Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

**December 23, 2015**

**ENFORCEMENT + LITIGATION**

**FTC Enters into Settlement with Oracle over Java SE**

The Federal Trade Commission (FTC) has announced that it has settled an investigation with Oracle over the software Java SE, which reportedly has been installed on over 850 million computers.

According to the FTC's press release: "Oracle has agreed to settle Federal Trade Commission charges that it deceived consumers about the security provided by updates to its Java Platform, Standard Edition software (Java SE), which is installed on more than 850 million personal computers. Under the terms of a proposed consent order, Oracle will be required to give consumers the ability to easily uninstall insecure, older versions of Java SE."

The consent order entered into between the FTC and Oracle states that Oracle must not "misrepresent: (1) the privacy or security of the Covered Software on a consumer's computer, including but not limited to the effect on privacy or security of any installation or update of the Covered Software; or (2) how to uninstall older Iterations of" Java SE.

Further, the consent order requires Oracle to provide clear and conspicuous instructions to consumers about how they can uninstall old versions of the software.

The FTC alleged in its complaint against Oracle that "since acquiring Java in 2010, Oracle was aware of significant security issues affecting older versions of Java SE. The security issues allowed hackers' to craft malware that could allow access to consumers' usernames and passwords for financial accounts, and allow hackers to acquire other sensitive personal information through phishing attacks."

The FTC alleged that the "failure to disclose the limitations of the updates in light of the statements made about the security benefits of the updates was deceptive and in violation of Section 5 of the FTC Act."

*— Linn Foster Freedman*

---

**LifeLock Settles with FTC for Record $100 Million**

In its largest settlement ever obtained through an enforcement action, the Federal Trade Commission (FTC) announced last week that it had settled with identity theft protection firm LifeLock for $100 million. The no-fault settlement relates to a 2010 FTC enforcement action against LifeLock in which the FTC alleged that LifeLock misrepresented the effectiveness of its products in advertisements and had not

properly secured its customers' information. The 2010 settlement required LifeLock to establish a comprehensive security program and pay a $12 million fine. Earlier this year, the FTC alleged that LifeLock violated the 2010 settlement in several ways, including falsely advertising that LifeLock used the same data protections as financial institutions and that customers would receive immediate notice as soon as LifeLock suspected a potential identity theft. Customers who were part of a class action against LifeLock related to its previous security measures and advertising statements will receive $68 million of the settlement.

*— Pamela Del Negro*

---

**Update on Excellus Data Breach Litigation**

Excellus Blue Cross Blue Shield (Excellus) was hit with another proposed class action suit late last week (view related posts here and here).

The case, filed by a New York woman, accuses Excellus BlueCross BlueShield of failing to prevent a massive data breach that exposed the personal information of 10 million customers. This is the latest suit—the sixth—to be filed against Excellus in federal court over the cyber-attack that started in December of 2013.

The intrusion compromised the names, birth dates, Social Security numbers, addresses, and financial information of 10 million members and occurred on the heels of other high-profile data breaches of insurers, including Anthem, CareFirst, and Premara.

*— Linn Foster Freedman*

---

**CYBERSECURITY**

**Omnibus Funding Bill Creates Healthcare Cybersecurity Task Force**

The $1.1 trillion spending and tax extender bill that is on President Obama's desk awaiting signature creates a healthcare industry cybersecurity task force, which must be established within 90 days of enactment.

This is important news since a recent report issued by the International Data Corporation forecasts that one in three consumers will have their health data compromised in the next year due to weak security measures. On top of that, the most recent Ponemon Institute report in May indicates that criminal attacks on healthcare providers are up a whopping 125 percent since 2010.

The proposed task force will study cyber threats and how other industries combat cyber intrusions, as well as the challenges facing healthcare organizations in securing health information. It also includes a provision to ensure that information on cyber threats is shared within the industry (similar to other industries) and can be accessed in real time and with no cost.

The bill requires the Department of Health and Human Services to work with the Department of Homeland Security and NIST to create voluntary guidelines and best practices for healthcare organizations. The goal is also to encourage healthcare organizations to share cyber threats and vulnerabilities so organizations can help each other and access information from the federal government and other industries.

This is good news for the healthcare industry. It needs all the help it can get in combatting cyber intrusions, because 2015 goes down in history as seeing the four largest healthcare data breaches in history.

*— Linn Foster Freedman*

---

**DATA SECURITY**

**RBAC – Is It Implemented in Your Organization?**

Traditionally, it was very common for organizations to adopt an optimistic security model. Give everyone access to everything unless specifically denied access to sensitive areas, like HR or Finance. While this approach is generally regarded as more convenient for end users, it is less secure and leaves organizations more vulnerable than pessimistic security models. Pessimistic security models generally deny access to everything for everyone unless specifically granted access. While more secure, the pessimistic model tends to hamper collaboration and can be tedious to maintain properly. Early security models were very static and assigned permissions to individual users for individual systems or tasks. In large organizations, such models become extremely difficult to administer.

Formalized in 1992 by David Ferraiolo and Rick Kuhn, Role Based Access Control (RBAC) has become one of the most widely used security models. RBAC grants access to systems or the ability to perform tasks based on roles. Roles are determined by job function, job responsibilities, job competency, authority within the organization, etc. There are essentially only three primary rules in an RBAC system:

1. Role Assignment: users can only perform function(s) if they have been assigned a role.
2. Role Authorization: user must be authorized for the role to which they are assigned.
3. Permission Authorization: the specific function or permission must be authorized to the role.

Implementing an RBAC security model allows for more dynamic provisioning of security permissions while maintaining a high level of accountability and auditability. Users receive the rights and access necessary based on their assigned role without having to configure each individual system. RBAC can even be used to automate many business processes, providing more efficiencies to your environment.

For more detailed and technical information on RBAC, visit the recommended sites listed below.

National Institute of Standards and Technology
Ferraiolo and Kuhn's 1992 White Paper

*— Sean C. Lawless*

---

**CHILDREN'S PRIVACY**

**Two Mobile App Developers Collect Persistent Identifiers and Pay Out $360,000 in Fines for COPPA Violations**

LAI Systems, LLC (LAI), and Retro Dreamer agreed to pay civil penalties of a combined $360,000 to settle charges issued by the Federal Trade Commission (FTC) that they violated the Children's Online Privacy Protection Act (COPPA) by allowing advertising companies to use persistent identifiers, collected through their mobile apps, to elicit specific advertisements to children. The director of the FTC's Bureau

of Consumer Protection, Jessica Rich, said, “It’s vital that companies understand the rules of the road when it comes to handling children’s personal information online[, and] these cases make it clear that we’re closely watching this space to ensure children’s privacy online is being protected.”

This is the first time that the FTC has brought an action against a mobile app developer for the collection and misuse of persistent identifiers. However, persistent identifiers were one of the data categories added to COPPA back in 2013.

LAI makes several children’s apps, including My Cake Shop, My Pizza Shop, Hair Salon Makeover, Friday Night Makeover, Marley the Talking Dog, and Animal Sounds. Retro Dreamer makes Ice Cream Jump, Happy Pudding Jump, Ice Cream Drop, Sneezie, Wash the Dishes, Cat Basket, and Tappy Pop. The FTC alleged that both developers allowed third-party advertising companies to collect children’s personal information through these apps and failed to inform the advertising companies that the apps were directed at children under 13. The developers also did not provide notice or obtain consent from parents before collecting the children’s information. LAI will pay $60,000 and Retro Dreamer will pay $300,000.

*— Kathryn M. Rattigan*

---

**DATA PRIVACY**

**Does Your Organization’s New Year’s Resolution Violate Employee Privacy?**

One of the most common New Year’s resolutions is a renewed commitment to health and fitness. Many employers also seek to update or introduce wellness programs at the beginning of the year with the goal of improving their employees’ health, which can lead to increased employee productivity and reduced group health care costs. Corporate wellness is a multibillion-dollar industry that incorporates the most advanced medical and data technology to assist employees in improving their personal health and fitness. Yet the industry’s advancements in technology may result in increased employer exposure to potential employee privacy and discrimination claims.

Often wellness programs are not regulated by statute nor is there a long history of case precedent to provide guidance to employers as to how best to implement a wellness program while reducing its exposure to employee litigation. In 2015, after pursuing several court cases in different jurisdictions, the EEOC released proposed rules aimed at protecting employees through the Americans with Disabilities Act. The proposed rules signify that the EEOC remains focused on the issue of wellness programs and employee privacy and will continue its litigation strategy against employers it believes are subjecting employees to programs that potentially violate statutory and privacy laws.

Many wellness vendors try to avoid legal exposure by using blanket employee authorization forms. Employees are increasingly voicing concerns about broad authorizations and submitting their personal health information to third-party vendors contracted by their employer without a clear sense of how the information is protected, what the information is being used for, and if it is accessible to an employer in an identifiable way. In addition, employees are concerned that third-party vendors do not have the appropriate measures in place to safeguard their personal health information from a potential data breach. These issues warrant careful employer consideration when implementing wellness programs in the workplace.

*— Rachel V. Kushel*

---

**Update on EU Data Protection Regulation**

On December 17, 2015, the European Parliament's Civil Liberties, Justice, and Home Affairs Committee approved the final text of the European Union General Data Protection Regulation, after lengthy negotiation.

The regulation, intended to replace the EU Data Protection Directive, which is over 20 years old, is supposed to help the 28 EU member states consistently address privacy compliance and enforcement against companies. Significantly, the regulation dramatically increases the fines and penalties that the privacy authorities can assess for a violation—up to 4 percent of a company's global income—a significant amount for global companies.

The regulation must be approved by the European Parliament, which is reportedly set to happen in the next few weeks. If approved, which is predicted to be likely, companies will have a two-year transition period to get into compliance. Many companies are already getting a head start on compliance now, and those that aren't should consider doing so.

*— Linn Foster Freedman*

---

**DRONES**

**Center for Democracy and Technology Proposes Drone Privacy Best Practices**

The Center for Democracy and Technology (CDT) issued a set of best practices for private drone users, both in the commercial and noncommercial arenas. The CDT hopes to help individuals use drones safely while also encouraging them to respect others' privacy. Some highlights from the CDT's best practices include:

- All commercial drone operators should have a privacy policy describing how the drone is used, the types of data the drone collects, and how the information is disclosed;
- Private drone operators should also make reasonable efforts to notify others if they are collecting information through their drone;
- Private drone operators should not enter private property without first obtaining consent;
- Private drone operators should not collect information for persistent monitoring of a specific individual, for employment purposes, or for credit or healthcare eligibility without individual consent;
- Data collected through drone use should be destroyed or de-identified if retention of the data is not necessary; and
- All commercial drone operators should implement commercially reasonable security standards to protect the data they collect.

All of the CDT's drone privacy practices stem from the White House's Consumer Privacy Bill of Rights and the Fair Information Practice Principles. Overall, the CDT seeks to encourage increased privacy, transparency, and accountability of drone operators. Click here to access the complete CDT's drone privacy best practices.

*— Kathryn M. Rattigan*

---

**Fact Sheet Issued by FAA on State and Local Drone Laws**

Last week, the Federal Aviation Administration (FAA) issued a new fact sheet outlining state and local regulations related to the operation of unmanned aircraft systems (better known as drones). The FAA said in its fact sheet, "Unmanned aircraft systems (UAS) are aircrafts subject to regulation by the FAA to ensure safety of flight, and safety of people and property on the ground. States and local jurisdictions are increasingly exploring regulation of UAS or proceeding to enact legislation relating to UAS operations." Because of this increase in drone regulation by state and local governments, the FAA's fact sheet provides "basic information about the federal regulatory framework for use by states and localities when considering laws affecting UAS" and cautions that "[s]tate and local restrictions affecting UAS operations should be consistent with the extensive federal statutory and regulatory framework pertaining to control of the airspace, flight management and efficiency, air traffic control, aviation safety, navigational facilities, and the regulation of aircraft noise at its source."

The fact sheet provides a list of examples of drone laws that are likely to fall under the state and local government authority umbrella: use of drones by police and the necessity of obtaining warrants prior to any police surveillance efforts, prohibition on the use of drones for voyeurism, exclusions on the use of drones for hunting or fishing, and prohibitions on attaching firearms or other types of weapons to a drone. We will likely see increased state and local regulation this coming year until the FAA sets clearer standards across the board.

*— Kathryn M. Rattigan*

---

**DATA PRIVACY TIP #15**

**Protecting Your Privacy During Holiday Travel**

The holiday season means traveling to see family and friends and is a wonderful time of year. That travel includes planes, trains, and automobiles. Although that movie was hilarious, travel can be hazardous to the protection of your privacy.

Here are some basic tips to keep in mind while traveling on planes, trains, and automobiles during the holiday season:

**1.** Don't leave your laptop, tablet, USB drive, other removable media, or mobile phone in your car trunk. I get a call once a month on stolen removable media from cars. They are stolen all the time, and the consequences can be dire for you, individually, and for your company.
**2.** Don't leave your laptop, tablet, or mobile phone, unattended on a plane or train. I take the train all the time and love it, but it is amazing to see how people go to the restroom or café car and leave their mobile devices unattended. Bad idea.
**3.** Use complex passwords on all devices so, if you forget them or they are stolen, your data is not immediately vulnerable and accessible. Sometimes if you leave your devices in the waiting area in the airport, or on the plane or train, a nice individual will return it; but still, you don't want your data automatically exposed.
**4.** Be careful not to store or leave your devices in the seat pockets of airplanes or trains. This also happens all the time!
**5.** Destroy your travel documents (including boarding passes) when you are finished with them by shredding them. There is a lot of personal information on those documents and savvy hackers can use the barcodes to get all sorts of information about you.
**6.** If your mobile technology is lost or stolen, call your company IT department immediately or remote wipe them yourself.
**7.** Lock your laptop and other mobile devices in your hotel safe.
**8.** Wipe your laptop before and after you travel to high-risk areas such as China, Russia, the Ukraine, Iran, or Iraq. If you are traveling with a company computer, get a loaner and work with your IT department to make sure there are no "presents" on your laptop when you return from these high-risk areas.

**9.** Use your VPN connection any time you are accessing your company information and not free wifi.
**10.** Frequently update your virus and firewall protections.

Happy holidays and safe travels!

*— Linn Foster Freedman*

---

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.

---

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

---