GT GreenbergTraurig | 50th ANNIVERSARY

Cybersecurity, Privacy and Crisis Management | Advisory

January 2017

Seven Privacy Tips & Recent Developments in Honor of Privacy Day

To celebrate Privacy Day (Jan. 28), here are updates on selected recent developments in cybersecurity and data privacy, as well as some tips on the use of personal information.

1. Internet of Things - Security by Design

Devices connected to the internet ("IoT devices") often have access to critical and highly personal information about their users. Security vulnerabilities or deficiencies can cause the unauthorized disclosure or modification of highly sensitive information collected by an IoT device. Recent events have also demonstrated that IoT devices can be turned into a conduit for harmful attacks on other equipment connected to the internet. These deficiencies are receiving attention from consumer protection agencies and class action litigators.

Recent litigation and enforcement actions indicate that IoT device manufacturers are expected to adopt security measures to help protect the data collected and processed by these devices. IoT manufacturers are expected to build security into each device at its creation and use ongoing measures to ensure security throughout the life of the product and service. As part of the security by design process, manufacturers are expected to conduct privacy and security risk assessments, as well as to minimize the amount of data they collect and retain. Manufacturers should also consider testing products' security measures before launching them, monitoring their products throughout their life cycle, and—to the extent feasible—patch known vulnerabilities.

2. Ransomware

Ransomware is a key threat for enterprises. Ransomware takes advantage of weak IT safeguards. Taking the following actions may help to prevent and mitigate loss from ransomware:

- maintaining the most updated operating system version to help ensure security;
- updating firewalls, and antivirus and malware software;
- training employees to raise awareness about strong passwords, social engineering, and social media use;
- frequently backing up your data off-network or to the cloud;
- adding a response plan for ransomware to your company's written security incident response plan; and
- purchasing or updating existing cybersecurity liability insurance that includes coverage for ransomware.

3. EU General Data Protection Regulation

It is well known that the EU General Data Protection Regulation (GDPR) will apply to the processing of personal data for entities established in the EU/EEA, effective May 25, 2018.

It is less known that it also applies to the processing of personal data of EU/EEA residents by an entity that is not established in the EU/EEA, including if the processing relates to the offering of goods or services to these individuals or the monitoring of an individual's behavior.

The GDPR creates significant obligations for non-EU/EEA entities. For example:

- there are stringent rules for what can qualify as "consent" to the processing of personal data of EU/EEA data subjects;
- companies must document their data protection and compliance activities in writing and keep detailed records that may be reviewed by the applicable supervisory authority;
- companies must designate in writing a representative in the EU/EEA (with exceptions);
- companies must promptly respond to a breach of security. They must notify the competent supervisory authority "without undue delay" and, if feasible, no later than 72 hours after the breach occurs;
- if the breach is likely to result in a high risk to the rights and freedoms of individuals, the company must also inform the data subjects of the breach without undue delay, unless an exception applies;
- there are significant administrative fines attached to violations of the GDPR, and each Member State may define other penalties applicable to infringements of the GDPR. Fines for violations of the basic GDPR principles can reach EUR 20 million or 4 percent of the total worldwide annual turnover of the company for the preceding financial year, whichever is higher.

4. United Kingdom - Brexit

Despite Brexit, UK businesses should continue with (or indeed commence) their General Data Protection Regulation (GDPR) compliance programs. The UK will implement the GDPR, and the GDPR will apply to UK companies that process EU personal data even after the UK has left the EU.

5. China – Cybersecurity Law

China recently adopted a new cyber security law. The law, to be effective on June 1, 2017, reiterates and strengthens the existing regime protecting personal information of individual users. Network operators must safeguard the secrecy of personal information collected. The collection and use of personal information must follow the principles of legitimacy, rightfulness, and necessity. Data collectors must disclose their data collection practices and obtain individuals' consent. In case of a breach of security, network operators must report the breach to the relevant authority, and must contact affected users.

Although these requirements and constraints apply to "network operators" only, other business operators who collect consumers' personal information by other means should consider following the same principles and guidance.

6. Personal Privacy - Social Media

Beware of the potential pitfalls of social media. Explore and understand the privacy settings on your social media accounts to help ensure you are comfortable with how your information is shared.

Think carefully about what you post to your social media account, including who may see it and how it may be perceived now and in the future. Even if you deactivate your social media account, or delete old posts, pictures, and other content, your information still may be retained on social media backup servers, in copies of webpages cached (*i.e.,* saved) by search engines, and by third parties.

7. Personal Electronic Privacy

In terms of maintaining your personal electronic privacy, there are certain measures you can take as well:

- cover your laptop's camera when not in use can prevent hackers from being able to view what you are doing without your knowledge;
- practice safe browsing;
- take advantage of the full-disk encryption that may be already offered on your computer;
- use a privacy screen to help prevent others from potentially seeing confidential and/or protected information as they sit next to you on public transportation, or in airports and other public places.

This *GT Advisory* was prepared by **Françoise Gilbert**, **Elizabeth C. Rogers**, **Luke Dixon**, **Wenjing Zhao**, **Stephanie A. Reiter**, and **Thaddeus C. Houston**. Questions about this information can be directed to:

- Françoise Gilbert | +1 650.804.1235| gilbertf@gtlaw.com
- Elizabeth C. Rogers | +1 512.320.7256| rogersel@gtlaw.com
- Luke Dixon| +44 (0) 203.349.8756| dixonl@gtlaw.com
- Wenjing Zhao | +86 (0) 21.6391.6633| zhaow@gtlaw.com
- Stephanie A. Reiter | +1 312.456.8415| reiters@gtlaw.com
- Thaddeus C. Houston| +1 415.655.1290| houstont@gtlaw.com
- Or your Greenberg Traurig attorney

Albany
+1 518.689.1400

Amsterdam
+ 31 20 301 7300

Atlanta
+1 678.553.2100

Austin
+1 512.320.7200

Berlin¬
+49 (0) 30 700 171 100

Berlin-GT Restructuring¯
+49 (0) 30 700 171 100

Boca Raton
+1 561.955.7600

Boston
+1 617.310.6000

Chicago
+1 312.456.8400

Dallas
+1 214.665.3600

Delaware
+1 302.661.7000

Denver
+1 303.572.6500

Fort Lauderdale
+1 954.765.0500

Houston
+1 713.374.3500

Las Vegas
+1 702.792.3773

London*
+44 (0)203 349 8700

Los Angeles
+1 310.586.7700

Mexico City+
+52 55 5029.0000

Miami
+1 305.579.0500

New Jersey
+1 973.360.7900

New York
+1 212.801.9200

Northern Virginia
+1 703.749.1300

Orange County
+1 949.732.6500

Orlando
+1 407.420.1000

Philadelphia
+1 215.988.7800

Phoenix
+1 602.445.8000

Sacramento
+1 916.442.1111

San Francisco
+1 415.655.1300

Seoul∞
+82 (0) 2.369.1000

Shanghai
+86 (0) 21.6391.6633

Silicon Valley
+1 650.328.8500

Tallahassee
+1 850.222.6891

Tampa
+1 813.318.5700

Tel Aviv^
+972 (0) 3.636.6000

Tokyo¤
+81 (0)3 4510 2200

Warsaw~
+48 22 690 6100

Washington, D.C.
+1 202.331.3100

Westchester County
+1 914.286.2900

West Palm Beach
+1 561.650.7900