SPRING 2015 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery and cybersecurity needs. With the growth of fitness trackers and the recent release of the Apple Watch, we chose to theme this E-Newsletter on the impact wearables has for digital evidence preservation and electronic discovery.

DIGITAL MOUNTAIN'S GUEST CONTRIBUTOR
ROBERT D. BROWNSTONE, FENWICK & WEST LLP

A "WEARABLES" CAROL - BEWARE THE THREE GHOSTS

There is no stopping the inexorable march of innovation in computer technology. Great ideas and consumer enthusiasm have launched the era of digital "wearables" -- smart glass products, watches, health and fitness trackers, wristbands and the like. The typical wearable comes equipped with a camera, a microphone and/or one or more sensors. In our new era of the "Internet of Things" ("IoT"), everyone from the FTC to the EU to the Chinese Army is concerned about the many potential ramifications. So, what's a corporation to do? Even a compliance regime that already covers Bring-Your-Own-Devices (BYOD) should be modernized so its policies and protocols encompass Wear-Your-Own-Devices (WYOD). Employees' use of wearables brings to life three Dickensian ghosts - from the past, present and future.

I. Information Security – The Ghost of Data Past

Each wearable allowed to connect to an employer's network increases the risk of unauthorized access to company systems and thus to all pre-existing sensitive data. Examples include: intellectual property; and personally identifiable information not only as to customers/users but also regarding employees. Via phishing, malware or the like, a bad actor can co-opt a wearable for illicit purposes. The small size and relative simplicity of a wearable renders it even more susceptible to hacking, loss or theft than a larger device. In addition, a visitor or a disgruntled or disloyal employee can more readily use a wearable to secretly copy data or photograph hardcopy documents.

II. Individuals' Privacy – The Ghost of Data Present

In addition to its ability to gather volumes of data about the wearer (locations, physical activities, physiological metrics, etc.), in real time a wearable can easily surreptitiously gather data on others. For example, a wearer could audio record a conversation without a co-worker's or customer's knowledge or legally required consent. *See, e.g.*, Cal. Penal Code § 632 et seq. Or he or she could engage in videotaping without the typical disclosure that an organization posts when premises are under video surveillance. Then, a victim could accuse the employer of being vicariously liable for the wearer's recording activities.

III. Electronic Discovery – The Ghost of Data Future

Aside from day-in-day-out issues, downstream – in electronic discovery (eDiscovery) – wearables' data could play a role. And if past is prologue, then, at least in some future circumstances, judges are likely to find company litigants in "possession, custody or control" of WYOD devices' data. *Compare* ***Small v. Univ. Med. Ctr. of S. Nev.***, 2014 WL 4079507 (D. Nev. Aug. 18, 2014) (finding corporate responsibility for preserving BYOD and corporate-owned-personally-enabled, a/k/a COPE, devices' data); ***Puerto Rico Telephone v. San Juan Cable***, 2013 WL 5533711 D. P.R. 10/7/13) (same as to three corporate officers' personal Gmail accounts where company presumably knew accounts were used to manage company business). In another vein, in employment investigations and litigations, an employer could become very aggressive in seeking WYOD data to combat an employee's allegations as to medical conditions, physical locations, stress levels and the like. Let the games begin!

Conclusion

It behooves every 21st Century organization to embark on a WYOD assessment journey that addresses all three ghosts, namely information-security, individuals' privacy and eDiscovery preparedness.

TO LEARN MORE:

- Eric Baculinao, ***Chinese Army Bans Smartwatches, Wearable Tech Over Security Fears***, NBC News (May 12, 2015)
- Michele C.S. Lange, ***Ediscovery and the Security Implications of the Internet of Things***, ASIS Int'l Security Mgmt. (Apr. 13, 2015)
- Federal Trade Commission (FTC), ***FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks***, News Release (Jan. 27, 2015) ("*Report Recognizes Rapid Growth of Connected Devices Offers Societal Benefits, But Also Risks That Could Undermine Consumer Confidence*")
- FTC, ***internet of things***, FTC Staff Report (Jan. 26, 2015) ("Privacy & Security in a Connected World")
- Christina Bonnington, ***DATA FROM OUR WEARABLES IS NOW COURTROOM FODDER***, Wired (Dec. 12, 2014)
- Parmy Olson, ***Fitbit Data Now Being Used In The Courtroom***, Forbes (Nov. 16, 2014)
- Tom Starner, ***Risks of Wearables***, Risks & Insurance (Oct. 15, 2014) ("Wearables bring with them a host of liability concerns")
- ARTICLE 29 DATA PROTECTION WORKING PARTY, ***Opinion 8/2014 on the on Recent Developments on the Internet of Things***, 14/EN WP 223 (Sep. 22, 2014) (authoring entity is composed of representatives of: European national data protection authorities; the European Data Protection Supervisor; and the European Commission).

*Robert D. Brownstone is the Technology & eDiscovery Counsel and Chair of the Electronic Information Management (EIM) Group at Silicon Valley headquartered Fenwick & West LLP, a 300+ attorney Silicon Valley-based law firm specializing in providing comprehensive services to prominent technology and life sciences clients. Robert advises clients on electronic discovery, retention/destruction policies, information security, data privacy, workplace EIM policies and social media rewards and risks. He is also in his second decade as a nationwide advisor, conference chair, speaker, writer and press resource on a variety of electronic information topics. Robert is a member of three state bars and on the National Employment Law Institute's Advisory Board. To learn more, please see Robert's full bio and extensive bibliography at his **Insights page**.*

If you would like to be considered as a future Guest Contributor to a Digital Mountain E-Newsletter, please provide a biography and a description of the proposed article to marketing@digitalmountain.com.

COME VISIT US AT LEGALTECH WEST COAST - BOOTH #411 ON JULY 13 AND JULY 14, 2015

UPCOMING INDUSTRY EVENTS

June 2015
ILTA's LegalSec Summit: June 8-9
Cybit Cyber Security and IT Security: June 11-12

July 2015
LegalTech West Coast: July 13-14

August-September 2015
HTCIA 2015: August 30 - September 2

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at some upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054

Contact us today!

866.DIG.DOCS

www.digitalmountain.com

FOLLOW US AT: