The California Consumer Privacy Act and Impact for Network Measurement and Research

Scott Jordan
University of California, Irvine

Who has responsibilities?

CCPA (California)

- "business":
  - for profit
  - does business in California
  - collects personal information
  - determines the purposes and means of processing of personal information
  - is large:
    - >$25M gross revenues, or
    - buys or sells personal information for >50k consumers

GDPR (Europe)

- "controller":
  - determines the purposes and means of processing of personal information
  - of consumers in Europe

What constitutes an identifier?

CCPA (California)

- a persistent identifier that can be used to recognize
  - a consumer
  - a device that is linked to a consumer
- includes
  - device identifier
  - IP address
  - cookie
  - ad identifier
  - customer number
  - telephone number
  - email address
- also includes
  - a combination of personal data that probabilistically identifies an individual or device

GDPR (Europe)

- (*similar*)

What constitutes personal information?

CCPA (California)

- information that
  - is linked (via an identifier) with a particular consumer, or
  - is reasonably linkable (via a join with other data) with a particular consumer

- includes:
  - identifiers themselves
  - Internet activity information
    - browsing history
    - search history
    - interaction with a website or app
  - geolocation
  - inferences to create a consumer profile

GDPR (Europe)

- (*similar*)

Notice requirements

CCPA (California)

- collection / use:
  - categories of personal information
  - purposes
  - categories of sources
- sharing:
  - categories of personal information
  - purposes
  - categories of parties with whom shared

GDPR (Europe)

- (*similar*)

Data minimization requirements

CCPA (California)

- collection and use limited to that provided in notice

GDPR (Europe)

- *(similar)*

+

- limited to what is necessary in relation to stated purposes

Consent requirements

CCPA (California)

- No consent requirements for collection & use.
- Consent requirements for sharing:
  - terms & conditions for business purposes
    - reasonably necessary and proportionate to achieve the operational purpose:
      - transient use, auditing, customer service, billing, order fulfilment, …
      - security, debugging
      - internal R&D
  - opt-out consent for personal information of adults
  - opt-in consent for personal information of minors

GDPR (Europe)

- Consent requirements for collection, use, & sharing:
  - terms & conditions for user-contracted services
  - opt-in consent for anything else

Deletion requirements

CCPA (California)

- upon verifiable request, a business shall delete the consumer's personal information and direct any service providers to similarly do so

- Exceptions:
  - when needed to complete a transaction, provide service requested by consumer
  - security, debugging
  - free speech
  - research

GDPR (Europe)

- erasure of personal data if no longer necessary for purpose collected or consent withdrawn

Who qualifies as a Researcher?

- academic?
- within a company?
- for profit?

What qualifies as Research?

For what purpose?

- network security?
- networking?
- R&D?
- other?

CCPA:

- scientific, systematic study and observation, including basic research or applied research that is in the public interest
- compatible with the business purpose for which the personal information was collected
- used solely for research purposes that are compatible with the context in which the personal information was collected
- not be used for any commercial purpose

GDPR:

- archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes

Protections: De-identified / Anonymous

CCPA (California)

- De-identified if and only if:
  - not linked (via an identifier) with a particular consumer, and
  - not reasonably linkable (via a join with other data) with a particular consumer
  - "subsequently pseudonymized and deidentified, or deidentified and in the aggregate"

GDPR (Europe)

- Pseudonymisation:
  - not linked
  - linkable, but requires additional safeguarded information

Protections: re-identification

Re-identification:

- technical safeguards
- protected from any reidentification attempts
- business processes that specifically prohibit reidentification

Data security:

- limit access to the research data
- prevent inadvertent release

Protections: IRB

CCPA:

- adheres to all other applicable ethics laws

Current bills

- IRB

Research exception (to what?)

CCPA (California)

- Research exempt from deletion requirements
- De-identified data exempt from collection, use, and consent requirements

GDPR (Europe)

- Research exempt from deletion requirements
- Non-PII exempt from all requirements?

WHOIS

GDPR

- ICANN and Registrars are likely joint controllers
- Personal information includes information linked to consumers
- Notice includes purposes
- Consent from domain name holders required:
  - terms & conditions for user-contracted services, or
  - opt-in consent

ICANN response

- Trying to figure out the WHOIS purpose …
- Response to query will only contain:
  - sponsoring Registrar, status, and creation and expiration dates
  - no personal data
- Registrars not required by ICANN to obtain consent
  - Pushes the issue down to Registrars:
    - Is the personal data required for the Registrar provided service?

DNS

Comcast

- Privacy Policy:
  - Collection:
    - network traffic data
  - Use:
    - marketing and advertising.
  - Sharing:
    - Opt-in consent required for sharing of personally identifiable web browsing information
    - No consent required for de-identified information
      - but de-identified not defined here …
- Public Statement:
  - we do not track the websites you visit …

Mozilla

- DoH Resolver Policy:
  - Collection:
    - Resolver may collect identifiable user data
  - Use:
    - Only for the purpose of operating the resolver service
    - No combining of collected data with other data to identify users
  - Sharing:
    - No sharing of personal information