Cybersecurity and Privacy Issue-Spotting in Vendor Agreements

ACC NCR Privacy Forum

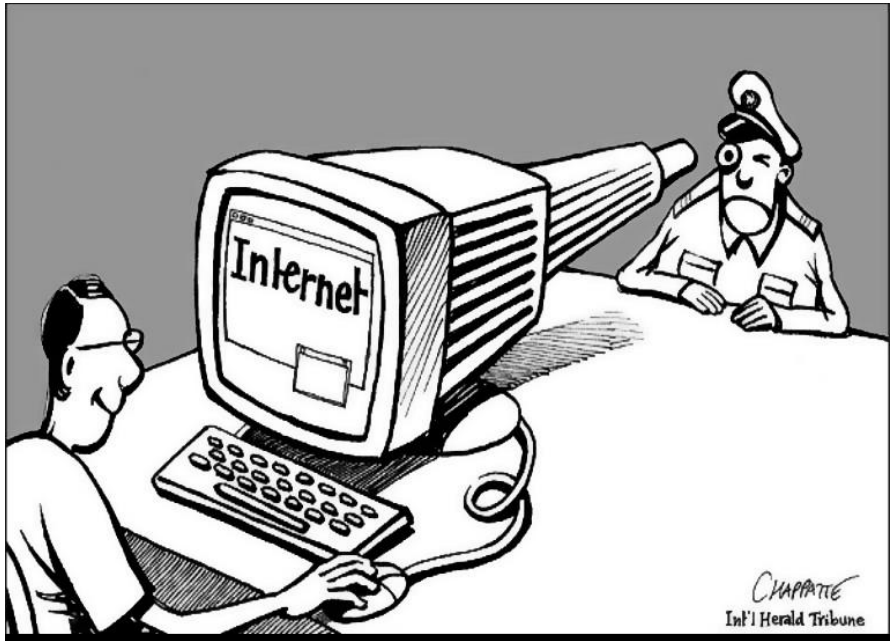
July 30, 2019

Presented by:
Doug Bonner, Partner
Jeff Kosseff, Counsel
Potomac Law Group, PLLC

Rebecca Shore-Suslowitz, Director, Global Privacy
Under Armour

What we will cover today…

- The “moving target” of U.S. privacy legislation: new legislation continues apace in the states. CCPA, but also newer bills resembling the CCPA: CT, NY PA and TX
- Need for business/vendor compliance exists now: GDPR and CCPA
- What businesses are subject to the GDPR? CCPA?
- GDPR compliance issues
- CCPA compliance issues – California residents only? Or perhaps a de facto national baseline standard?
- Expectations for Vendors
- Corporate “Best Practices” – a global approach
- How will CCPA affect supply chain management?



CCPA Overview

CCPA is a disclosure law. Establishes right of California residents

- To know what categories and "pieces" of PI is collected; business purpose for it; and with whom such PI will be shared.
- Business must provide the information in (a) on "verifiable consumer request." Sec. 1798.100(a)-(c).

- Business disclosure of privacy practices is required "at or before the point of collection". Sec. 1798.100(b).
- **Broad definition of "personal information".** Includes: identifiers (name, postal address , IP address, email address, SSN, DL #, passport #); commercial info.; biometric info.; browsing hx; search hx; geolocation data; etc.
- **Broad definition of "sell"** – doesn't track business/legal definition of a "sale": includes "disclosing, disseminating, making available, transferring" consumer's PI for "monetary or other valuable consideration." Sec. 1798.140(t)(1)

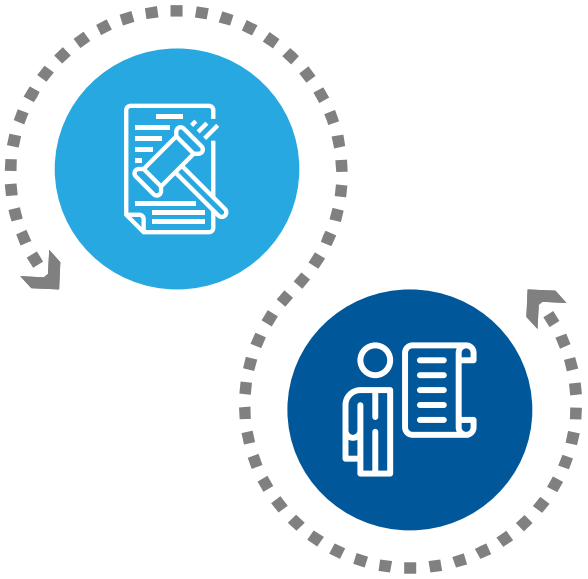
CCPA Disclosure and Deletion Processes

Responses to consumer requests	Must deliver requested information to consumer free of charge within 45 days of receipt of a "verifiable consumer request." Sec. 1798.110; .130 ▪ Must disclose: categories of PI and sources from which collected; business purpose; categories of PI sold **and 3rd parties to whom it was sold**; specific pieces of PI collected about consumer. ▪ Need at a minimum, a toll-free telephone number and a Web site address (if you maintain an Internet Web site). ▪ Disclosure must be for 12 month period preceding receipt of request.
Right to deletion	▪ Upon receipt of "verifiable consumer request", must delete consumer's **PI and direct any service providers to delete it too**. Some exceptions. ▪ **What is your verification process?**
Right to opt out	▪ **Consumer has right at any time to "opt out" of the sale to third parties of its personal information.** Sec. 1798.120

“What are you doing with my personal information?”

Small businesses are exempt from CCPA if: (a) <$25 Million in gross annual revenue; (b) do not annually buy, sell or share for commercial purposes the P.I. of 50,000 or more consumers, households or devices; OR (c) at least 50% of company revenues do not come from selling PI

CCPA – How will it be enforced?



California Attorney General

- Penalties of up to $2,500 per violation, $7,500 per intentional violation
- Mandatory 30 day period to “cure” a violation once put on notice before CA AG may pursue enforcement or private action may be brought. May seek opinion of AG on how to comply

Private Right of Action

- For data breaches if fail to maintain reasonable security procedures
- Minimum statutory damages of $100 -$750 per consumer, per incident

What can businesses do to prepare?

- **Understand your data flows – do you map your data?** What consumer information are you collecting, using, sharing or selling? And with whom?
  - EU Personal Data?
  - California Personal Information?
  - For EU Personal Data, is the recipient in a country whose privacy regime is “adequate”? If not, have SCCs executed by Subprocessor, and Controller consent?
- **What relationships do you have with service providers or third parties that involve personal data?** Does the service provider exemption apply?
- **Reexamine your third party vendor agreements.** Is personal information of CA consumers shared with third parties? Do they share that data with other third parties? Will you treat all U.S. Consumer data similarly or have distinct California and other U.S. Consumer standards/processes?
- **Are you staffed/prepared to respond to verifiable consumer disclosure or deletion requests?** What mechanisms are in place? Are there dedicated staff who are trained to respond to such requests? What corporate policies exist to ensure that responses are accurate, complete and timely?
- **Amend your agreements** - include specific terms agreeing to comply with the CCPA, and not to share personal information of your consumers with third parties without consumer consent
- **Set up systematic internal program** - for data mapping, and confirming CCPA-compatible agreements are in place with third party vendors.
- **Are your privacy policies and notices CCPA-compliant?** (Website; mobile applications, including of affiliates/subsidiaries).

GDPR Compliance Issues: the “horror”

Apportioning liability risk between Controller and Processor

Issue

Your company has a 2016 MSA with 5 year term for data processing services. The MSA provides for "super" liability cap of $250 Million for processor for any liability stemming from data breaches or other data protection liability. Controller's GDPR amendment proposes unlimited liability for GDPR violations. How resolve this?

- Substantial increase in risk (and cost) for GDPR compliance (security measures; data breach reporting; enforcement penalties up to 4% of global turnover)
- If there was a pre-GDPR MSA, there may a special cap to the limitation of liability for data breaches or breaches of confidentiality. Additional potential GDPR exposure is unacceptable level of risk for unlimited liability
- Processors need a reasonable cap on potential damages in the GDPR world. Controllers should be able to share some of their liability risk with Processors, but also need to self-insure some of it.
- Risk can be mitigated by security protections, audit rights, etc.
- Increased liability exposure for vendor may impact contract rates

“Appropriate” security measures under the GDPR

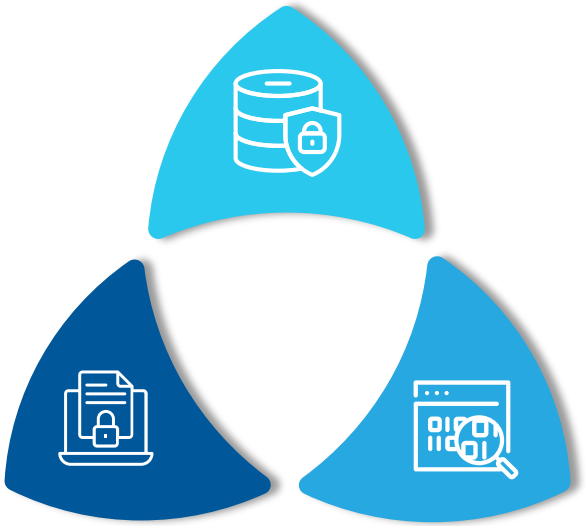
What security measures are required? Controller and Processor “shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk….” (Art. 32)

- MAY include pseudonymization and encryption
- Evaluate risks of processing
- Requires input from Corporate Security. Usually the techies can reach a mutual understanding about appropriate level of protection for the data involved based on industry standards and common practice.

Processor/ Sub-Processor transfer issues

- Onward Transfers to Sub-Processors (staffing agencies, etc.): Processor can only engage a sub-processor with "specific or general written authorization of the controller" (Art. 28.2). If Processor, can be advantageous to get authorization when negotiating GDPR amendment.
- If to a non-EEA country that has not been recognized by EU or Swiss Federal DPA as providing adequate level of privacy protection, need SCCs. Agree on form and terms of SCCs.
- GDPR requires processor to obtain same data protection obligations by agreement with subprocessor as agreed to in controller/processor agreement, **including** appropriate technical and organizational measures to meet the GDPR requirements. (Art. 28.4.)
- Issue*: Will the subprocessor data protection liability cap for a subprocessor in India be the same as that of U.K. processor?*

Other issues: Data breach reporting; audits; DPIAs



Data breaches: conform to respective GDPR requirements for controller and processor

Audits: provide reasonable limits on frequency, T&Cs, by whom

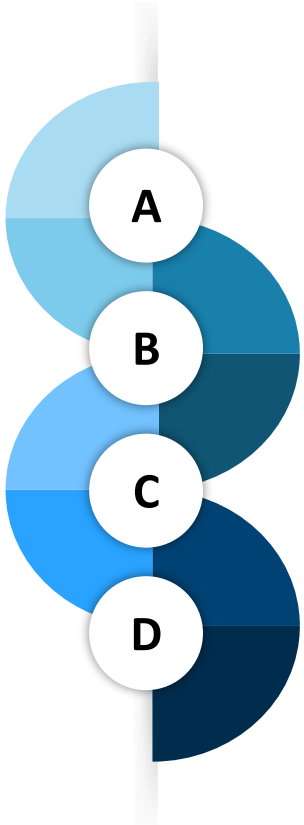
Data Protection Impact Assessments: if processor, restrict to deployment of "new technologies" and at controller expense. If controller, require advance notice of new technologies and successful DPIA before technologies are used for processing

California Consumer Protection Act Vendor Issues

Threshold issue: Does CCPA apply and to what personal information?

Is Company subject to CCPA Jurisdiction?

Will you be doing so on 1/1/20?



Do you use or share P.I. of California consumers with third parties or service providers?

What P.I. is being protected by the Company under the CCPA disclosure and deletion requirements (only CA residents, or all U.S. citizens)?

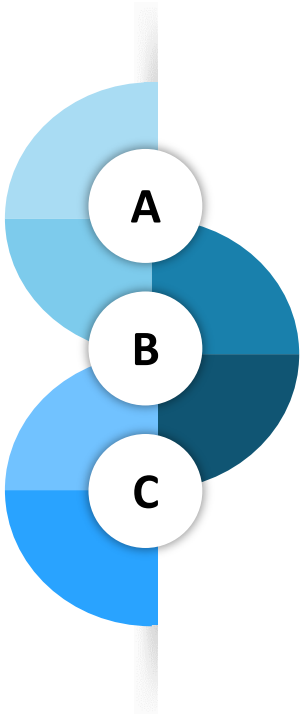
Step 2: Understand your data flows

- Have you fully mapped your data?
- What P.I. are you collecting, using, sharing, or selling? And to whom? What is the scope of the P.I.? Remember, CCPA Personal Information ≠ GDPR Personal Data!
- Is P.I. being shared by vendors with other third parties?

Does the “service provider” CCPA exemption apply?

To qualify, need to identify “commercial purposes” for sharing of P.I. in your vendor agreement AND restrict the use, retention or disclosure of that P.I. for a commercial purpose other than providing the services specified in the agreement

Include appropriate disclosures in your privacy notice of “acceptable business purposes” for sharing of personal information with vendor(s)



Include additional language to avoid being categorized as “selling” personal information to your vendor, even if only a processor

Specific CCPA contractual provisions to include in your vendor agreements

01 Prohibit use, retention or disclosure of P.I. to any third party for any purpose other than for the commercial purpose of performing the services under the agreement

02 Prohibit third party sharing or sale of P.I.

03 Include provision requiring vendor develop mechanism to timely respond to "Verifiable Consumer Requests for disclosing categories and pieces of P.I. collected, and to delete P.I. within x days (i.e. 30 days) of V.C.R.

04 Add new or amended governing law provision requiring agreement to comply with all California law, including CCPA, any amendments, and California AG regulations implementing CCPA

Issue: Will Vendors/Service Providers Agree to CCPA Amendments before Effective Date of CCPA and California AG Regulations?

- Some vendors, so far, are only agreeing to amendments covering employee data.
- Others taking wait-and-see approach until CA AG Regulations are effective – 7/1/20
- Vendors taking it seriously, but treading carefully.
- *How will companies be able to respond to V.C.R.s effective 1/1/20 without conforming vendor agreements? Will vendor agreements meet commitments of Company's updated privacy policy?*

Expectations on Vendors – Demonstrating “Compliance”

- Complete third party assessment reviews (including cybersecurity evaluation)
- Obtain information on: Data retention practices, Deletion practices and processes, Access requests practices and processes
- Identify incident notification channels and processes
- Review Data Maps/Data Flows
- Identify whether there is any onward transfer
- Review CCPA Compliance White Paper, etc.

Some CCPA Best Practices

- Map the definitions of “P.I.” and “sell” to your business activities
- Conduct a gap assessment
- Break down CCPA obligations into achievable and distinct projects
- Data Mapping/Data Flows
- Deletion Request Process
- Access Request Process
- Evaluate your Notice, Consent and Transparency practices
- Update your Privacy Policy
- Do Not Sell Page (location and content)

Top security issues for vendor contracts

- Standard of care for administrative, technical, and physical safeguards (i.e., “industry-standard” vs. “commercially reasonable”)
- Specific compliance standards (i.e., ISO 27001)
- Right to receive security audit reports or conduct security audits (consider confidentiality provisions)
- Incident response provisions (timeline for vendor notification to client; client maintaining control of breach response and notification; cooperation with security investigations)
- Indemnification for data breaches (broadly including response, notification, remediation, credit monitoring, etc.)
- Requirement to maintain security insurance
- Flow-down security provisions to subvendors
- Employee/contractor training

Hot Topics – Food for thought

How will CCPA affect supply chain management, especially among vendors, suppliers, and their sub-contractor relationships? Will it restrict their access? Will this require formalized tracking system for all access/deletion?

How will the customer right to deletion be ensured/addressed by third parties

Will vendors be able to meet all requirements/principles of the CCPA whatever regulations are adopted by the CA AG

How should CCPA compliance be future-proofed? Does that mean applying it to all U.S. Consumers, not just to California residents

Is a high level data privacy risk assessment a good idea

Thank You

Questions and Answers?

Douglas G. Bonner
(202) 352-7500
dbonner@potomaclaw.com
Jeff Kosseff
(703) 489-9046
jkosseff@potomaclaw.com
Potomac Law Group, PLLC
1300 Pennsylvania Avenue, NW
Washington, DC 20004