

The CCPA Progeny: Data Ethics

June 22, 2021, 1:00pm ET

Julia B. Jacobson, Partner, Arent Fox LLP

About the presenter



Julia Jacobson

Partner

Arent Fox LLP

State Privacy Laws: Where are we now?

Amended:

- California Consumer Privacy Act (CCPA) and Consumer Privacy Rights and Enforcement Act (CPRA);
- Act relating to Internet Privacy (aka Nevada Opt-out of Sale Law) <https://www.leg.state.nv.us/App/NELIS/REL/81st2021/Bill/7805/Text#>

New: Virginia Consumer Data Protection Act (VCDPA)

Effective 1 Jan 2023 - <https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+SB1392ER>

New: Colorado Privacy Act (CPA, CoPA, ColoPA?)

Effective 1 July 2023 - <https://leg.colorado.gov/bills/sb21-190>

Key Consumer Right / Controller Obligation	California CPA	California PRA	Virginia CDPA	Colorado PA
Right to know/access	+	+	+	+
Right to deletion	+	+	+	+
Right to opt out of “sale”	+	+	+	+
Right to correct inaccurate personal information	X	+	+	+
Reasonable security	+	+	+	+
Right to limit use/disclosure of sensitive personal information	X	+	Process only after obtaining consumer consent	Process only after obtaining consumer consent
Other rights	X	Right to opt out of “sharing” for “cross-context behavioral advertising”	Right to opt-out of significant effect “profiling” and “targeted advertising”	Right to opt-out of significant effect “profiling” and “targeted advertising”
Data Protection Assessments	X	+	+	+

Business Ethics

“A business is a productive organization—an organization whose purpose is to create goods and services for sale, usually at a profit. Business is also an activity. One entity (e.g., a person, an organization) “does business” with another when it exchanges a good or service for valuable consideration. Business ethics can thus be understood as the study of the ethical dimensions of productive organizations and commercial activities.”*

- Environmental, Social and Governance (ESG) Initiatives - “Doing well by doing good”
- Diversity, Equity and Inclusion (DEI) Initiatives

Data Ethics

- Type of business ethics
- Evaluation of “moral problems related to **data** (including generation, recording, curation, processing, dissemination, sharing and use), **algorithms** (including artificial intelligence, artificial agents, machine learning and robots) and **corresponding practices** (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (e.g. right conducts or right values)” *

Legal Landscape

- Anti-Discrimination Laws
- Competition Laws
- Consumer Protection Laws
- Contracting / Confidentiality
- Intellectual Property Laws
- Cybersecurity Law and Standards
- Privacy Laws

What is the relationship between data ethics and the CCPA Progeny?

Trust

CCPA and the CCPA Progeny are in reaction to perceived over-collection / overuse / misuse of personal information commonly associated with automated processing

Vast data stores made possible by decreased cost and increased power of cloud computing

More data = more privacy risk, e.g., risk of re-identification, attractive to hackers

Anonymization

Per EU guidance, anonymization requires elimination of re-identification risks:

1. *Singling out risk*: is it still possible to single out an individual by isolating some or all records within a data set that identify an individual or device?
2. *Linkability risk*: is it still possible to link records relating to an individual, i.e., linking two or more records (in the same database or in different databases) relating to the same individual or device or to the same group of individuals? For example, if a third party can establish (e.g., by means of correlation analysis) that two records are assigned to the same group of individuals but cannot single out individuals in this group, then the anonymization technique eliminates the singling out risk but not linkability risk.
3. *Inference risk*: can information concerning an individual be inferred with significant probability, e.g., the value of an attribute is inferred from the values of a set of other attributes?

CPRA Preamble

“Rather than diluting privacy rights, California should strengthen them over time. Many businesses collect and use consumers’ personal information, sometimes without consumers’ knowledge regarding the business’s use and retention of their personal information. In practice, consumers are often entering into a form of contractual arrangement in which, while they do not pay money for a good or service, they exchange access to that good or service in return for access to their attention or access to their personal information. Because the value of the personal information they are exchanging for the good or service is often opaque, depending on the practices of the business, consumers often have no good way to value the transaction. In addition, the terms of agreement or policies in which the arrangements are spelled out, are often complex and unclear, and as a result, most consumers never have the time to read or understand them...

One of the most successful business models for the internet has been services that rely on advertising to make money as opposed to charging consumers a fee. Advertising-supported services have existed for generations and can be a great model for consumers and businesses alike. However, some advertising businesses today use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests. Some companies that do not charge consumers a fee subsidize these services by monetizing consumers’ personal information. Consumers should have the information and tools necessary to limit the use of their information to noninvasive proprivacy advertising, where their personal information is not sold to or *shared* with hundreds of businesses they’ve never heard of, if they choose to do so.”

VCDPA Principles

- Limit the collection of personal data to what is **adequate, relevant, and reasonably necessary** in relation to the purposes for which such data is processed, as disclosed to the consumer
- Not process personal data for purposes not reasonably necessary to, or compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent
- Establish, implement, and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data
- Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers
- Not process sensitive data concerning a consumer without obtaining the consumer's consent

Colorado PA Preamble

- “The ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society, but it has also created risks to privacy and freedom”
- “Technological innovation and new uses of data can help solve societal problems and improve lives, and it is possible to build a world where technological innovation and privacy can coexist ...”
- “By enacting [CPA], Colorado will be among the states that empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate ...”

Why consider a data ethics program?

- ✓ Rebuild and grow customer / consumer trust
- ✓ Enhance brand loyalty
- ✓ Shift focus to quality data
 - ▶ Better quality data is more valuable, e.g., anticipate customer wants and needs
 - ▶ Counterbalance limits in privacy laws and phase-out of third-party cookies
- ✓ Potential to drive revenue

Core Ethical Principles in AI/ML Frameworks

- Ethical Purpose – “Beneficial Intelligence”
- Accountability
- Transparency and Explainability
- Fairness & Non-discrimination
- Privacy & Confidentiality
- Safety and Reliability

How to get started

Who is / should be involved and when?

- Leadership
- Marketing / Sales
- Information Security
- Procurement
- Privacy

Which principles are most important to the business?

- Asking difficult questions
- Genuine commitment

How to get started

What are the data assets?

- What data *can* the business use?
 - Who “owns” the data?
 - Is it personal data?
 - Contractual restrictions?
 - Promises made to data subjects?
- What data *does* the business use?
 - Is the use necessary, consistent with principles, lawful?

How to get started

What does the organization want to do with its data assets?

- Are intended uses consistent with the ethical principles (see, e.g., core principles in AI frameworks)
- Are intended uses consistent with scope of notice and/or consent?

What needs to change?

- Ask questions first, not later
- Data retention / minimization practices
- Stakeholder involvement
- Ongoing working group

Questions?

Julia Jacobson

Julia.Jacobson@arentfox.com

617.549.1055 MOBILE

617.973.6297 OFFICE

