Daily Journal

Trial Skills Training For Your Practice
Building Trial Skills: Los Angeles | January 2-8, 2015 Sign Up Now

Classifieds/Jobs/Office Space : Experts/Services : MCLE : Search : Logout

FRIDAY MONDAY TUESDAY WEDNESDAY TODAY

Previous Next

Bookmark Reprints

This is the property of the Daily Journal Corporation and fully protected by copyright. It is made available only to Daily Journal subscribers for personal or collaborative purposes and may not be distributed, reproduced, modified, stored or transferred without written permission. Please click "Reprint" to order presentation-ready copies to distribute to clients or use in commercial marketing materials or for permission to post on a website.

With privacy policies, do what you say

Hsiao (Mark) C. Mao *is a partner and vice chair of the Financial Services Practice Group in the San Francisco office of Kaufman Dolowich & Voluck LLP. He may be reached at mmao@kdvlaw.com.*

Sheila Pham *is an attorney in the San Francisco office of Kaufman Dolowich & Voluck LLP. She may be reached at spham@kdvlaw.com.*

High profile data breaches are appearing in newspaper headlines at increasing rates. Although many businesses have focused their attention on preventing cyberattacks through stronger technical safeguards, the recent enforcement actions of the U.S. Federal Trade Commission teach us that tighter administrative controls should not be ignored.

Carefully drafted privacy statements and written response protocols are just as important because they have become one of the yardsticks by which the FTC measures "deceptive" online practices and the reasonableness of data security. The FTC may assess a company's privacy policies against actual practice, before a breach has even occurred. Once personally identifiable information has been compromised, the company's written policies will only be under closer scrutiny.

Encryption May Not Be Sufficient

Many selling encryption software tout their products as the panacea for data breaches. most states (including California) now exclude sufficiently encrypted data from the definition of "breach." Other states, like Kansas and South Carolina, may exclude a breach from notification laws where encryption prevents material harm.

However, encryption alone may not address privacy concerns. The needs of a company's technical architecture may demand that the company use less than what the FTC considers "industry-standard encryption." In the 2008 consent decree against Valueclick, the FTC alleged that Valueclick used "only an insecure form of alphabetic substitution that [was] not consistent with, and less protective than, industry-standard encryption." The FTC later stated in its 2013 consent decree against CBR Systems that companies using encryption should instead render personally identifiable information "unusuable, unreadable, and indecipherable."

The technological needs of businesses may not always permit them to encrypt data at every level. It is also possible for hackers to steal encryption keys, which was the fear of many during the recent panic on the "Heartbleed" bug.

Do What You Say

Businesses can often dismiss of the importance of privacy statements to their own detriment, although the FTC has given more than its fair share of hints at the importance of properly drafted privacy statements and updates. A number of security breaches of Twitter years ago led the FTC to assess Twitter's information systems and networks. In its consent decree in 2009, the FTC alleged that although Twitter claimed in its privacy statement that it employed "administrative, physical, and electronic measures designed to protect" nonpublic user information, from at least 2006 through 2009, Twitter failed to take reasonable and appropriate measures to prevent unauthorized hacker access to user accounts and passwords. Although the FTC focused on how Twitter could have taken some steps to better protect user passwords and information, the commission also repeatedly pointed to the inconsistency between what Twitter said it did to protect information, versus what it did in practice.

Questions and Comments

NEWS RULINGS VERDICTS

SPECIAL REPORT
Entertainment Law

Thursday, November 6, 2014

Discipline
Federal Circuit disciplines prominent Silicon Valley patent litigator
Edward R. Reines, a Weil, Gotshal & Manges LLP partner, was publicly reprimanded Wednesday by a federal appellate court for improperly distributing a laudatory email written by the circuit's former chief judge to clients.

Government
Misconduct signals need to retool US attorney's office
The U.S. attorney's office for the Central District of California was once firmly established among the top prosecutors' offices in the country, but the office's reputation has fallen in recent years. By **Edward J. Loya Jr.**

Mergers & Acquisitions
Dealmakers
A roundup of recent transactions and the lawyers involved.

Government
Private practitioners snag top prosecutor spots in Madera, Sutter counties
In runoff district attorney elections, David Linn ousted incumbent Michael Keitz in Madera County, while Amander Hopper defeated Butte County Deputy District Attorney Jennifer Dupre in Sutter County.

Judges and Judiciary
Solano County judge admonished for berating litigants
Solano County Superior Court Judge Daniel J. Healy was publicly admonished Wednesday for berating litigants who appeared before him in family law proceedings and, in one case, becoming embroiled in a matter.

Law Practice
Senator-Elect joins Glaser Weil Fink Howard Avchen & Shapiro LLP
Glaser Weil Fink Howard Avchen & Shapiro LLP on Wednesday announced that Senator-Elect Robert M. Hertzberg of the San Fernando Valley will be joining its government and regulatory law practice.

Zoning, Planning and Use
Malibu voters limit formula retail development, setting stage for legal battles
In an effort to preserve the coastal city's local character, voters in Malibu approved a controversial land use ordinance Tuesday that will

The FTC will hold businesses accountable to what they say in their privacy statements in more instances than just in the event of a data breach. In all four of its well-known cases requiring comprehensive privacy programs - MySpace, Facebook, Google and Snapchat - the FTC made clear that the company's privacy statements will also be used to measure product design and whether marketing efforts by a business are "deceptive." In its consent decree with Facebook in 2011, the FTC alleged that Facebook told its users they could keep their information on Facebook private, and then repeatedly allowed such information to be made public and shared.

In its consent decree with Snapchat in May 2014, the FTC alleged that while Snapchat made various promises about the private nature of their disappearing messages, Snapchat collected the geographic location of its users and did not protect user privacy to the extent promised. In addition, the FTC pointed out that Snapchat did not disclose in its privacy statement that its "Find Friends" feature collected names and phone numbers, while giving the appearance of privacy and confidentiality to its users. The FTC was persuaded that what Snapchat promised by way of how it marketed its product and disclosed in its privacy statement did not accord with how its product actually worked.

Businesses need to draft and maintain their privacy policies and terms and conditions both in anticipation of data breaches and a more generalized review by the FTC for consistency between product design and what is promised to the consumer. Employing expensive technologies alone will not prevent FTC audits or enforcement.

Expect an Increasingly Aggressive FTC

In the last few years, the FTC has been increasingly flexing its powers pursuant to Section 5 of the Federal Trade Commission Act. In addition to prosecuting companies for "unfair and deceptive acts and practices," the FTC has now cautioned corporate executives about their individual exposures for privacy violations.

On Sept. 30, a senior FTC attorney analogized misleading privacy practices with a deceptive sales practices action against Innovative Marketing and one of its executives. The FTC alleged that Innovative Marketing was running a "scareware" scheme that tricked consumers into thinking that their computers were infected with malicious malware in order to sell supposed fixes. See FTC v. Kristy Ross, 12-2340 (4th Cir. Feb. 25, 2014). The FTC argued that just as the Innovative Marketing executive can be held individually liable where the executive knew about the deceptive practices and could have controlled them, executives condoning privacy violations may be individually liable.

The FTC's comments follow similarly aggressive enforcements efforts, such as those in FTC v. Wyndham Worldwide Corp., 13-1887 (D.N.J. April 7, 2014), where the it continues to test the full breadth of the "unfair" prong of its Article 5 powers, which is generally considered to be more vague than its more often used power against "deceptive" practices.

The FTC's increasingly aggressive enforcement actions demonstrate that businesses should expect only closer scrutiny of their privacy practices, which will include their administrative controls in addition to their technological safeguards.

Looking Ahead

Online privacy law is rapidly changing, spearheaded by rapid changes in technology and the "online industry." Within just a decade, we have moved at a blurring speed from desktops to mobile phones and personal wearables. And as personally identifiable information becomes even more readily available, enforcement agencies such as the FTC will only become more aggressive in its efforts to protect such information.

The FTC cases from the last few years demonstrate that the FTC's measure of a company's "reasonable" safeguards to protect personally identifiable information will include its privacy statements and written response protocols. It will also be more difficult for executives and decision makers to merely delegate the responsibilities to those below them without some fitting direction and supervision.

Lawyers should advise that their clients regularly sit down with their technical teams, and discuss how user information is collected, stored, edited and disseminated. As an online company grows and its products evolve, there is often an increasing "disconnect" between the business and technical teams. The lessons from the FTC teach us that all those involved in decision-making should look at their privacy statements and written security protocols with great interest.

Hsiao (Mark) C. Mao *is a partner and vice chair of the Financial Services Practice Group in the San Francisco office of Kaufman Dolowich & Voluck LLP. He may be reached at* mmao@kdvlaw.com.

require formula retail development proposals to seek approval from residents.

Law Practice
Star prosecutor joins WilmerHale in LA
Former San Diego federal prosecutor Timothy C. Perry joined the firm's Los Angeles office as counsel in the securities and litigation departments.

Public Interest
Electronic Frontier Foundation leader to step aside
The executive director of the San Francisco-based Electronic Frontier Foundation, Shari Steele, is leaving the nonprofit after more than 20 years on staff, setting in motion a series of leadership changes at the organization.

Corporate
Third quarter venture funding reports show optimism
Recent reports by Wilson Sonsini and Cooley covering the venture financing market during the third quarter showed exuberance as up financing rounds shot to all time levels. Deal terms shifted in the issuers favor.

Corporate Counsel
Andrew Thau
Chief operating officer and general counsel of United Talent Agency Beverly Hills

Government
Prosecutor fights suspension, saying he was singled out for punishment
A Santa Clara County prosecutor suspended for withholding potentially exculpatory evidence in an eight-defendant murder case struck back at his bosses on Wednesday, claiming his conduct was normal within the district attorney's office.

Civil Rights
The seeds of the Civil Rights Act of 1964
As we celebrate this year the landmark 50th anniversary of the Civil Rights Act of 1964, few realize that the seeds of that historic law were planted right here in California. By **Elaine Elinson**

Law Practice
When the state tells professionals what they can say
The state can regulate professions in many ways, but when state regulation and professional insights clash, we see the tension between regulation of the professions and professionals' free speech interests. By **Claudia E. Haupt**

Perspective
With privacy policies, do what you say
Privacy statements and written response protocols have become one of the yardsticks by which the FTC measures "deceptive" online practices and the reasonableness of data security. By **Hsiao C. (Mark) Mao and Sheila Pham**

Judicial Profile
Adrienne M. Grover
Justice 6th District Court of Appeal (San Jose)

Judges and Judiciary
Two judges lose elections, while prosecutor beats professor in $1 million race
Voters threw two sitting Superior Court judges off the bench, and they chose a senior prosecutor over a law professor in what may be the state's most expensive judicial election campaign.

Sheila Pham *is an attorney in the San Francisco office of Kaufman Dolowich & Voluck LLP. She may be reached at spham@kdvlaw.com.*

Previous **Next**

HOME : MOBILE SITE : CLASSIFIEDS : EXPERTS/SERVICES : MCLE : DIRECTORIES : SEARCH : PRIVACY : LOGOUT