to Object and Increased Granularity

- Full accommodation of **legitimate interests legal basis**.
- Providing a means for consumers to exercise their **right to object** to processing based on a legitimate interest legal basis and a new signal to allow vendors to know that the user has objected to such processing / exercised the RTO.
- New controls over how vendors may use certain "features" (i.e., data types and aspects of processing whose use can be integral to processing for many purposes)
- More specificity – previous 'compound' purposes have been broken down into their constituent parts
- Adding new publisher restrictions signalling so that downstream recipients will know that the publisher has restricted some purpose(s) for some vendor(s)
- Publishers will be able to restrict / prohibit vendors' subsequent use of data collected on their sites
- CMPs will be able to combine purposes in "stacks" for first-layer presentation to users – reconciling need for concise, transparent, intelligible, clear and plain language with need for specificity
    - Purpose definitions are standardised
    - Agreed "stacks" of purposes will also be standardised
    - Stack names will be standardised
- No backward-compatibility – Versions 1,0 and 2,0 are not interoperable

iab.canada

Consent Management Platform (CMP) Validator

Compliance Checks

The Validator allows any CMP to be checked for a number of common compliance issues, where a CMP implementation does not adhere to the TCF technical specifications and/or TCF policies.

- Validator is a Chrome extension
- Shows whether consent string is generated properly
- Identifies CMP ID
- Any CMP found not complying will be contacted by IAB Europe and advised what action they need to take.
- Aim is to support CMP community and bring CMPs into compliance

iab.canada

Canadian Privacy Update

Adam Kardash, Chair, Privacy and Data Management
Osler, Hoskin & Harcourt LLP
Co-Lead, AccessPrivacy

April 2019

iab.canada

Canadian privacy update: Overview

- Three key developments in Canadian privacy arena that will impact IAB Canada members
  - OPC consultation on transborder dataflow guidance
  - OPC guidance on consent
  - PIPEDA Reform

OPC consultation on transborder dataflows

- OPC announced consultation process on April 9
- OPC is revisiting its current policy position on transborder data flows under PIPEDA.
- Will impact most IAB Canada members
  - This includes cross border data transfers between “controllers” and “processors”.

- **Key draft positions - Consent**
  - "*A company that is disclosing personal information across a border, including for processing, must obtain consent. Individuals must be given the opportunity to exercise their legal right to consent to disclosures across borders, regardless of whether these are transfers for processing or other types of disclosures. When information is disclosed between organizations, absent an exemption in PIPEDA, consent is required.*"
  - "*Where there is a meaningful risk that a residual risk of harm will materialize and will be significant, consent should be expressed, not implied.*"

OPC consultation on transborder dataflows

- **Key draft positions – Consent (cont'd)**
  - *"It is the OPC's view that individuals would reasonably expect to be notified if their information was to be disclosed outside of Canada and be subject to the legal regime of another country. Whether this affects their decision to enter into a business relationship with an organization or to forego a product or service should be left to the discretion of the individual. "*
  - *"Individuals must be informed of any options available to them if they do not wish to have their personal information disclosed across borders. As we state in our consent guidance, organizations must make available to individuals a clear and easily accessible choice for any collection, use or disclosure that is not necessary to provide the product or service. Depending on the circumstances, a transfer for processing may well be integral to the delivery of a service and in such cases, organizations are not obligated to provide an alternative. Nonetheless, by being provided with clear and adequate information about the nature, purpose and consequence of any disclosure of their personal information across borders, individuals will be able to make an informed decision about whether to consent to the disclosure and therefore do business with the organization."*

OPC consultation on transborder dataflows

- Key draft positions – Accountability
  - "*When disclosing personal information to a third party for processing, a company does not relinquish control of the information. That being said, business relationships can be very complex and determining which organization has personal information "under its control" needs to be assessed on a case-by-case basis, and informed by factors such as relevant contractual arrangements, commercial realities, as well as evolving business models and shifting roles. For instance, if an organization that is a processor uses or discloses the same personal information for other purposes, it is no longer simply processing the personal information on behalf of another organization and is thereby acting as an organization "in control" of the information.*"
  - "*An organization that processes personal information on behalf of another organization may still have obligations under the Act in respect of the personal information in its possession or custody, as an organization that collects, uses or discloses personal information in the course of commercial activities."*

OPC consultation on transborder dataflows

- Consultation Process
  - The OPC intends to provide guidance on disclosures for processing and related consent and accountability requirements.
  - OPC is seeking input from interested parties on its updated policy position, as well as on specific areas for which related guidance would be most needed.
  - Notably, update to the OPC's policy position will impact a number of existing OPC guidance documents
  - Deadline for submissions is June 4, 2019.
  - IAB Canada will be making a submission.

Meaningful consent

- New *Guidelines for obtaining meaningful consent*, jointly issued by the OPC, OIPC Aberta, and OIPC BC, are now being "applied" by the OPC as of January 1, 2019.
  - Cited as "Non-binding", but newly articulated expectations
  - All IAB Canada members impacted by this guidance
  - Re-affirmation of the Canadian privacy regulatory view of the "centrality" of consent in Canadian privacy legislation
    - Under PIPEDA, a consent is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the **nature, purpose and consequences** of the collection, use or disclosure of the personal information to which they are consenting
  - Intended by regulators to set out practical and actionable guidance regarding what organizations should do to ensure that they obtain meaningful consent

Meaningful consent

- Seven guiding principles for obtaining meaningful consent:
  1. Emphasize key elements, namely;
     - What personal information is being collected,
     - With which parties personal information is being shared,
     - For what purposes personal information is collected, used or disclosed, and
     - Risk of harm and other consequences;
  2. Allow individuals to control the level of detail they get and when;
  3. Provide individuals with clear options to say 'yes' or 'no';
  4. Be innovative and creative;
  5. Consider the consumer's perspective;
  6. Make consent a dynamic and ongoing process; and
  7. Be accountable: “Stand ready to demonstrate compliance”.

Meaningful consent

- "Must do" (from OPC guidance):
  - Make privacy information readily available in complete form, while giving emphasis or bringing attention to four key elements:
    - What personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to.
    - With which parties personal information is being shared
    - For what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to.
    - **Risks of harm and other consequences**
  - Provide information in manageable and easily-accessible ways.
  - Make available to individuals a **clear and easily accessible choice** for any collection, use or disclosure that is not necessary to provide the product or service.
  - **Consider the perspective of your consumers**, to ensure consent processes are user-friendly and generally understandable.
  - Obtain consent when making significant changes to privacy practices, including use of data for new purposes or disclosures to new third parties.
  - Only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate, under the circumstances.
  - Allow individuals to withdraw consent (subject to legal or contractual restrictions).
  - **Obtain explicit consent for collections, uses or disclosures which generally: (i) involves sensitive information; (ii) are outside the reasonable expectations of the individual; and/or (iii) create a meaningful residual risk of significant harm.**
  - Obtain consent from a parent or guardian for any individual unable to provide meaningful consent themselves (including under the age of 13), and ensure that the consent process for youth able to provide consent themselves reasonably considers their level of maturity.

iab canada

Meaningful consent

- "Should do" (from OPC guidance):
  - Allow individuals to **control** the amount of detail they wish to receive, and when.
  - Design or adopt innovative and creative ways of obtaining consent, which are **just-in-time, specific to the context, and suitable to the type of interface.**
  - **Periodically remind** individuals about the consent choices they have made, and those available to them.
  - **Periodically audit** privacy communications to ensure they accurately reflect current personal information management practices.
  - **Stand ready to demonstrate** compliance – in particular, that the consent process is understandable from the perspective of the user.
  - In designing consent processes, consider:
    - Consulting with users and seeking their input;
    - Pilot testing or using focus groups to evaluate the understandability of documents;
    - Involving user interaction / user experience (UI/UX) designers;
    - Consulting with privacy experts and/or regulators; and/or,
    - Following established best practices or standards.

PIPEDA reform

- Significant amendments to Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) were proposed on March 1, 2018 by the ETHI Committee.
- The recommendations are heavily influenced by the EU General Data Protection Regulation.
- If implemented through legislative amendments, the recommendations would have a substantial operational impact on all organizations subject to PIPEDA, including all IAB Canada members
- Reform process will commence at some point after November federal election

PIPEDA reform

- Key recommendations for PIPEDA amendments include:
  - to **explicitly provide for opt-in consent as the default** for any use of personal information for secondary purposes, and with a view to implementing a default opt-in system regardless of purpose;
  - to provide for a **right to data portability**;
  - to include a framework for a **right to erasure** based on the model developed by the European Union that would, at a minimum, include a right for young people to have information posted online either by themselves or through an organization taken down;
  - to clarify the terms under which personal information can be used to satisfy legitimate business interests;

PIPEDA reform

- **Key recommendations for PIPEDA amendments include (cont'd):**
  - to examine the best ways of protecting depersonalized data;
  - to include a framework for the **right to de-indexing in PIPEDA** and that this right be expressly recognized in the case of personal information posted online by individuals when they were minors;
  - to strengthen and clarify organizations' obligations with respect to the destruction of personal information;
  - to make **privacy by design a central principle** and to include the seven foundational principles of this concept, where possible;
  - to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance; and
  - to give the Privacy Commissioner **broad audit powers**, including the ability to choose which complaints to investigate.

Get Involved

Join IAB Canada Privacy Policy Committee

policy@IABCanada.com