

Personal Information, Private Information, Personally Identifiable Information...What's the Difference?

Article By:

Joseph J. Lazzarotti

When privacy geeks talk “privacy,” it is not uncommon for them to use certain terms interchangeably –personal data, personal information, personally identifiable information, private information, individually identifiable information, protected health information, or individually identifiable health information. They might even speak in acronyms – PI, PII, PHI, NPI, etc. Blurring those distinctions might be OK for casual conversation, but as organizations develop data privacy and security compliance programs, the meanings of these terms can have significant consequences. A good example exists within the California Consumer Privacy Act (“CCPA”) and its interaction with other laws.

The CCPA, effective January 1, 2020, contains an expansive definition of “personal information.” See [Cal. Civ. Code Sec. 1798.140\(o\)](#). The basic definition is 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. The definition goes on to enumerate, without limitation, certain categories of information (e.g., identifiers, website activity, biometric information, geolocation) if they identify, relate to, describe, are reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. With respect to this broad set of data, the CCPA extends to California consumers substantial rights, including the right to request deletion of that data or to opt-out of its sale.

The CCPA’s private right of action for data breaches, however, applies to a much narrower subset of “personal information” defined above. Specifically, the CCPA incorporates another section of California law, [Cal. Civ. Code Sec. 1798.81.5\(d\)\(1\)\(A\)](#), to define personal information that, if breached, and which the owner failed to reasonably safeguard, could expose the owner to statutory damages of up to \$750 per person. For this purpose, personal information means:

An individual’s first name or first initial and the individual’s last name in combination with any one or more of the following data elements...:

(i) Social security number.

(ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government

document commonly used to verify the identity of a specific individual.

(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

Note also that the CCPA excludes certain information from its general definition of personal information, such as "[protected health information](#)" maintained by covered entities and business associates under the Health Insurance Portability and Accountability Act ("HIPAA").

But the PI, PII, PHI...conundrum does not end with the CCPA. An organization with CCPA obligations also may maintain "private information" of New York residents. Under the [New York Stop Hacks and Improve Electronic Data Security Act](#) ("SHIELD Act"), that organization would have to adopt reasonable safeguards to protect "private information" which is defined to mean, in general, any information concerning a natural person which, because of an identifier, can be used to identify such natural person if it is in combination with any one or more of the following data elements:

- *social security number;*
- *driver's license number or non-driver identification card number;*
- *account number, or credit or debit card number, which alone or together with a required code would permit access to an individual's financial account;*
- *biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity.*

Private information also includes a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Confused yet? Perhaps your organization is not subject to the CCPA or the NY SHIELD Act, but you own and operate a website that collects personal information from consumers who reside in California and Delaware. Laws in those states require a website private policy that describes certain practices concerning "personally identifiable information" defined [in Delaware](#) to mean:

any personally identifiable information...collected online by the operator...from that user...including a first and last name, a physical address, an e-mail address, a telephone number, a Social Security number, or any other identifier that permits the physical or online contacting of the user, and any

other information concerning the user collected by the operator...from the user and maintained in personally identifiable form in combination with any identifier described in this paragraph.

A similar definition exists under the [California law](#). These distinctions just scratch the surface and add to the complexity of the emerging patchwork of data privacy and security law in the United States.

So, when thinking about personal information, it is important to remember that not only does the definition extend beyond just one's name and social security number, but the term itself and its definition likely will differ depending on the particular statutes or regulations you are analyzing. When assessing an organization's threats and vulnerabilities to personal information, or preparing policies and procedures to safeguard it, be sure to develop an appropriate definition that takes into account the necessary elements of data.

Jackson Lewis P.C. © 2024

National Law Review, Volumess IX, Number 364

Source URL:<https://natlawreview.com/article/personal-information-private-information-personally-identifiable-information-what-s>