Analysis of "American Privacy Rights Act": Input Welcome

The Bipartisan/bi-cameral "American Privacy Rights Act" was introduced on April 7, 2024, and it appears to be on a fast track. It is time to quickly determine how the bill will affect alarm industry, and determine what advocacy may be appropriate. In particular, are there restrictions that will make it difficult to timely and effectively handle alarms? Do the exceptions in the Act adequately cover the industry?

In general, the new bill would --

- limit the type of data companies can collect and use. Need to have good justification for collecting SSNs, other data now routinely acquired.

- require a transparency notice about how data is used, in the manner required by the Act.

- impose data security measures that each company must follow, including appointment of a Data Security Officer, and deployment of technology as necessary to meet the standard.

- broaden enforcement options, allowing FTC, State AGs, and consumers to bring actions for violations of the Act.

- allow multiple consumer opt out rights:
    - Individuals can opt out of certain data collections, transfer of their info, and targeted ads based on their data.
    - 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 do.
    - Individuals must be able to edit their data easily.
    - You cannot retaliate by refusing service or raising prices.

- preempt many state privacy laws, with exemptions for certain health and consumer protection laws. This is one potential silver lining of federal legislation, by creating uniformity.
    - This is also the biggest remaining controversy concerning passage of this legislation, and halted previous Fed. Privacy bills.

- Specific provisions that may impact alarm companies:
    - Approval needed to collect or transfer "sensitive covered data", e.g.:
        - SSN, driver's license, etc.: Likely collected from all employees and perhaps contractors.
        - Bank, credit card, debit card or other financial information: Likely collected from all customers.
        - Voicemails, emails, texts, login/password, telephone call registers, web search history, etc.: Likely collected from employees and perhaps customers.
        - Geolocation information: part of cargo or security guard tracking, and possibly PERS?
        - Background info re job applicants: will it be more difficult to get the information needed to thoroughly vet applicants?
        - Bill restricts use of sex videos, computer/AI-generated sex photos, nudity and similar items. Could someone misbehaving within range of your video surveillance create a legal issue for your company?

    - Must get affirmative consent to collect, retain or transfer "biometric" data: Affects medical PERS?

    - Equity requirement: Must not "collect, process, retain, or transfer covered data in a manner that discriminates in <u>or otherwise makes unavailable the equal enjoyment of goods or services</u> 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 requirements of the Bill are complex enough that if it becomes law, each alarm company will want to dedicate personnel and resources (including legal advice) to implement compliance, and have a manual and checklist in place to ensure it is followed in the future.

    - The Bill will likely change how alarm companies interact with their customers, employees and possibly suppliers/contractors.

    - There are certain exceptions that may prove valuable in protecting alarm companies from adverse effects, depending on the particular practices of each company. For example, companies are allowed to collect and retain data necessary to:
        - Protect data security
        - Comply with Federal, State or Tribal law (that has not been preempted).
        - Comply with a legal subpoena or defend against legal claims.
        - Implement a product recall
        - Do market research
        - Develop or enhance a product (if you "de-identify" the data)

    - 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.

PLEASE PROVIDE ANY INPUT ON HOW THE PRIVACY BILL MAY ADVERSELY AFFECT ALARM COMPANIES TO TMA/AICC AS SOON AS POSSIBLE.

NOTE: This analysis seeks to provide an overview summary, and does not touch on all provisions of the proposed Privacy bill. You are encouraged to view the full details for yourself. The text of the bill can be found at:

American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf (d1dth6e84htgma.cloudfront.net)