Proposed "American Privacy Rights Act" Could Change How Alarm Industry Handles Customer Data, Surveillance.

The Bipartisan/bi-cameral "American Privacy Rights Act" (APRA) was introduced on April 7, 2024, and it appears to be on a fast track as Americans grow tired of repeated breaches of their sensitive information. If enacted, the APRA would require significant changes for all but the smallest of companies. Below is a more detailed analysis of the potential impact on the alarm industry.

NOTE: Nothing in this article constitutes legal advice, and the applicability of the proposed legislation should be reviewed on a case-by-case basis to determine applicability to a particular company's practices. This overview does not touch on all provisions of APRA. You are encouraged to view the full text of the bill at:

American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf (d1dth6e84htgma.cloudfront.net)

PERMISSIBILITY OF GATHERING, RETAINING AND TRANSFERRING DATA

The draft APRA restricts the collection, processing, retention and/or transfer of "covered data", which is defined as "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals." In general, companies must not collect, process, retain or transfer covered data "beyond what is necessary, proportionate, and limited to provide or maintain" their services and relationship with the customer. Section 3(d) of the draft Act defines several situations in which the collection and use of covered data is permissible. At least three of these allowances appear to authorize alarm company data collections, with subsection (11) most directly addressing typical alarm operations (and echoing AICC language provided for a prior privacy bill). Under these allowances, an alarm company could collect and use data that is necessary, proportionate, and limited:

(11) To prevent, detect, protect against, or respond to an ongoing or imminent network security *or physical security incident, including an intrusion or trespass, medical alerts, fire alarms, or access control*.

(12) *To prevent, detect, protect against, or respond to an imminent or ongoing public safety incident (such a mass casualty event, natural disaster, or national security incident)*, excluding the transfer of covered data for payment or other valuable consideration to a government entity.

(13) Except with respect to health information, *to prevent, detect, protect against, investigate, or respond to criminal activity*, excluding the transfer of covered data for payment or other valuable consideration to a government entity. *[Emphasis added]*

Here are alarm companies' typical business practices that appear to qualify under Section 3(d)(11) of APRA (except as noted):

1. Collecting customer identity and address information: Should qualify, but **social security, passport or driver's license information may be questionable unless alarm co. can show why it is needed.**

2. Recording and retaining phone calls coming into the central station.

3. Video surveillance of protected premises.

4. Controlling access to protected premises.

5. Status monitoring: pipeline pressure, refrigeration temperature, etc.: If there is a threat of fire or explosion if monitored functions exceed safe limits, should qualify as needed to detect **medical alerts or fire alarms** under Section 3(d)(11). If threat of harm to the public (e.g., chemical release), monitoring should also qualify as a "public safety incident."

6. PERS fall alert/medical alert: Should qualify as data needed to "detect **medical alerts**." Elderly persons are likely to suffer injury in a fall.

7. Cargo tracking: Appears to qualify as data needed to detect **an intrusion or trespass,** as tracking is to detect theft, damage, etc.

8. Customer location tracking:

   Appears to qualify, as tracking of customer (or its personnel) is in part to make sure that company personnel and assets are not being attacked, kidnapped, stolen, or involved in a dangerous situation. If guards are being tracked, this should qualify as being needed to protect against or respond to a security incident, with is a guard's job description.

   a. Presence Awareness (e.g., use of data regarding the location of the customers, their family members for persons on the call list) likewise appears to qualify.

9. Customer billing/accounting info: Section 3(a)(1)(A) of APRA expressly allows collection of data necessary, proportionate, and limited to provide or maintain . . . a specific product or service requested by the individual to whom the data pertains, **including any associated routine administrative, operational, or account-servicing activity such as billing**, shipping, delivery, storage, or **accounting".**

10. Customer complaint info: Section 3(a)(1)(B) of APRA allows data necessary to maintain customer communications "reasonably anticipated within the context of the relationship", which should cover customer complaint information.

11. Marketing services, etc. to existing customers: While "targeted advertising" is restricted, this term would not include:
    (i) advertising or marketing content to an individual in response to their specific request for information or feedback;
    (ii) first-party advertising based on an individual's visit to a website or online service that offers a product or service that is related to the subject of the advertisement;
    (iii) contextual advertising when an ad is displayed online based on the content of the webpage or online service on which it appears; or

(iv) data solely for measuring or reporting advertising, marketing, or media performance, reach, or frequency, including by independent entities.

Other forms of marketing would have to be evaluated under APRA.

12. Employee information: Section 2(9)(b)(ii) expressly excludes "employee information" from the definition of "covered data". Therefore, collection of employee data is generally not restricted; however, the employer must only collect data defined as allowed employee info per Section 2(19) of APRA. This definition appears broad enough to include a criminal background check, but other state statutes may restrict how such info is used. NOTE: The fact that employee information is "excluded" rather than simply being a permitted collection should mean that most of the other requirements of the APRA do not apply to this information (such as the opt out option, transparency notice requirement, etc. discussed below).

APRA Requirements Applicable to "Permissible Data Collections": While the above alarm company data collections are "permissible", they are not "exempt" (except for employee info) and thus companies must still comply with the other new requirements of APRA re customer info:

OBTAINING CUSTOMER OPT IN FOR "SENSITIVE COVERED DATA"

- **Affirmative Consent:** Customer approval (i.e., "opt in") is needed to collect or transfer "sensitive covered data", e.g.:
  - SSN, driver's license, passport info, etc.: Collected from certain customers? (e.g., bad credit risk/delinquency)
  - Bank, credit card, debit card or other financial information:
  - Voicemails, emails, texts, login/password, telephone call registers, etc.
  - Geolocation information: Part of cargo or security guard tracking, and possibly PERS? (FCC just issued $200 million

in fines against big carriers for selling customer geolocation data without customer consent.)

- Videos or photos showing sex or nudity: Could someone misbehaving within range of your video surveillance cameras create a legal issue for your company?

- Biometric" data: Affects medical PERS?

- Equity requirement: Must not "collect, process, retain, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national 20 origin, sex, or disability." Includes impact due to use of algorithm. How do you avoid unintended disparate impact outcome?

- ***The handling of "sensitive covered data" may dictate changes in customer contracts to include opt in language & signature line.***

REQUIREMENT TO CREATE OPT OUT OPTIONS

APRA would impose a requirement to create certain options for their customers to opt out of the collection of "covered data":

- Individuals can opt out of certain data collections, transfer of their info, and targeted ads based on their data at any time.
- If you change your privacy policy in a material way, *or if you undergo an ownership change, merger, etc.*: You must give customers notice and opportunity to opt out.
- Opt out procedure must be well publicized and easy to follow.
- Individuals must be able to edit their data easily.
- You cannot retaliate by refusing service or raising prices.

REQUIREMENT TO PROVIDE TRANSPARENCY NOTIFICATIONS

APRA would impose a requirement to provide transparency notifications in the manner and with the content required by APRA.

ADDITIONAL REQUIREMENTS FOR LARGER ALARM COMPANIES

- Certain alarm companies could be considered "large data holders" as defined in the APRA, subjecting them to additional requirements:
    - **Must publish privacy policies from the past 10 years:** Would require keeping a log of policies and any material changes going forward.
    - **Must publish annual transparency reports about consumer requests.**
    - **Must Conduct biennial audits and privacy impact assessments.** – Not clear that this provision requires third-party audits, but even if done in-house it requires more time and resources and adds more compliance overhead.
    - **Must submit annual certifications of compliance to the FTC:** Could become a "gotcha" in a subsequent enforcement action.

    Large Data Holder Definition: annual gross revenue of not less than $250,000,000 and, collected, processed, retained, or transferred—

    (i) the covered data of—

    (I) more than 5,000,000 individuals;

    (II) 15,000,000 portable connected devices that identify or are linked or reasonably linkable to 1 or more individuals; and

    (III) 35,000,000 connected devices that identify or are linked or reasonable linkable to 1 or more individuals; or

    (ii) the sensitive covered data of—

    (I) more than 200,000 individuals;

(II) 300,000 portable connected devices that identify or are linked or reasonable linkable to 1 or more individuals; and

(III) 700,000 connected devices that identify or are linked or reasonably linkable to 1 or more individuals.

DATA SECURITY REQUIREMENTS

APRA would impose requirements to implement additional data security measures, including appointment of a Data Security Officer and deployment of updated technology as necessary. Issue: How can companies assure compliance when privacy/cybersecurity technology constantly evolves? Can APRA create a "safe harbor" based on e.g., Federal cybersecurity standards?

OTHER ISSUES OF CONCERN

- **Private Right of Action** - APRA would provide a broad individual private right of action for noncompliance, unlike certain state laws where private rights for action are limited. Also, APRA could be enforced by the FTC and state AGs, which could increase enforcement actions.
- **Preemption/Exceptions** - Generally APRA would preempt state laws, but it includes carveouts allowing for recovery under certain state laws (e.g., Illinois's BIPA and GIPA, and security breach damages under the CCPA). So there could be claims under both APRA and the above state laws for the same issue.
- **Effective Date** - If passed, APRA would go into effect in 180 days, which is a short timeline. Some of the provisions may be delayed and contingent on the FTC implementing regulations, but still a short runway for the ambitious set of new requirements.
- **Submit annual impact assessments to the FTC when AI poses a consequential risk of harm:** It is probably just a matter of time before AI is in use throughout alarm technologies and practices.

ON THE POSITIVE SIDE:

- Small businesses are exempt: Under $40m avg. gross revenues in past 3 years, holds “covered data” for fewer than 200,000 individuals, doesn’t sell that data.
- A company can submit their compliance program to FTC for an approval certification that creates a rebuttable proof of compliance.

AICC/TMA is reaching out to Capitol Hill to discuss some of the concerns identified above, so further clarifications or changes may be coming. Association members will want to monitor this legislation closely and size up how compliance would affect them, and perhaps change their business practices and contracts.