It Appears The Law Is Trending Towards Providing Fewer Privacy Protections To Individuals...

by Proud Usahacharoenporn

Although we are in an era where privacy rights in one's electronic data are particularly important given the sheer wealth of personal information that is stored electronically—from health data to personal shopping preferences to GPS locations—it appears that in many ways, the law is trending towards providing fewer privacy rights to individuals.

For example, in December 2015, the Cybersecurity Information Sharing Act ("CISA") was enacted in order to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes."[1] CISA allows businesses to share cyber threat information, including data from or concerning private citizens, with federal agencies in the interest of security. CISA was passed despite being a hotly contested bill, with opposers objecting that the law jeopardizes citizens' privacy rights in their electronically-stored data.

This tension between national security and individual privacy came to a head earlier this year when the FBI moved to compel Apple to unlock the phone of Syed Farook, who was involved in the San Bernardino shooting.[2] The Central District of California issued an order compelling Apple to assist the FBI's investigation, over Apple's objection. However, before the order became final, the FBI withdrew its motion because a third party was able to unlock the phone without Apple's assistance.

In May 2016, this trend toward fewer privacy rights was taken a step further when a federal court ordered Paytsar Bkhchadzhyan to provide her fingerprint to unlock her iPhone so that the authorities could collect evidence from her phone to use in its criminal investigation against her.[3] This was ordered over the defendant's objection that providing her fingerprint for this use violated her Fifth Amendment right against self-incrimination.

This trend applies in the civil context as well. In the recently-decided case of *Spokeo v. Robins*,[4] the United States Supreme Court made it more difficult for individuals to prevail on statutory claims relating to the invasion of electronic privacy. In that case, the plaintiff alleged that a website that inaccurately reported his marital status, income level, and education violated the Fair Credit

Reporting Act ("FCRA"), which was enacted to promote the accuracy of personal data reported by consumer reporting agencies. The U.S. Supreme Court held that the plaintiff was required to affirmatively prove he suffered an injury that is both particularized and concrete in order to have standing to sue for a FCRA violation—over the plaintiff's objection that the FCRA assumes consumers are injured when their personal information is inaccurately reported because the FCRA provides for statutory penalties.

However, this apparent trend towards fewer individual privacy rights in electronic data does not mean that companies can be lax about their privacy policies and protocol. Famously, in 2015, Target agreed to pay over $39 million in a settlement relating to the company's widespread data breach.[5] Earlier this year, a court approved a settlement requiring Sony to pay approximately $8 million to victims of its data breach.[6] In light of these severe potential consequences, companies should be proactive about regularly reviewing and revising their privacy policies and security measures, and should consider obtaining cyber liability insurance.

---

1 S.754—114th Congress (2015-2016).
2 *USA v. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300*, C.D. Cal. Case No. 5:16-cm-00010-SP.
3 *See, e.g.*, http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html, http://www.computerworld.com/article/3063607/security/iphone-fbi-finger-itbwcw.html.
4 *Spokeo v. Robins*, 136 S.Ct. 1540 (2016).
5 *In re: Target Corporation Customer Data Security Breach Litigation*, D. Minn Case No.14-md-02522.
6 *Corona v. Sony Pictures Entertainment Inc.*, C.D. Cal. Case No. 14-CV-09600.

Proud Usahacharoenporn
(714) 338-1885
pusaha@rutan.com

To see related articles listed below click here

Is Your Website Privacy Policy Compliant | Privacy and Security Concerns Resulting From A Lack of Regulation of IoT Devices and the Data Collected Therefrom | Cybersecurity Strategies for Small and Middle-Market Companies