California Consumer Privacy Act Exemptions: Illusory or Real?

Nancy L. Perkins
Arnold & Porter

Kate Godfrey
Adaptive Biotechnologies

Jill Whitby
First Republic Bank

Privacy + Security Forum

Overview

- General Exemptions
- Health Information Exemptions
- Financial Information Exemptions

General Exemptions

Privacy+ Security Forum

Personal Information

"Personal Information"

"Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"
inferences drawn from any such identifiable information … to create a profile about a consumer

Examples (*not* exclusive):

Identifiers: names, addresses, email addresses, IP addresses, geolocation data, characteristics of protected classes (race, religion, etc.), Internet or other electronic network activity, such as browsing history

- **Is information "personal information" if *anyone* could "reasonably link" it to a particular consumer?**

Exemption: Publicly Available Information

- **“Publicly Available Information”**
  - “information that is lawfully made available federal, state, or local government records”
- **NOT:**
  - information that is publicly available on social media sites, business websites, or any other non-governmental source of information made available to the public
  - biometric information collected by a business about a consumer without the consumer’s knowledge

Exemption: Deidentified Information

- **"Deidentified" Information:** Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, *provided that a business that uses the information:*
  - Has technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;
  - Has business processes that specifically prohibit reidentification of the information;
  - Has implemented business processes to prevent inadvertent release of deidentified information; and
  - *Makes no attempt to reidentify the information*
- **If someone holds a key linked to the identity of an individual, can information about that individual ever be "deidentified"?**
- **What does this mean for research?**

Business Information ("B2B") Exemption

- Until January 1, 2021, most CCPA obligations on a business do not apply to personal information:
  - about a consumer acting as an entity representative (employee, owner, director, officer, contractor)
  - "reflecting" a communication or transaction between the business and the consumer" that:
    - "occurs solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from the entity the consumer represents"
- LIMITS of exemption:
  - consumers maintain private right of action for breach of security of such personal information
  - consumers maintain right to opt out of sales of such personal information

Meaning of B2B Exemption?

- When does personal information "reflect" a business' communication during due diligence or about providing or receiving a product or service?
  - Must the personal information have been provided during such a communication?
  - Would contact information for a company CEO found by a business on the company's website "reflect" a subsequent contact with the CEO about negotiating for purchase or sale by the business of a product of that company?

Employment-Related Exemption

- **Employment-related information:** Until January 1, 2021, most CCPA obligations on a business will not apply to personal information:
  - About the consumer and collected and used solely in the context of a consumer acting (currently or formerly) as the business' job applicant, employee, owner, director, officer, or contractor;
  - Provided as emergency contact information or needed to, and collected and used solely to, administer benefits for another person relating to a consumer acting as the business' job applicant, employee, owner, director, officer, medical staff member, or contractor.
- **Limits of Exemption**
  - Notice must still be provided to regarding collection of such information and the purpose for its collection
  - Consumers maintain private right of action for breach of security of such personal information

Credit Report-Related Exemption

- **Expanded by recent CCPA amendments**
- **Exemption now extends to any activity:**
  - involving personal information that is “consumer report” information under the federal Fair Credit Reporting Act (“FCRA”);
  - undertaken by a consumer reporting agency or a furnisher or user of such information;
  - to the extent the activity is regulated by FCRA and the personal information is not used or disclosed except as permitted by FCRA.

Health Information Exemptions: Compliance Challenges

Privacy+ Security Forum

Health Information Exemptions

1) **Medical information governed by the California Confidentiality of Medical Information Act ("CMIA") or "protected health information" ("PHI") collected by a covered entity or business associate under HIPAA**

2) **Other information maintained by an HCP (as defined by CMIA) or a HIPAA covered entity *if protected in the same manner as PHI***

3) **Information collected as part of a *clinical trial* subject to the Common Rule, clinical practice guidelines issued by the International Council for Harmonisation, or pursuant to human subject protection requirements of the FDA**

Challenge: “other” information

Personal information not created or collected as part of the payment, treatment or health care operations trifecta

HIPAA covered entities may engage in activities that involve the collection of personal information from individuals who are not patients or individuals covered by a health plan.

For example, a covered entity may collect personal information from a member of the public for marketing purposes or as part of its community engagement activities.

Challenge: no HIPAA covered entity

Privacy+ Security Forum

Information that was never PHI (or is excluded from the definition of PHI) under HIPAA

Information that identifies an individual and relates to the individual's health is not PHI unless is it *created or received* by a health care provider, health plan, employer, or health care clearinghouse.

Possible examples:

- email address, device identifiers, biometrics, geolocation and other personal data that could be associated to a person's physical movements, use of websites or online services, and other activities that do not necessarily pertain to health, treatment or payment for treatment

- normal web traffic and similar behaviors tracked and collected by covered entities engaged in activities so mundane as hosting an informational website

Challenge: de-identified data

Information that was once PHI, but has been de-identified under HIPAA

- Health information that has been de-identified in accordance with HIPAA is not PHI, and, thus, is no longer subject to the CCPA carve-out for PHI.
  - Standards for de-identification under HIPAA are different than those under CCPA, so de-identified PHI under HIPAA may still constitute Personal Information under CCPA

De-Identified: HIPAA vs CCPA

Privacy+ Security Forum

HIPAA Privacy Rule defines "de-identified":

- A covered entity may determine that health information is not individually identifiable health information only if:
  - (1) **Expert Method:** A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.
  - (2**) Safe Harbor:**
    - **(**i) All of 18 types of identifiers of the individual or of relatives, employers, or household members of the individual, are removed; and
    - (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

CCPA defines "de-identified":

- Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses the information:

  (1) Has technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;

  (2) Has business processes that specifically prohibit reidentification of the information;

  (3) Has implemented business processes to prevent inadvertent release of deidentified information; and

  (4) Makes no attempt to reidentify the information.

Challenge: Inferences

Inferences derived from PHI

Inferences drawn from PHI used to create a new information set that contains no PHI may be CCPA Personal Information

CCPA “personal information” includes “inferences” drawn from information “that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to” a California resident or household.

Example: inferences are drawn from PHI and used to create a new data set that is used for enhancing customer experience, fraud detection or marketing activities.

Deletion of research data

CCPA: "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."

Exception: Where necessary to maintain personal information in order to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, IF:

- research adheres to all other applicable ethics and privacy laws;
- deletion of the information is likely to render impossible or seriously impair the achievement of such research; and
- consumer has provided informed consent to the research.

Deletion right exception limits

Research must be "public," "peer-reviewed," and in the "public interest."

Research using personal information that may have been collected *in the course of interactions for other purposes:*

(1) must "not be used for any commercial purposes"

- *Did the CA legislation intend this, or did it intend to require that the **personal information** not be used for a commercial purpose?*

(2) must be "used solely for research purposes that are compatible with the context in which the personal information was collected."

- *Is the collection of patient data for treatment (including lab test) purposes "compatible" with a research purpose?*

(3) Protected from any reidentification attempts

- *Does this mean after the research is completed?*

The GLBA/CalFIPA Exemption

Privacy+ Security Forum

What is the GLBA/CalFIPA Exemption?

The CCPA does not apply to personal information ("PI") collected, processed, sold or disclosed "pursuant to" the Gramm-Leach-Bliley Act ("GLBA") or California Financial Information Privacy Act ("CalFIPA")

GLBA/CalFIPA Exemption is Limited

- **GLBA/CalFIPA applies to "nonpublic personal information" ("NPPI") about a "consumer"**

- **"Consumer" under the GLBA/CalFIPA:**
  - an individual (or his/her legal representative) who has applied for, obtains, or has obtained
  - a financial product or service from a financial institution ("FI")
  - to be used *primarily for personal, family or household purposes*

NPPI under the GLBA/CalFIPA

- **NPPI ("GLBA "personally identifiable financial information"):**
  - Information a consumer provides to a FI *to obtain a product or service* from the FI
  - About a consumer resulting from any *transaction involving a product or service* between the consumer and the FI
  - That the FI otherwise obtains about a consumer *in connection with providing a product or service* for that consumer

- **Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable personal information that is not publicly available**

What Personal Information is NOT NPPI?

- **NOT NPPI:**
  - prospecting information
  - information from account aggregators, social media profiles
  - profiles built on the information listed above

- **Maybe not NPPI?**
  - website behavior, keystroke/mouse patterns and rhythms
  - web history/tracking, clickstream data
  - geolocation
  - profiles built on these

GLBA/CalFIPA Customer Considerations

- **FI obligations to respond to CCPA consumer requests will not apply to:**
  - Deposit account set up information, transaction information, online account activity, loan application information, information used in underwriting, payment and balance history, investment and portfolio activity and information and the like would not be produced
- **How will consumers react to that information void?**
  - Will they understand or accept the messaging of why information was excluded from the response?
  - Customer lifecycle database notes/comments and profiling information will stand out

GLBA/CalFIPA Customer Considerations

- **Regardless of whether FI response to an individual rights request excludes GLBA/CalFIPA NPPI**
  - How does the FI preserve trade secrets?
  - How does the FI produce information such as clickstream data, website behavior, keystroke/mouse patterns and rhythms?
    - Do you want to produce that information if it is developed and used for fraud detection purposes?

- **How are consumer follow-on questions answered and who answers them?**

Prospecting Considerations

- **If the FI relies on a centralized marketing function, individual rights responses may be a light lift**
- **But! PI developed and used by the FI in prospecting may surprise the public**
  - Profiling information from resolution services – estimated age, salary, marital/family status, personal interests
- **Even if FI relies on a centralized marketing function, sales personnel may engage in their own intelligence gathering**
  - Google alerts, LinkedIn, Facebook, Social Media
  - Inadvertent (?) capturing of PI of other individuals
- **When does a lead become a customer and how does that shape the response to an individual rights request?**
  - Does the 12-month clock restart if prospecting data is revisited?

Visitor Considerations

- **Personal information on individuals who use the FI for isolated transactions are outside the scope of GLBA/CalFIPA:**
  - Wires, check cashing, money order purchases, ATMs
  - On premises or ATM video/audio recordings
  - Web data - cookies and similar technologies, website behavior, geolocation
  - What information is reasonably capable of being associated with or linked directly or indirectly with a particular consumer or household?

B2B Exemption

How does an FI respond to an individual rights request from a customer who is both a consumer customer and a business customer?

Speaker Contact Information

Nancy L. Perkins
Arnold & Porter
(202) 942-5065
nancy.perkins@arnoldporter.com

Kate Godfrey
Adaptive Biotechnologies
(206) 693-2227
kgodfrey@adaptivebiotech.com

Jill Whitby
First Republic Bank
(415) 364-4916
jwhitby@firstrepublic.com