PROGRAM MATERIALS
Program #3102
January 13, 2021

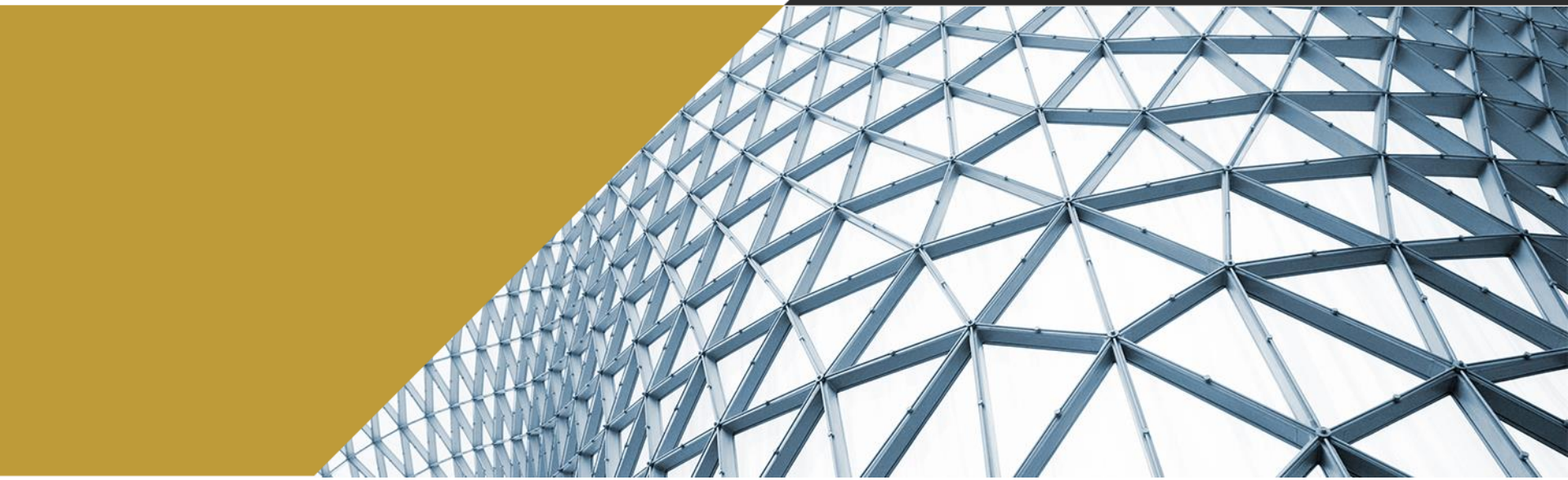
Evaluating a Vendor's Privacy Practices: The Rise of the Vendor Privacy Assessment Questionnaire

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919

GT GreenbergTraurig

www.gtlaw.com



Evaluating a Vendor's Privacy Practices:

The rise of vendor privacy assessment questionnaires

January 2021

Agenda

1. Overview of US data security & privacy laws
2. Historic focus on vendor data security
3. Recent data privacy trends impacting vendor assessments
4. Practical impact for vendor due diligence
5. Vendor privacy due diligence using questionnaires

Overview of US data security & privacy laws

Vs.

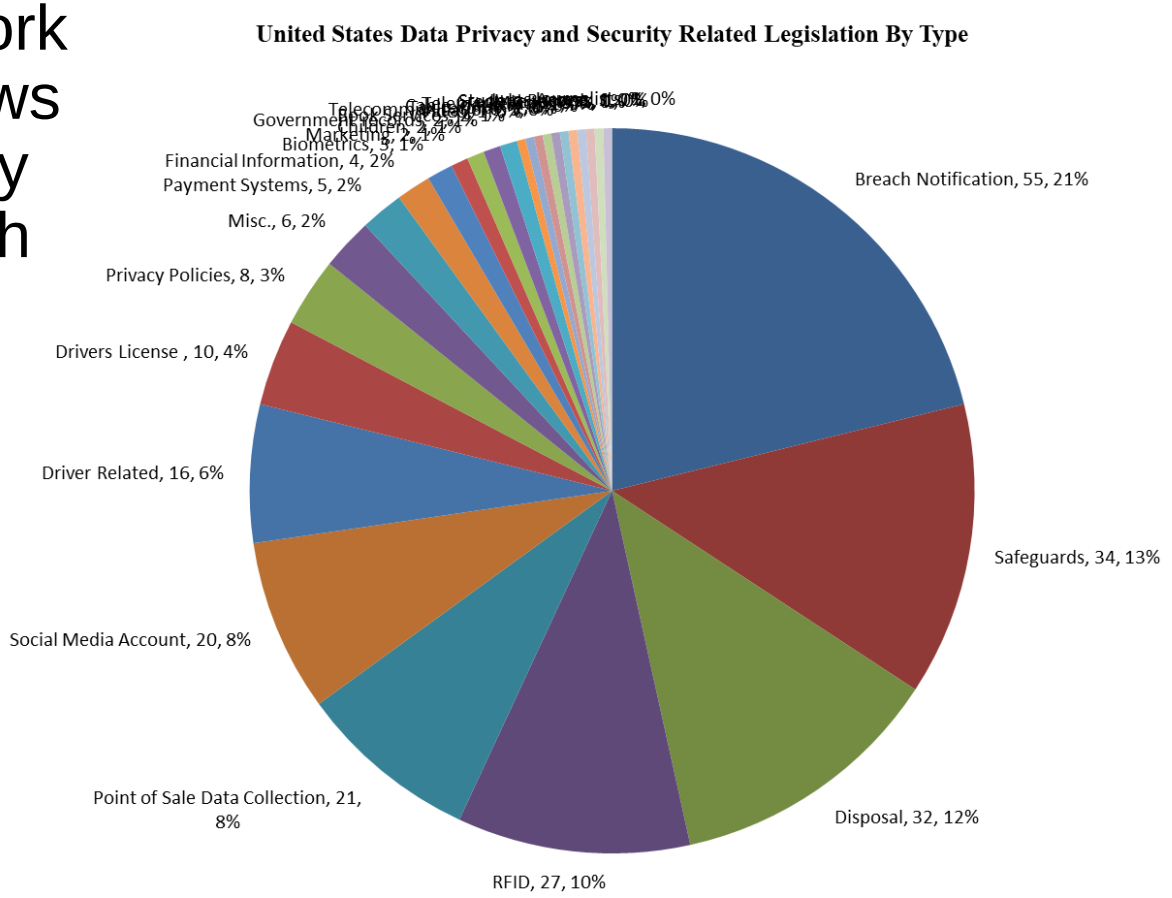
Data Security is about protecting data from malicious threats.

Data Privacy is about how data is collected, shared, and used.

Overview of US data security & privacy laws

The US has a patchwork of federal and state laws relating to data security and data privacy, which apply different rules based upon:

- type of data collected,
- the industry in which a company operates, and
- how data will be used



Historic focus on vendor data security

- In the US, focus has historically been on **data security** rather than on **data privacy.**
- Numerous federal and state data security laws explicitly require companies to take reasonable steps to select service providers with appropriate security and/or monitor service providers once selected.
- For example…

Historic focus on vendor data security

Gramm Leach Bliley Act ("GLBA") Safeguards Rule
(16 CFR 314.4)

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

Massachusetts Safeguards Regulation
(201 CMR 17.00)

(f) Oversee service providers, by:
1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with 201 CMR 17.00 and any applicable federal regulations; and
2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.03(2)(f)2. even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

Historic focus on vendor data security

New York Department of Financial Services (NYDFS) Regulations

500.11 Third party service provider security policy.

(a) Third party service provider policy.

Each covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers. Such policies and procedures shall be based on the risk assessment of the covered entity and shall address to the extent applicable:

(1) the identification and risk assessment of third party service providers;

(2) minimum cybersecurity practices required to be met by such third party service providers in order for them to do business with the covered entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third party service providers; and

(4) periodic assessment of such third party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

New York Shield Act

PROCEDURES;

(5) SELECTS SERVICE PROVIDERS CAPABLE OF MAINTAINING APPROPRIATE SAFE-GUARDS, AND REQUIRES THOSE SAFEGUARDS BY CONTRACT; AND

Historic focus on vendor data security

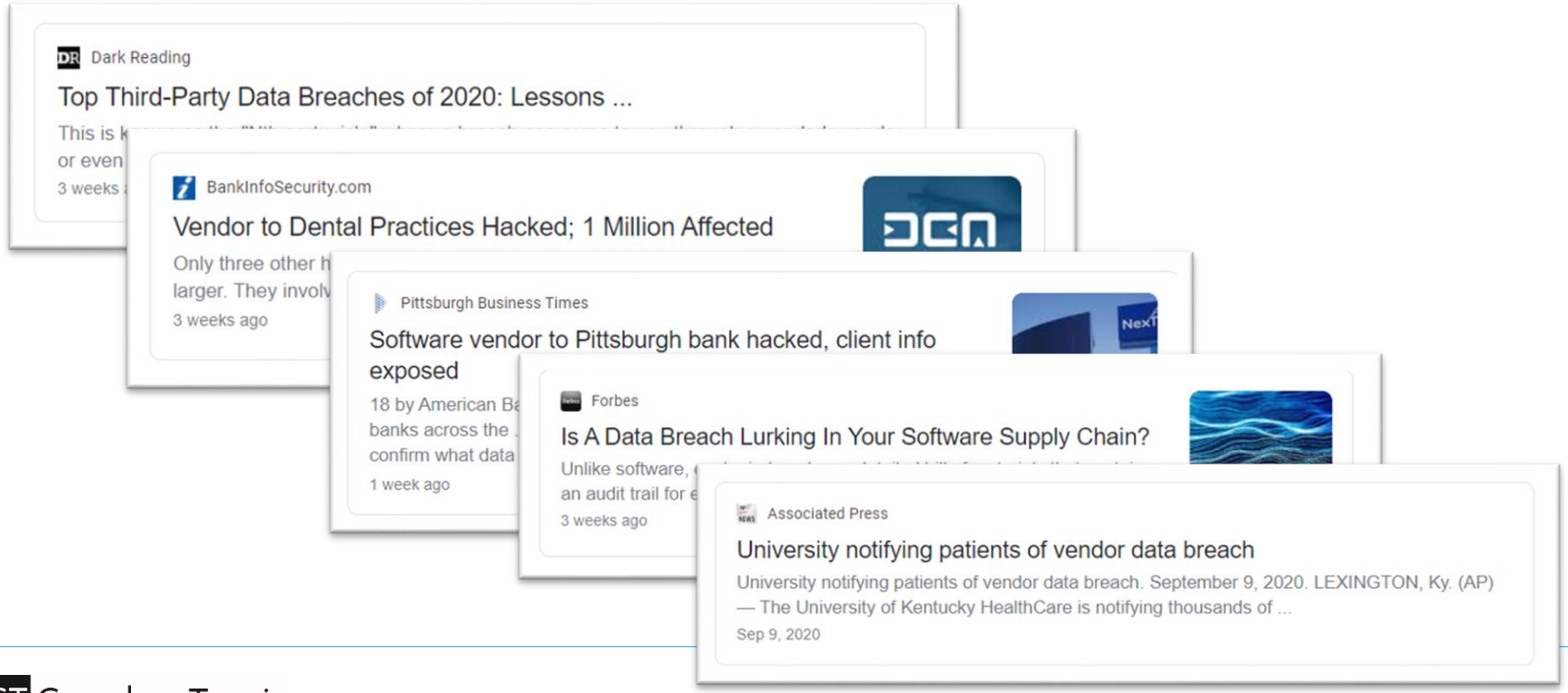
- Other laws are less explicit in their discussion of selecting and/or monitoring service providers.
- However, some impose a general negligence-like data security standard that might extend to all aspects of the data ecosystem including service providers.
- For example…
  - **California law requires:**

(b) A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Cal. Civil Code 1798.81.5(b)

Historic focus on vendor data security

- In addition to statutory and regulatory obligations, legal and business risks arise when a vendor has a data security breach



Historic focus on vendor data security

- Data privacy traditionally conceptualized in the US with a free-market-like approach where companies could compete as to their privacy practices.
- That approach has shifted over the past two years with greater privacy regulation and restrictions.

Recent data privacy trends impacting vendor assessments

- CCPA
- CPRA
- Schrems II
- App Privacy Questionnaire

Recent data privacy trends impacting vendor assessments

CCPA

California Consumer Privacy Act of 2018

- Enacted in 2018, went into force in 2020
- Explicit *contractual* requirements for service providers:
  - (1) Prohibition on the use of personal information,
  - (2) Prohibition on the disclosure of personal information, and
  - (3) Prohibition on the retention of personal information.
- Implicit requirements for service providers:
  - (4) Ability to process a “flow down” access request, and
  - (5) Ability to process a “flow down” deletion request.

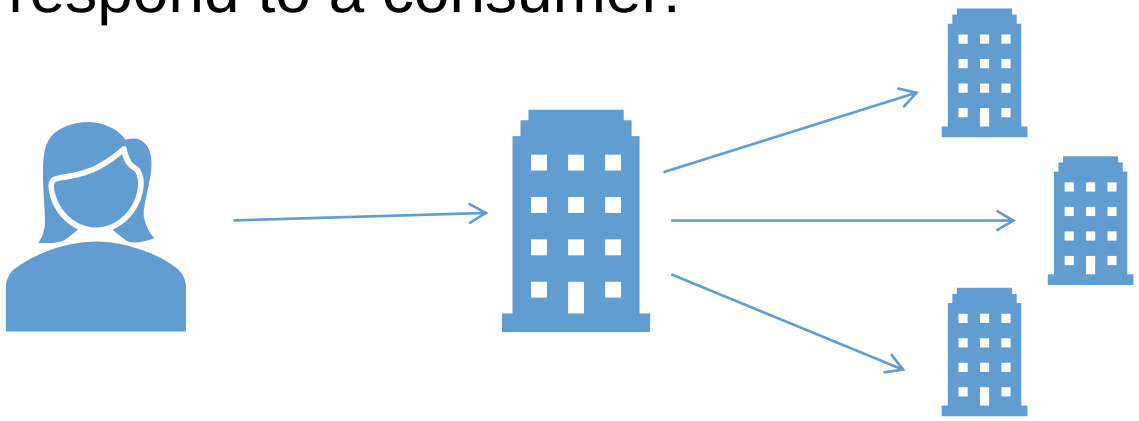
Cal. Civil Code § 1798.140(v)

Recent data privacy trends impacting vendor assessments

CCPA

California Consumer Privacy Act of 2018

- A “flow down” occurs when a business must push down an access or deletion request to its vendors in order to properly respond to a consumer:



Recent data privacy trends impacting vendor assessments

CCPA

California Consumer Privacy Act of 2018

- Impact on vendor due diligence
  - **Contract Review and Amendment –** Because the CCPA's requirements could be satisfied by contractual provisions, most vendor due diligence focused on contract review and amendment.
  - **Assess Flow Down Capabilities** – Some companies did engage in due diligence in connection with the flow down obligations of the CCPA, but most companies trusted their vendor's ability to follow flow down instructions and/or identified gaps in vendor capabilities after the law went into effect.

Recent data privacy trends impacting vendor assessments

CCPA

California Consumer Privacy Act of 2018

- Impact on vendor due diligence (cont.)
  - The CCPA may contain a provision, however, that provides a perverse incentive when it comes to vendor due diligence.

(j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

Cal. Civil Code § 1798.145(j)

Recent data privacy trends impacting vendor assessments

CCPA

California Consumer Privacy Act of 2018

- Enacted in 2018, went into force in 2020
- Explicit *contractual* requirements for service providers:
  - (1) Prohibits service provider from ***using*** personal information
  - (2) Prohibits service provider from ***disclosing*** personal information
  - (3) Prohibits service provider from ***retaining*** personal information
- Implicit requirements for service providers:
  - (4) Ability to process a “flow down” access request
  - (5) Ability to process a “flow down” deletion request

Recent data privacy trends impacting vendor assessments

CPRA

California Privacy Rights Act of 2020

- Enacted (by referendum) in 2020, will become operative in 2023
- Amends the CCPA by adding to the explicit contractual requirements:
  - (1) Prohibits vendor from combining personal information
  - (2) Prohibits vendor from “selling or sharing personal” information
  - (3) Requires vendor to notify business of it cannot meet its legal obligations
- Additional requirements beyond the contractual obligations:
  - (4) Notify business if vendor engages another person (e.g., subprocessor)
  - (5) Flow down contractual requirements to subprocessors
  - (6) Cooperate in responding to access, deletion, and rectification requests

Recent data privacy trends impacting vendor assessments

CPRA

California Privacy Rights Act of 2020

- Impact on vendor due diligence
  - **Beyond Contract Review –** Although there are still contractual requirements, the CPRA goes beyond the mere existence of contractual terms.
  - **Assess Flow Down Capabilities –** Companies are considering whether to conduct due diligence regarding flow down obligations of the CPRA (i.e., access, deletion, and rectification capabilities).
  - **Subprocessor Obligations –** Companies are considerin whether to conduct due diligence in connection with subprocessor obligations.

Recent data privacy trends impacting vendor assessments

Schrems II

***Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("Schrems II")**

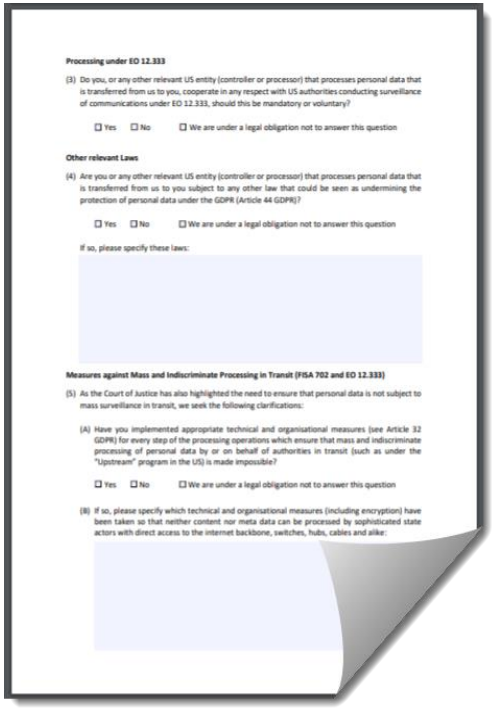
- **Background**
  - A privacy advocate - Max Schrems - challenged Facebook's ability to transmit personal information from Europe to the United States under the EU-US Privacy Shield or by utilizing EU-approved Standard Contractual Clauses.
  - The European Court of Justice ("ECJ") invalidated the EU-US Privacy Shield Framework.
  - The ECJ stated the use of Standard Contractual Clauses does not necessarily satisfy legal requirements, and that companies "should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses" when data might be accessed by the United States government.

Recent data privacy trends impacting vendor assessments

Schrems II

***Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("Schrems II")**

- Following the ECJ decision, the plaintiff in the Schrems II litigation recommended that companies transmitting information from Europe to the United States (or other non-EEA countries) should request that the entity receiving the information complete a privacy questionnaire as a "preliminary attempt" to identify what supplemental measures might be warranted.



Processing under EO 12.333

(3) Do you, or any other relevant US entity (controller or processor) that processes personal data that is transferred from us to you, cooperate in any respect with US authorities conducting surveillance of communications under EO 12.333, should this be mandatory or voluntary?

☐ Yes ☐ No ☐ We are under a legal obligation not to answer this question

Other relevant Laws

(4) Are you or any other relevant US entity (controller or processor) that processes personal data that is transferred from us to you subject to any other law that could be seen as undermining the protection of personal data under the GDPR (Article 44 GDPR)?

☐ Yes ☐ No ☐ We are under a legal obligation not to answer this question

If so, please specify these laws:

Measures against Mass and Indiscriminate Processing in Transit (FISA 702 and EO 12.333)

(5) As the Court of Justice has also highlighted the need to ensure that personal data is not subject to mass surveillance in transit, we seek the following clarifications:

(A) Have you implemented appropriate technical and organisational measures (see Article 32 GDPR) for every step of the processing operations which ensure that mass and indiscriminate processing of personal data by or on behalf of authorities in transit (such as under the "Upstream" program in the US) is made impossible?

☐ Yes ☐ No ☐ We are under a legal obligation not to answer this question

(B) If so, please specify which technical and organisational measures (including encryption) have been taken so that neither content nor meta data can be processed by sophisticated state actors with direct access to the internet backbone, switches, hubs, cables and alike:

Recent data privacy trends impacting vendor assessments

Schrems II

***Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("Schrems II")**

- The European Data Protection Board ("EDPB") later proposed recommendations on supplemental measures that stated that a company that sends data outside of the EEA should, among other things:
  - ✓ Assess the legal conditions in the receiving country.
  - ✓ Consider whether the receiving entity utilizes one of several technical measures (e.g., encryption, pseudonymization, de-identification, etc.) to protect information from disclosure to government agencies.
  - ✓ Consider whether the receiving entity will agree to other contractual and process-oriented protections. These include….

Recent data privacy trends impacting vendor assessments

Schrems II

***Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("Schrems II")**

List laws that permit government access. Importer enumerates laws and regulations in its country that would permit access by public authorities (Para. 99-101)

No back door to government. Importer certifies that it has not purposefully created "back doors" to allow for government access (Para. 103-104)

Audit against government access. Importer grants audit rights to exporter so that they can verify there has been no disclosures to government. (Para. 105-106)

Notify data subject of law enforcement requests. Importer/exporter will notify data subject of any government data request. (para. 118-119)

No onward transfers. Commitment from the importer not to engage in any onward transfers. (Para. 137)

Notify of changes in law. Importer must notify exporter of any changes in local law that would interfere with SCC compliance. (Para. 107-109)

24 hour warrant canary. Warrant canary transmitted every 24 hours to the importer. (para. 110-111)

Document gov. access requests. Document and record access requests from public authorities for exporter. (Para. 127-128)

Policy to challenge law enforcement requests. Law enforcement policy to challenge any order if there are local grounds to do so. (Para. 112-113)

Policy to educate law enforcement of GDPR. Law enforcement policy to inform government agency of incompatibility with EEA laws. (Para. 114-115)

Limit access to those situations in which there is consent. Importer will only access data with consent of data subject or exporter (Para. 116-117))

Ongoing assessments. Commit to the adoption and regular review of internal policies to assess suitability of complementary measures. (para. 136).

Rapid deployment privacy team. Creation of a team in the EEA to challenge foreign government requests. (Para. 124-126)

Assist data subject to exercise rights. Importer/exporter will assist data subject to exercise their rights in the foreign country. (Para. 120-121)

Transparency reports. Publication of transparency report summarizing government requests for information. (Para. 129-130)

Recent data privacy trends impacting vendor assessments

Schrems II

***Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("Schrems II")**

- Impact on vendor due diligence
  - Many of the recommendations of the EDPB relate to information that can be solicited from vendors. For example:

100. The importer could be for instance required to:

(1) enumerate the laws and regulations in the destination country applicable to the importer or its (sub) processors that would permit access by public authorities to the personal data that are subject to the transfer, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision applicable to the transferred data;

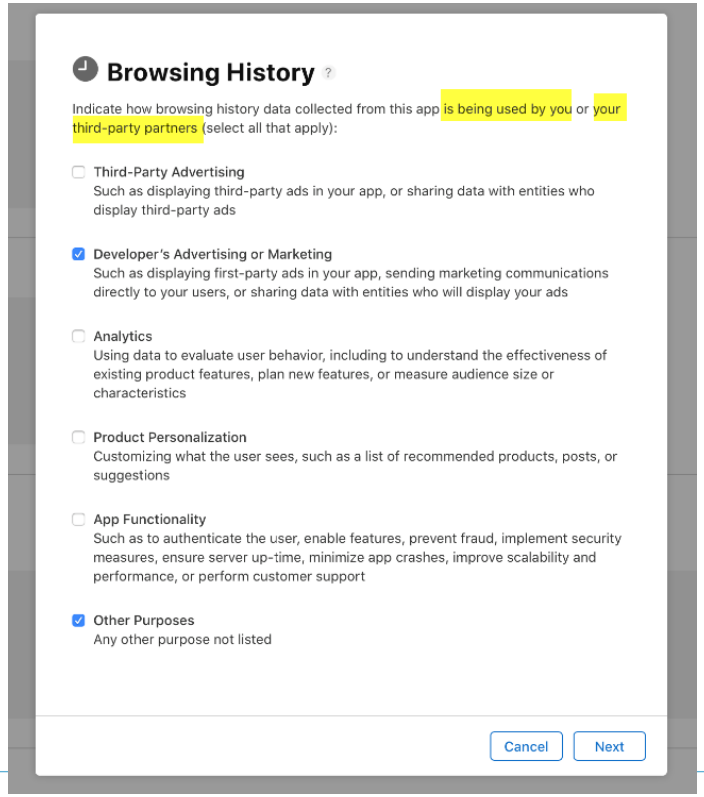
110. Insofar as allowed by national law in the third country, the contract could reinforce the transparency obligations of the importer by providing for a "Warrant Canary" method, whereby the importer commits to regularly publish (e.g. at least every 24 hours) a cryptographically signed message informing the exporter that as of a certain date and time it has received no order to disclose personal data or the like. The absence of an update of this notification will indicate to the exporter that the importer may have received an order.

Recent data privacy trends impacting vendor assessments

App Privacy Questionnaire

App Store Privacy Nutrition Label

- **Background:**
  - On December 8, 2020, as a requirement to submit a new App to the App Store (or to submit an update to an existing App) an App developer must complete a questionnaire concerning the App's collection and use of personal information.
  - App developers must respond based upon their own collection and use practices as well as the collection and use practices of their "third-party partners"

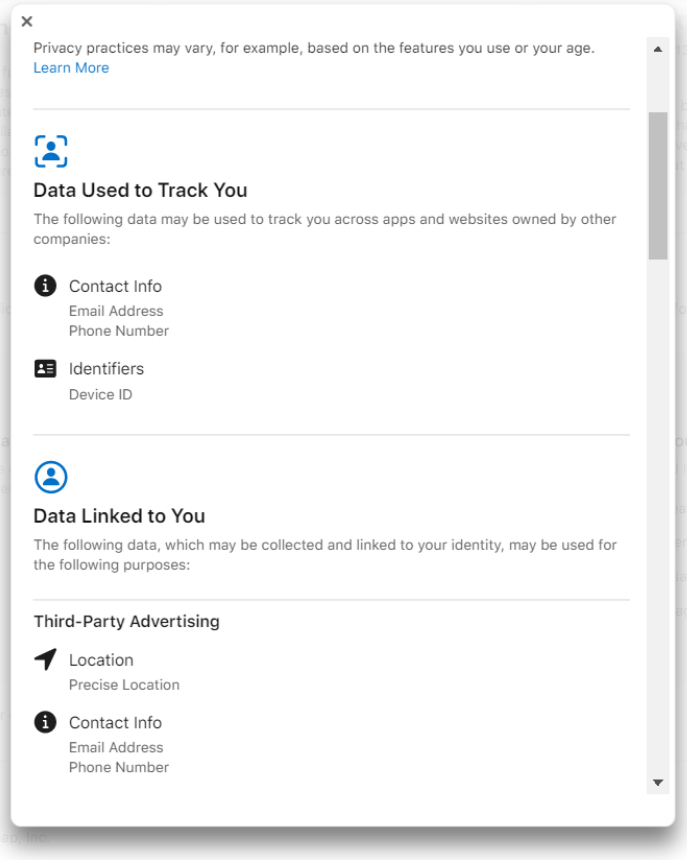


Recent data privacy trends impacting vendor assessments

App Privacy Questionnaire

App Store Privacy Nutrition Label

- **Background:**
  - The information collected from the questionnaires is then published within the App Store in what some have called a privacy “nutrition label.”



Recent data privacy trends impacting vendor assessments

App Privacy Questionnaire

App Store Privacy Nutrition Label

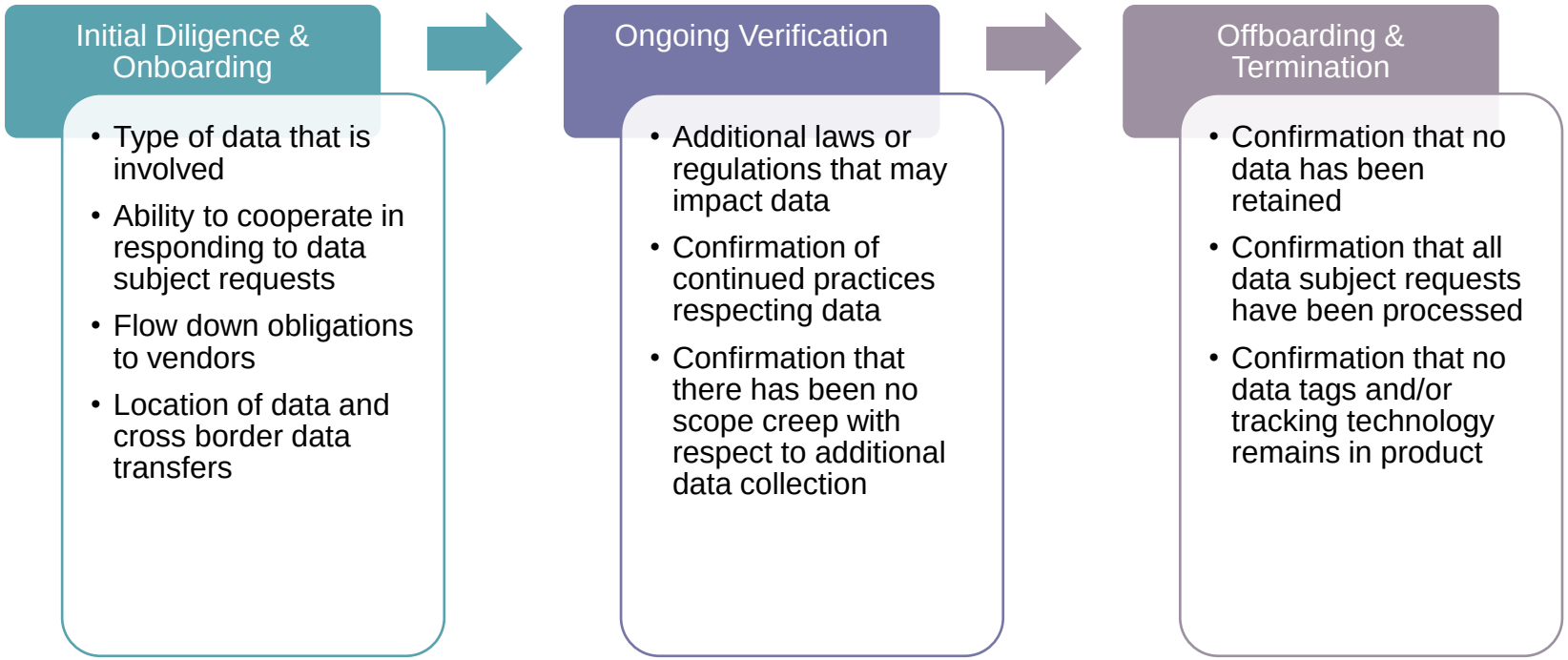
- Impact on vendor due diligence
  - For each third party that installs code in an App (i.e., SDK providers), a company is supposed to identify:
    - Which of 32 different data types the SDK is designed to collect.
    - For each data type collected, whether the third party partner uses the information for:
      - ✓ third party advertising,
      - ✓ first party advertising,
      - ✓ analytics,
      - ✓ product personalization,
      - ✓ app functionality, or
      - ✓ other purposes.

Practical impact for vendor due diligence

- Companies are increasingly requiring vendors to complete questionnaires focused on the vendor's privacy practices.
- Companies typically consider the dissemination of questionnaires at three stages of the vendor life cycle:

Practical impact for vendor due diligence

- The questions companies ask may vary depending on the stage:



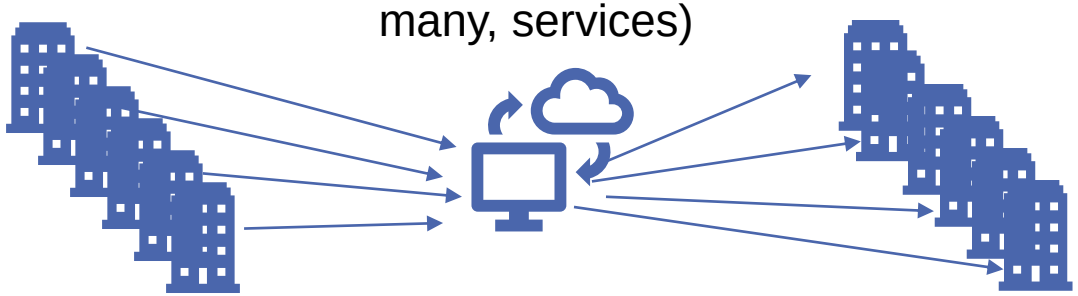
Vendor privacy due diligence using questionnaires

- No industry standard “questionnaire” or uniform template.
- One challenge that arose in the context of security questionnaires, vendors were inundated with bespoke forms from their clients (e.g., 10,000 questionnaires in different formats, with different numbering and in different text, asking the same basic questions).
- Some vendors pivoted toward
  - offering their own uniform security questionnaires, or
  - commissioning third parties to certify practices against an industry framework in lieu of responding to questionnaires.

Vendor privacy due diligence using questionnaires

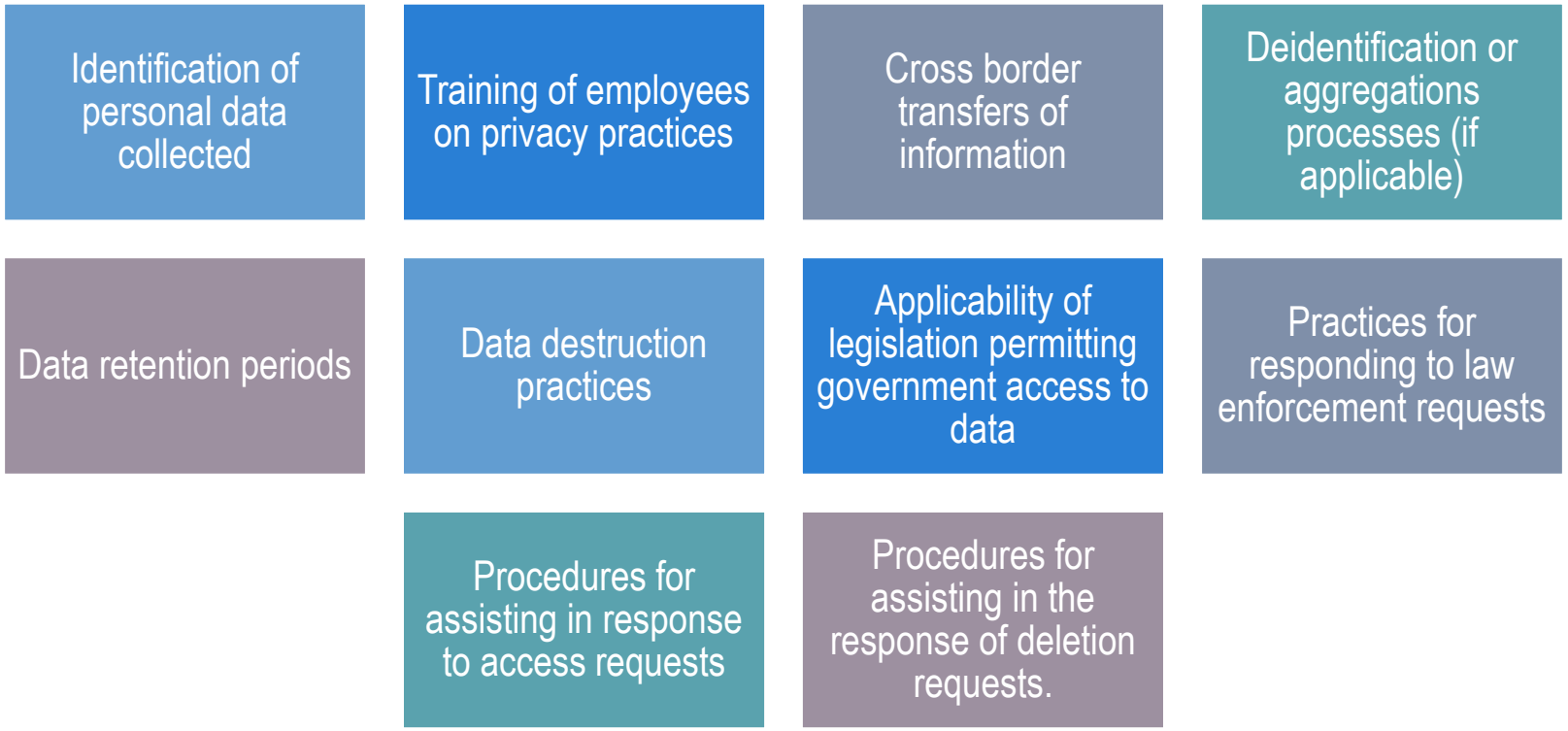
- Other solutions
  - Third-party services (e.g., Security Scorecard Atlas)

- facilitates the rapid dissemination of questionnaires and responses
- aggregates requests from multiple clients to one vendor, and
- allows the vendor to promulgate responses to multiple clients (i.e., many to one, and one to many, services)



Vendor privacy due diligence using questionnaires

- Most privacy questionnaires focus on the following core areas:



David Zetoony
Shareholder; Co-Chair of the firm's U.S. Data, Privacy and Cybersecurity Practice

DENVER +1 303.685.7425
zetoonyd@gtlaw.com | LinkedIn | Detailed Biography

David Zetoony focuses on helping businesses navigate data privacy and cyber security laws from a practical standpoint. David has helped hundreds of companies establish and maintain ongoing privacy and security programs, and he has defended corporate privacy and security practices in investigations initiated by the Federal Trade Commission, and other data privacy and security regulatory agencies around the world, as well as in class action litigation.

Karin E. Ross
Associate
U.S. Data, Privacy and Cybersecurity Practice

DENVER +1 303.685.7472
rossk@gtlaw.com | Detailed Biography

Karin E. Ross focuses her practice on data privacy, cybersecurity, and technology transactions. Karin has counseled a diverse array of companies from startups to Fortune 500 companies in both local and global markets. She works closely with clients on data privacy and security compliance programs and advises on existing and emerging privacy and data protection. Her experience spans a range of industries including consumer goods, medical technology, financial services, e-commerce, and restaurants.