CITE AS
39 *Energy & Min. L. Inst.* 14 (2018)

Chapter 14

Personally Identifiable Information and the Energy Industry

Mary L. Fullington
Wyatt, Tarrant & Combs, LLP
Lexington, Kentucky[1]

Synopsis

§ 14.01. What is "Personally Identifiable Information" (PII)?

The term "personally identifiable information" ("PII") in the context of the law of data privacy and security is used to refer to information that alone or in combination with other information can be used to identify a natural person. Its precise definition varies from source to source. In almost all states in the United States, PII consists of a first and last name, a social security number, other government issued identification number such as a driver's license number or a passport number, and all information which, in combination, facilitates access to financial accounts of any type, such as usernames and passwords. Even dates of birth and the maiden name of an individual's mother may constitute PII because they are both commonly used in combination with other information to confirm the identity of an individual. In some states, biometric information constitutes PII, such as the data that facilitates identification by facial, retinal, iris, and thumbprint identification software. This is the type of information to which the unauthorized access may result in the imposition of legal obligations on the party who possessed the information at the time it was accessed.

---

1 The opinions expressed in this chapter are the author's alone and should not be attributed to Wyatt, Tarrant & Combs, LLP. Nothing in this chapter should be construed as legal advice.

PII is not the only personal information in need of protection. Some states impose obligations resulting from the unauthorized access of personal information deemed "sensitive." Sensitive personal information, or SPI, may include electronic or physical information about an individual's medical treatment, diagnosis or history, tax information, and health insurance information.

If your company has employees, it possesses PII and SPI. If it issues 1099s to any individuals, it possesses their PII and SPI. In this respect, companies operating in the energy field are no different from many companies in any industry unless they are collecting, analyzing, or storing detailed "smart grid" data which, in combination with an address, can potentially reveal sensitive information regarding individual inhabitants.

§ 14.02. Threats to PII and SPI.

For it is no longer a question of "if," but "when" and "how often."

Robert S. Mueller
Director, FBI
March 1, 2012

The energy industry may be comforted to know that the majority of the security breaches in 2017 occurred in the healthcare and the hospitality industries together with public agencies. These sectors accounted for about fifty-three percent (53 percent) of security breaches in 2017.

The motive behind security threats to PII is almost always financial. It is used by criminals to commit identity fraud, file fraudulent tax returns to receive refunds, apply for loans or credit cards, or to sell to someone else who intends to use it for one or more of those purposes. Of nine (9) classifications of data compromised in 2017, PII was at the very top of the list ahead of payment card data, medical information, and access credentials. Almost forty percent (40 percent) of all data breaches in 2017 involved PII.[2]

No matter how good your organizational and technical data security policies and procedures are, PII in your company's possession is always

---

2 2018 Data Breach Investigations Report, 11th Ed., Figure 9, page 7, Verizon (2018). [hereinafter cited as *2018 DIBR*]