April 5, 2013

BakerHostetler

Social Media and the Law: Privacy Issues

Gerald J. Ferguson, Esq. gferguson@bakerlaw.com
Blog: www.dataprivacymonitor.com
Twitter: JerryFergusonNY

Overview

- Sources of Privacy Law
- Breach Notification
- Sharing Consumer Information
- Emerging Issues

Sources of Privacy Law

- Federal Privacy Laws
- State Privacy Laws
- Industry Self-Regulation
- Foreign Law
- Contractual Obligations

Federal Privacy Law

- FTC Privacy Rules: Unfair & Deceptive Practices
- Gramm-Leach-Bliley: Financial Institutions
- HIPAA: Healthcare Provider
- COPPA: Children
- SEC Guidelines: Public Companies
- Cyber Security Executive Order: Critical Infrastructure

State Privacy Laws

- Breach Notification Law
- Massachusetts Privacy Law
- Common Law Privacy Rights
  - Social media sites protected by Communication Decency Act
  - Users liable for common law violation

Industry Self-Regulation

- Payment Card Industry (DSS)
- Internet Advertising Bureau (IAB)
- Network Advertising Initiative

Foreign Law

- European Union Privacy Directives
  - Influential Worldwide
  - EU – US Safe Harbor
- Dozens of Countries Have Recently Enacted National Privacy Laws
- Compendium of International Laws at www.dataprivacymonitor.com

Contractual Obligations

- Posted Privacy Policies
- Google Guidelines and Best Practices

What is PII?

- Information that can be used to uniquely identify an individual
- May be used for Identity Theft
- Sensitive Information accorded greater protection
  - Religious Belief
  - Political Affiliation

What is **NOT** PII?

BakerHostetler

- Publicly Available Information

- Confidential Business Information and Trade Secrets

Data Breach Issues

- Breach Notification Obligations
- Costs of Compliance
- Class Action

Linkedin Breach

- June 2012: 6.5 million passwords posted on Russian hacker forum
- Passwords encrypted but encryption easily hacked
- PII?

LinkedIn Blog

Home > Full Story

Taking Steps To Protect Our Members

Vicente Silveira, June 7, 2012

It is of the utmost importance to us that we keep you, our members, informed regarding the news this week that some LinkedIn member passwords were compromised. We want to reiterate that we sincerely apologize for the inconvenience this has caused our members.

From the moment we became aware of this issue, we have been working non-stop to investigate it. While we continue to learn more as a result of our ongoing investigation, here is what we know now:

Yesterday we learned that approximately 6.5 million hashed LinkedIn passwords were posted on a hacker site. Most of the passwords on the list appear to remain hashed and hard to decode, but unfortunately a small subset of the hashed passwords was decoded and published.

To the best of our knowledge, no email logins associated with the passwords have been published, nor have we received any verified reports of unauthorized access to any member's account as a result of this event.

Since we became aware of this issue, we have been taking active steps to protect our members. Our first priority was to lock down and protect the accounts associated with the decoded passwords that we believed were at the greatest risk. We've invalidated those passwords and contacted those members with a message that lets them know how to reset their passwords.

Going forward, as a precautionary measure, we are disabling the passwords of any other members that we believe could potentially be affected. Those members are also being contacted by LinkedIn with instructions on how to reset their passwords.

We are also actively working with law enforcement, which is investigating this matter.

Finally, our current production database for account passwords is salted as well as hashed, which provides an additional layer of security.

We are working hard to protect you, but there are also steps that you can take to protect yourself, such as:

- Make sure you update your password on LinkedIn (and any site that you visit on the Web) at least once every few months.
- Do not use the same password for multiple sites or accounts.
- Create a strong password for your account, one that includes letters, numbers, and other characters.
- Watch out for phishing emails and spam emails requesting personal or sensitive information.

Our efforts to protect LinkedIn members impacted by this incident are ongoing and we will continue to keep you posted here.

Topics: Security

Trackback: http://blog.linkedin.com/2012/06/07/taking-steps-to-protect-our-members/trackback/

965 Share 687 Tweet 674 Like

Follow Us Links

USA | UK | Europe | India | Asia | Sign In | Subscribe

Must-Attend, 8-Part Webinar Series
FFIEC Authentication Guidance:
FDIC on Understanding and Conforming with the 2011 Update
NEW
Learn More

BANK INFO SECURITY

Authentication | Compliance | Fraud | Governance | Mobility | Payments | Risk Mgmt | Technology

News | Blogs | Interviews | Webinars | White Papers | Memberships | Resources | Events

Home > Blogs

The Public Eye with Eric Chabrow

Keeping tabs on federal government efforts to protect citizens' privacy

Get Daily Email Updates
Sign up!

LinkedIn Has Neither CIO nor CISO

Failing to Learn Lessons from the RSA, Sony Breaches

By Eric Chabrow, June 8, 2012. Tweet 64

LinkedIn, the social network that's investigating the pilfering of what could be more than 6.5 million of its members' hashed passwords, has neither a chief information officer nor chief information security officer (see *LinkedIn: Hashed Passwords Breached*).

"We don't currently have executives with those specific titles, but **Kevin Scott**, senior vice president, engineering, and **David Henke**, senior vice president, operations, oversee the functions," a LinkedIn spokesperson wrote in response to my inquiry.

> *Organizations can not function efficiently in today's society if they lack a key executive focused on IT security; otherwise, their stakeholders will be at risk.*

LinkedIn isn't the first technology company to experience a breach that has lacked a specific senior executive responsible for assuring the security of its data and systems. Two of the most prominent breaches of 2011 - to security provider RSA and consumer electronics giant Sony - occurred when neither of those companies had a CISO. Both, however, employed a CIO at the time.

Shortly after the RSA and Sony breaches, both companies hired highly regarded IT security experts as their CISOs (see *RSA Explains Duties of New CSO* and *Ex-DHS Official*

RELATED CONTENT

- Centralizing Web Application Security
- FBI: Insider Stole from Fed Reserve
- 6 Steps to Secure Big Data
- How Organized Crime Uses Banks
- The Real Source of Fraud

Solutions

INTERVIEW
Risk of Insider Fraud

WEBINAR
Using the NIST HIPAA Security Rule Toolkit for Risk Assessments

WHITEPAPER
Security Solutions Guide

More solutions...

Recent Content | Most Popular

1. FTC Highlights P-to-P Network Risks
2. LinkedIn Has Neither CIO nor CISO
3. eHarmony Reveals Breach
4. Mobile Users Want More Security Control
5. LinkedIn: Hashed Passwords Breached
6. LinkedIn Probes Possible Password Theft

State Breach Notification Laws

- 46 states, D.C., & U.S. territories
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent
  - What does “access” mean
  - What is a reasonable notice time

Notification

- Timing:
  - most expedient & without unreasonable delay
  - no later than 45 days
- Law enforcement may request delay
- Method: mail, e-mail*, or substitute notice (email, website, and media)

Costs of Response

- Forensics
- Notification
- Credit monitoring
- Call center
- Crisis response
- Legal fees
- Defense costs/settlement expenses
- PCI fines/assessments & regulatory fines

CATEGORY	DESCRIPTION	COSTS
1). Notification Costs	• Address list management • Printing, Inserting, Mailing • Post-Mailing Call Services • Returned Mail	$2,308,350
2). Credit Monitoring	• Flat Fee —$4 • Redemption — $15 @15% redemption rate	AVG: $5,512,500

Class Action: Theories of Harm

- Increased risk of identity theft;
- Time and effort to monitor/fix credit;
- Emotional distress;
- Personal information as property;
- Invasion of privacy
- Breach of contract
- Breach of fiduciary duty
- Negligence
- Unfair, deceptive and unlawful business practices
- Defamation, libel, and slander
- Unjust enrichment

Standing in Privacy Lawsuits

- Plaintiffs must generally show that there is something more than the mere exposure of personal information in order for there to be sufficient harm to establish standing.
- Plaintiffs must either allege facts demonstrating an actual injury or "a threatened injury must be ‘certainly impending.'"
- An indefinite risk of future harm is not sufficient.

LinkedIn Class Action

June 2012, hacker posted 6.5 million LinkedIn passwords on website.

November 2012 class action followed:

- Alleged LinkedIn failed to live up to security standards stated in its privacy policy
- Argued LinkedIn did not use industry standard protections storing passwords
- Standing claim– would not have purchased premium membership to LinkedIn had class action members known security was deficient

LinkedIn Class Action

March 2013

- Claim dismissed for lack of standing
- Complaint did not show putative class of premium LinkedIn members paid for additional security above what was given to free members
- Must allege more than insufficient performance of how product functions – such as theft of PII

Sharing Consumer Information

- FTC Regulation
- EU Regulation
- Class Actions

FTC Approach to Sharing Customer Information

BakerHostetler

- Section 5 of the FTC Act – prohibits unfair and deceptive trade practices

Recent Enforcement:

- Facebook
- Google
- Twitter
- Wyndham
- Compete
- Franklin's Budget Car Sales

FTC Regulatory Framework

1) **Privacy by Design**—building in privacy at every stage of product development;

2) **Simplified Choice**—simplifying consumers' and businesses' ability to make choices about their information, such as through a "Do Not Track" mechanism; and

3) **Greater Transparency**—improving transparency in and consumer access to data collection and use policies.

COPPA

- Children under the age of 13;
- “Verifiable parental consent";
- Parents’ review of collected personal information and prevent further use.

Google and the FTC

Google Buzz Settlement (2011)

Missteps:

- Used Gmail addresses to enroll users (whether they wanted it or not) in social network features
- Each individual user's contact list was visible to other users
- Contacts that users "followed" were made public. Who a user followed, however, was based on frequency of private contact.

Google and the FTC

Google Buzz Settlement (2011)

FTC Action:

- Thousands of complaints to FTC resulted in FTC suit that charged Google Violated User Privacy
- FTC's big problem—Google's Privacy Policy Stated:
  - "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then **we will ask for your consent** prior to such use."
- Yet, Google enrolled Gmail users in Buzz anyways
- Unfair or deceptive business practice

Google and the FTC

Google Buzz Settlement (2011)

FTC and Google came to settlement:

- No future privacy misrepresentations
- Comprehensive Privacy Program
- Independent Audits for 20 years

Just one year later…

Google and the FTC

Google Cookie Settlement (2012)

Missteps:

- Circumvented Safari browser privacy protections
- By default, Safari blocked cookies that tracked users
- Google evaded this and installed cookies that tracked users and delivered wide range of targeted advertising
- Did so in guise of “temporary cookies”- supposedly only designed to let Google know if user was logged in to Google services

Google and the FTC

Google Cookie Settlement (2012)

FTC settlement terms:

- FTC brings suit, alleging violation of 2011 settlement
- $22.5 million settlement (highest to date)
- Delete cookies it had placed on safari browsers

Facebook & Irish Data Protection

In 2011, Irish Data Protection Commissioner (DPC) audited Facebook

- Partly due to various complaints about privacy practices from public.
  - High profile complaint from Austrian law student to DPC accused Facebook of misusing users' personal information – creating "shadow profiles" (later determined false but spurred audit)
- Partly routine—Facebook Ireland responsible for all non-US, European data

Facebook & Irish Data Protection

DPC Major Recommendations:

- Mechanism for users to make informed choices about how their information is used and shared on the site, including in relation to third party apps
- Increased transparency and controls over how personal data is used for advertising purposes
- Transparency and control for users via the provision of all personal data held to them on request and as part of their everyday interaction with the site

Facebook & Irish Data Protection

DPC Major Recommendations:

- "Tag suggest" (feature that suggests friends' names based on facial recognition) too intrusive
- Increase ability for users to delete data
- Increase user ability to access data collected on them

Six Months to Implement

Facebook & Irish Data Protection

DPC Report on Facebook Implementation (September 2012):

- Majority of Recommendations Adopted
- “Tag suggest” switched off in Europe
- Better user control settings
- Increased user ability to view data and activity on Facebook (download activity tool)

Facebook: The Next Round

- Terms of Use Modification - Fall of 2012
- Allows Sharing with Affiliates
- Instagram
- An Ad Agency?

Information Class Action: Standing

- To determine standing in such cases, courts generally look to whether the statute can be "understood as granting persons in the plaintiff's position a right to judicial relief.“
- Standing question is independent of the merits of the case.
  - *In re Facebook Privacy Litigation*, 791 F.Supp.2d 705, 712-713 (N.D. Cal. 2011)
  - *In re Zynga Privacy Litigation*, No. 10-cv-04680-JW, 2011 WL 7479170 (N.D. Cal. June 15, 2011)

Information Class Action: Standing

- *Gaos v. Google Inc.*, Case No.: 5:10-CV-4809 EJD (March 29, 2012)
  - Named plaintiff alleged that Google "intentionally included the search terms in the URL of the search results page…As a result…, when a user of Defendant's search service clicks on a link from Defendant's search results page, the owner of the website that the user clicks on will receive the user's search terms…"
  - The user's identity could then be discerned through the process of "reidentification," whereby the terms of the searches can be linked with the user through the user's IP address, for example, which may be released with the clicked link.
  - Plaintiff alleged that she had "suffered actual harm in the form of Google's unauthorized and unlawful dissemination of Plaintiff's search queries, which contained sensitive personal information, to third parties."
  - Plaintiff alleged common law claims and violation of the Stored Communications Act (SCA)

Gaos v. Google Inc. (cont'd.)

- Court dismissed the named plaintiff's common law claims for failing to allege an Article III "injury in fact."
- But the Court allowed the named plaintiff's claims under the SCA to survive, holding that "a violation of the SCA itself is injury sufficient to allege an SCA claim."
  - "the SCA provides a right to judicial relief based only on a violation of the statute without additional injury."
  - Plaintiff had alleged a particularized injury under the SCA because she had alleged that her search information was transmitted by Google to third parties.

Del Vecchio v. Amazon.com, Inc.

- *Del Vecchio v. Amazon.com, Inc.*, No. C11-366RSL (W.D. Wash. June 1, 2012)
  - Plaintiffs alleged that Amazon circumvented browsers' security settings to force users to accept cookies, and used gathered information for its benefit and for the benefit of third parties in contravention of its Privacy Notice.
  - Plaintiffs further alleged that class members' property rights, and their rights to control dissemination of their own information, were violated in an amount "substantially in excess of 1/100 of one cent" for each class member.
  - Alleged a "loss" under various state laws and the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.
  - Alleged (1) that they had purchased anti-virus software that Amazon defeated, and (2) that their private information allegedly exploited by Amazon "had economic value far in excess of $5,000.

Del Vecchio v. Amazon.com, Inc. (cont'd.)

- Court "flatly reject[ed] Plaintiffs' position that '"[c]ost" does not exclude non-monetary detriments,'" because such detriments could not aggregate to $5,000.
- Further, even if the plaintiffs' alleged costs were "losses" under the CFAA, they "failed to allege facts from which it could plausibly be inferred that those costs total at least $5,000."
- In alleging that the private information allegedly exploited by Amazon had no monetary value to plaintiffs, but only to Amazon, the plaintiffs effectively conceded that they had not suffered a "loss" under the CFAA.

Looking Forward

- FTC Enforcement Priorities

- EU: Right to be Forgotten

FTC Future Areas of Focus

- Do Not Track
- Mobile
- Data Brokers
- Large Platform Providers
- Promoting Enforceable Self-Regulatory Codes

New EU Data Protection Directive

Draft law before European Parliament

- Introduced 2012
- Overhauls 1995 Data Protection Directive

Would create "right to be forgotten"

- Companies forced to delete any data held on a consumer upon request (with some limited exceptions)
- Designed to increase transparency regarding what data is collected and for what purpose

New EU Data Protection Directive

Social Network Objections to 'Right to be forgotten'

- Interfere with how social networks operate
- Result in *more tracking* of users to enable the sites to delete all information
- Interferes with freedom of expression on the internet
- Right of others to remember? (e.g. you posted on someone's wall, chatted, etc.)

Questions?

BakerHostetler

Gerald J. Ferguson, Esq. gferguson@bakerlaw.com

Blog: www.dataprivacymonitor.com

Twitter: JerryFergusonNY