

# INFORMATION SECURITY & PRIVACY NEWS

A Publication of the Information Security Committee  
ABA Section of Science & Technology Law

SUMMER 2011 VOLUME 2 ISSUE 3

## Editor

[Thomas J Shaw, Esq.](#)  
Tokyo, Japan

## Committee Leadership

### Co-Chairs' Message

Co-Chairs:

[David J. Navetta](#)  
Denver, CO

[Kathryn R. Coburn](#)  
Pacific Palisades, CA

Vice-Chairs:

[Benjamin Tomhave](#)  
Fairfax, VA

[Peter McLaughlin](#)  
Boston, MA

[SciTech Homepage](#)

[InfoSec Homepage](#)

[Join the InfoSec  
Committee](#)

© 2011 American Bar Association. All rights reserved.  
Editorial policy: *Information Security & Privacy News* endeavors to provide information about current developments in law, information security, privacy and technology that is of professional interest to the members of the Information Security Committee of the ABA Section of Science & Technology Law. Material published in *Information Security & Privacy News* reflect the views of the authors and does not necessarily reflect the position of the ABA, the Section of Science & Technology Law, or the Editor(s).



ABA SECTION OF  
SCIENCE & TECHNOLOGY LAW

## New Book: *Cloud Computing for Lawyers and Executives – A Global Approach*

By [Thomas Shaw](#)

This month, a new book on cloud computing, *Cloud Computing for Lawyers and Executives – A Global Approach*, was published ([here](#)). This book covers the global statutes affecting cloud computing, the information security and privacy risks of cloud computing, and an approach to analyzing the contractual provisions necessary to negotiate an agreement with a cloud services provider. Written in only a few months, it is up to date through May 2011 and covers cloud standards, cloud security controls, cloud specific statutes and cases, and those global statutes of concern to cloud users. It also covers the e-discovery and forensics in the cloud and data breach in the cloud plus the legal ethical issues for lawyers in use of the cloud. [Read more](#)

## Lurching Towards a Federal Privacy Regime: Will There Ever Be a First Coming?

By [Denis T. Rice](#)

Midway through 2011, the United States still has no overall federal privacy law. Instead, we have a complex patchwork of federal and state statutes directed to specific areas of commerce or society. Spring, 2011, saw introduction of two ambitious bills in the U.S. Senate, one aimed at creating the first federal privacy and data security law of general application, the other directed at federal right of consumers to avoid tracking online. Whether either of these will become law is hard to predict. The first, entitled the Commercial Privacy Bill of Rights Act of 2011 ("CPBRA"), is co-sponsored by Senators John Kerry (D-Mass.) and John McCain (R-Ariz.). [Read more](#)

## Managing Security Risks in Business Associate Agreements

By [Michael R. Overly](#), [Chanley T. Howell](#), [R. Michael Scarano](#)

Newspapers and trade journals feature a growing number of stories detailing instances in which organizations have entrusted their most sensitive information and data to a vendor or other business partner only to see that information compromised because the vendor failed to implement appropriate information security safeguards. Worse yet, those same organizations are frequently found to have performed little or no due diligence regarding their vendors and have failed to adequately address information security in their vendor contracts, in many instances leaving the organizations without a meaningful remedy for the substantial harm they have suffered as a result of a compromise. That harm may take a variety of forms: [Read more](#)

## Elephant in the Room – The Potential for Data Breach Statutory Damages

By [Paul Paray](#)

While some data breach victims will eventually sustain an ID theft, it is generally acknowledged that the vast majority will not. Accordingly, the direct damages sustained by ID theft victims are not very helpful in a class action – there are just not enough plaintiffs to excite class action attorneys. Over the years, plaintiffs' class action counsel have spent many hours trying to create a damages theory that would actually be common to all victims of a data breach event. The two theories that have gotten the most class action traction are based on "fear of ID theft" or "lost time and effort" allegations. Unfortunately – for plaintiffs' counsel, that is – neither theory [Read more](#)

## New Book: *Cloud Computing for Lawyers and Executives – A Global Approach*

By *Thomas Shaw*



This month, a new book on cloud computing, *Cloud Computing for Lawyers and Executives – A Global Approach*, was published ([here](#)). This book covers the global statutes affecting cloud computing, the information security and privacy risks of cloud computing, and an approach to analyzing the contractual provisions necessary to negotiate an agreement with a cloud services provider. Written in only a few months, it is up to date through May 2011 and covers cloud standards, cloud security controls, cloud specific statutes and cases, and those global statutes of concern to cloud users. It also covers e-discovery and forensics in the cloud and data breach in the cloud plus the legal ethical issues for lawyers in use of the cloud.

Written for both lawyers and executives, it provides the details that lawyers need to know to assess the risks involved with cloud computing, while at the same time providing introductions and summaries so executives know what questions to ask. It looks at both private sector organizations and governmental agencies and walks through negotiating agreements for both multinational organizations and small and medium-sized domestic organizations. It starts out by asking not only why to use the cloud, but when to use the cloud, including a financial analysis framework. Importantly it keeps a constant focus on what is different in the use of cloud. While highlighting the risks and issues both local and global, readers are shown that what may seem local is often global in the cloud. In addition to international and domestic organization, it also looks at individual consumers who use the cloud.

With the use of rapid publication and distribution technologies, it is the intent of the author to make regular updates to the book (it is available in printed and (soon) ebook formats). A second edition is planned before the end of the year. In this next edition, the author invites submissions on cloud-related topics that are new or significantly expand on the explanations already presented. Several members have already expressed their interest in doing so. Please contact the author as follows.

*Thomas J. Shaw, Esq. is an attorney at law, CPA, CIPP, CRISC, CISM, ERM<sup>P</sup>, CISA, CGEIT and CCSK based in Asia who works with organizations globally, on information law (data privacy, information security, e-discovery/litigation readiness), Internet law (cloud computing, social networking, e-commerce, intellectual property), international transactional law, compliance, information governance and technology risk assessment and management. He is the editor of the committee's recent book, Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists and editor of the E-Discovery and Digital Evidence committee's EDDE Journal. His recent publications have also appeared in the International Law News, SciTech Lawyer, IAPP Privacy Advisor, the Asia Law News and the Law Technology News. He runs CloudRisk Asia, which risk assesses organizations and cloud service providers ([www.cloudriskasia.com](http://www.cloudriskasia.com)) and a technology law practice ([www.tshawlaw.com](http://www.tshawlaw.com)). He can be reached at [thomas.shaw@cloudriskasia.com](mailto:thomas.shaw@cloudriskasia.com) and [thomas@tshawlaw.com](mailto:thomas@tshawlaw.com).*

## Lurching Toward a Federal Privacy Regime: Will There Ever Be a First Coming?

By Denis T. Rice



*Midway through 2011, the United States still has no overall federal privacy law. Instead, we have a complex patchwork of federal and state statutes directed to specific areas of commerce or society.<sup>1</sup> Spring, 2011, saw introduction of two ambitious bills in the U.S. Senate, one aimed at creating the first federal privacy and data security law of general application, the other directed at federal right of consumers to avoid tracking online. Whether either of these will become law is hard to predict.*

*The first, entitled the Commercial Privacy Bill of Rights Act of 2011 (“CPBRA”), is co-sponsored by Senators John Kerry (D-Mass.) and John McCain (R-Ariz.).<sup>2</sup> The second, introduced by Senator Jay Rockefeller (D-W. Va.), is the Do-Not-Track Online Act (“Do-Not-Track”).<sup>3</sup> The CPBRA observes that “with the exception of Federal Trade Commission enforcement of laws against unfair and deceptive practices, the Federal Government has eschewed general commercial privacy laws in favor of industry self-regulation, which led to several self-policing schemes, . . . some of which provide insufficient privacy protection to individuals.”<sup>4</sup> To cure this perceived gap, the CPBRA focuses on the way personal data is collected, used and shared in the online arena.*

### CPBRA

Key definitions under the CPBRA include “Covered Entity” and “Covered Information.”<sup>5</sup> A “Covered Entity” is any person who collects, uses, transfers or stores so-called “covered information” about more than 5,000 individuals during any consecutive 12-month period, and is either (a) subject to the FTC’s authority under Section 5 of the FTC Act, (b) a common carrier subject to the federal Communications Act of 1934 or (c) a non-profit.<sup>6</sup>

“Covered Information” means “personally identifiable information” (“PII”), “unique identifier information,” or any other information that may reasonably be used by a person collecting the

<sup>1</sup>Examples of federal statutes are the Fair Credit Reporting Act (15 U.S.C. §§1681-1681x) as amended by the Fair and Accurate Credit Transactions Act of 2003 (Pub. L. 108-159, 117 Stat. 1952); the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191, 110 Stat. 1936) modified by the Health Information Technology for Economic and Clinical Health Act (part of the Gramm-Leach-Bliley Act (Pub. L. 106-102, 113 Stat. 1338).

<sup>2</sup>Commercial Privacy Bill of Rights Act of 2011, S. 799 (2011) [hereinafter “CPBRA” or the “Act”].

<sup>3</sup>Do-Not-Track Online Act, S. 913 (May 9, 2011) (hereinafter “Do-Not-Track”). Rockefeller’s bill echoes one Congresswoman Jackie Speier (D-Cal.) introduced earlier in 2011, called the “Do Not Track Me Online Act of 2011.”

<sup>4</sup>CPBRA, §2, Finding No. (7). Under the Federal Trade Commission Act (“FTC Act”), the FTC can act to prevent or punish acts affecting commerce that constitute unfair methods of competition or are unfair or deceptive. The FTC’s focus has been on those who fail to follow their own announced privacy policies or otherwise misrepresent those policies.

<sup>5</sup>*Id.*, §§3 and 401.

<sup>6</sup>*Id.*, §401.

information when used with the foregoing types of information to identify a specific individual.<sup>7</sup> In turn, “PII” means any of the following:

- The individual’s first name (or initial) and last name, whether given at birth or time of adoption, or resulting from a lawful change of name
- The postal address of a physical place of residence of the individual
- An email address
- A telephone or mobile device number
- A Social Security number or other government issued identification number issued to the individual
- The account number of a credit card issued to the individual
- “Unique identifier information that alone can be used to identify a specific individual”
- Biometric data about the individual, including fingerprints and retina scans.<sup>8</sup>

“Covered information” excludes certain types of PII, such as:

- information obtained from public records and not merged with covered information gathered elsewhere;
- information obtained from a forum where it was voluntarily shared or authorized to be shared by the individual, is widely and publicly available and contains no restrictions on who can access and view such information;
- information reported in public media; and
- information dedicated to contacting an individual at the individual’s place of work.<sup>9</sup>

---

<sup>7</sup>*Id.*, §3(3).

<sup>8</sup>*Id.*, §3(5). PII also includes any of the following information if it is used, transferred or stored in connection with one or more of the items of information described above: (i) a date of birth; (ii) the number of a certificate of birth or adoption; (iii) a place of birth; (iv) “unique identifier information that alone cannot be used to identify a specific individual”; (v) precise geographic location, at the same degree of specificity as a global positioning system or equivalent system, and not including any general geographic information that may be derived from an Internet Protocol address; (vi) information about the individual’s quantity, technical configuration, type, destination, location and amount of uses of voice services, regardless of technology used; or (vii) any other information concerning an individual “that may reasonably be used by the party using, collecting or storing that information to identify that individual.” *Id.*

The Act defines “sensitive personally identifiable information” (“sensitive PII”) as:

- Personally identifiable information which, if lost, compromised or disclosed without authorization either alone or with other information, carries a significant risk of economic or physical harm; or
- Information related to a particular medical condition or a health record; or the religious affiliation of an individual.<sup>10</sup>

Finally, “unique identifier information” means a “unique persistent identifier,” like a customer number held in a cookie, user ID, or device serial number.<sup>11</sup>

#### Unauthorized Use of PII

The CPBRA forbids “unauthorized use” of covered information, defined as the use of covered information by a covered entity or its service provider for any purpose not authorized by the individual to whom such information relates.<sup>12</sup> “Unauthorized use” does not include the following uses if the use is reasonable and consistent with the practices and purposes described in the covered entity’s privacy notice given the individual:

- To process and enforce a transaction or deliver a service requested by the individual;
- To operate the covered entity that is providing a transaction or delivering a service requested by that individual (such as inventory management, financial reporting and accounting, planning and product or service improvement or forecasting);
- To prevent or detect fraud or provide for a physically or virtually secure environment;
- To investigate a possible crime;
- A use required by a provision of law or legal process;
- To market or advertise to an individual from a covered entity within the context of a covered entity’s own Internet website, services or products if the covered information used for such marketing or advertising was collected directly by the covered entity; or shared with the covered entity at the affirmative request of the individual; or by an entity with which the individual has an established business relationship;

---

<sup>9</sup>*Id.*, §3(3)(B).

<sup>10</sup>*Id.*, §3(6).

<sup>11</sup>*Id.*, §3(a).

<sup>12</sup>*Id.*, §3(8)(A).

- A use necessary for the improvement of transaction or service delivery through research, testing, analysis and development;
- A use necessary for internal operations, including (1) collecting customer satisfaction surveys and conducting customer research to improve customer service information and (2) information collected by an Internet website about the visits to such website and the click-through rates at such website to improve website navigation and performance; or to understand and improve the interaction of an individual with the advertising of a covered entity; or
- A use by a covered entity (1) with which an individual has an established business relationship; (2) which the individual could have reasonably expected, at the time such relationship was established, was related to a service provided pursuant to such relationship; and (3) which does not constitute a material change in use or practice from what could have reasonably been expected.<sup>13</sup>

Privacy practitioners are aware of different interpretations of “unauthorized use” under the Computer Fraud and Abuse Act (CFAA). There different federal courts have split on whether an employee’s originally authorized use of a computer becomes unauthorized when the employee uses the computer in a manner inimicable to the employer’s interests presents a potential issue under the CFAA.<sup>14</sup>

#### Requiring Privacy Programs and Practices

The CPBRA requires each covered entity, “in a manner proportional to the size, type and nature of the covered information that it collects,” to implement a “comprehensive information privacy program.”<sup>15</sup> This is accomplished by “incorporating necessary processes and practices through the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individual based on . . . the reasonable expectations of such individuals regarding privacy,” the “relevant threats that need to be guarded against in meeting those expectations” and maintaining “appropriate management processes and practices throughout the data life cycle.”<sup>16</sup>

The Act directs the FTC to initiate rulemaking requiring each covered entity to provide clear, concise, and timely notices of its privacy practices.<sup>17</sup> It further requires the FTC to generate rules requiring each covered entity to offer individuals “a clear and conspicuous mechanism for opt-out consent, for any

---

<sup>13</sup>*Id.*, §3(8)(B).

<sup>14</sup>*See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). *Compare International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). The CPBRA contains a “savings” clause that partly addresses this problem, stating that a use by a covered entity or its service provider may only be excluded from the definition of “unauthorized use” if the use is reasonable and consistent with the practices and purposes given under Section 201(a).

<sup>15</sup>CPBRA, §103.

<sup>16</sup>*Id.* Note that there is no definition of what is meant by “product” or “product life cycle,” and that a few clauses later the phrase is changed to “data life cycle,” which is also undefined.

<sup>17</sup>*Id.*, §201.

use of their covered information that would otherwise be unauthorized use, except that an individual's *opt-in* consent is required if sensitive PII is involved.<sup>18</sup> However, *opt-in* is not required for sensitive PII "to process or enforce a transaction or deliver a service requested by the individual, to prevent or detect fraud, or provide for a "secure physical or virtual environment."<sup>19</sup>

*Opt-in* is also required for use or transfer of previously collected covered information if there is any "material change in privacy practices" or a risk of economic or physical harm to an individual.<sup>20</sup> The individual must also have access to personally identifiable information and mechanisms to correct the information, as well as the option to request that the individual's PII be rendered not personally identifiable, if possible, when the entity enters bankruptcy or the individual terminates its relationship with the entity, except where the individual has shared the information with the covered entity in a "widely and publicly available forum."<sup>21</sup>

While the mechanisms for offering *opt-outs* must generally be "clear and conspicuous,"<sup>22</sup> if it relates to use by third parties for the purpose of behavioral advertising or marketing the mechanism must be "robust, clear, and conspicuous."<sup>23</sup> What "robust" adds to "clear and conspicuous" in this context is unclear.<sup>24</sup>

---

<sup>18</sup>*Id.*, §202(a)(1) and (3).

<sup>19</sup>*Id.*, §202(a)(3)(A).

<sup>20</sup>*Id.*, §202(a)(3)(B).

<sup>21</sup>*Id.*, §202(a)(4) and (5).

<sup>22</sup>*Id.*, §§202(a)(1) and (3).

<sup>23</sup>*Id.*, §202(a)(2) (emphasis added).

<sup>24</sup>One court, interpreting the adequacy of published notice to potential class action members required under the Private Securities Litigation Reform Act (PSLRA), stated that "[r]obust notice is clearly the best notice," concluding that the PSLRA did not require such best notice. *Burke v. Ruttenberg*, 102 F. Supp. 2d 1280 (N.D. Ala. 2006); applying PSLRA, subsection 21D(a)(3)(A)(i), (Plaintiff seeking lead plaintiff role in class action must publish a notice advising members of purported class of pendency of the action, claims asserted, purported class period and ability of others to seek lead plaintiff role). *Cf. Gillis v. SPX Corp. Individual Account Retirement Plan*, 511 F.3d 58, 63 (1st Cir. 2007) note 4 (notice satisfied ERISA where later amendment requiring "a more robust form of notice" was not in effect at the time).

### Minimizing Data Collection and Transfer

“Data minimization” is an important part of the CPBRA.<sup>25</sup> The Act therefore limits collection of information to only as much as “reasonably necessary” to process a transaction or request, prevent or detect fraud, investigate a possible crime, comply with a provision of law, market or advertise to an individual (if the covered information used was collected directly by the entity), conduct research and development to improve service, or for such informal operations as customer satisfaction surveys and website analytics.<sup>26</sup> A covered entity can retain covered information only as long as needed to process a transaction or deliver a service, conduct research and development, or comply with the law.<sup>27</sup> And the entity can transfer covered information to a third party only if it first performs due diligence indicating that the third party is reliable and requires by contract that the third party will use the information consistent with the Act and not combine it with other information in order to identify an individual, unless that individual gives the third party opt-in consent to such combination and identification.<sup>28</sup>

### Accountability

The Act requires each covered entity to have “managerial accountability,” proportional to its size and structure, for adopting and implementing policies consistent with the Act and have a process to respond to “non-frivolous inquiries from individuals regarding the collection, use, transfer, or storage of covered information relating to such individuals.”<sup>29</sup>

### Safe Harbor

The CPBRA calls for the FTC to approve non-governmental organizations to run voluntary safe harbor programs that would exempt participating entities from certain requirements of the Act, and specifically the sections dealing with obligations of notice, data minimization and data accuracy, if the FTC finds the safe harbor program is no less protective of individual privacy than such sections.<sup>30</sup>

The CPBRA’s section on enforcement is probably its most controversial aspect, particularly from the perspective of the consumer advocate bar. At present, certain states allow private actions for damages; a significant example is California, whose Online Privacy Protection Act of 2003 is enforceable through the state’s Unfair Competition Law (“UCL”).<sup>31</sup> Only the FTC and state attorneys general can enforce the CPBRA; moreover, all state laws relating to collection, use and disclosure of covered information or PII are preempted.<sup>32</sup> The FTC or state attorneys general can obtain injunctive

---

<sup>25</sup>*Id.*, §301.

<sup>26</sup>CPBRA, §301(1).

<sup>27</sup>*Id.*, §301(2).

<sup>28</sup>*Id.*, §302.

<sup>29</sup>*Id.*, §102.

<sup>30</sup>*Id.*, §§501-502.

<sup>31</sup>Cal. Bus. & Prof. Code, §§22575-22579; UCL is same code at §17200-17209.

<sup>32</sup>*Id.* at §§402(FTC), 403 (state attorneys general) and 405 (state laws relation to collection, use or disclosure of covered information as defined in the Bill of Rights Act are preempted); *but see id.* §405(b)(2) (the Act does not preempt state laws addressing collection, use or disclosure of health or financial information, data breach notification, or fraud).

relief or civil penalties of up to \$16,500 multiplied by either (a) each day the entity is not in compliance with the parts of the Act dealing with consent, notice, and safeguards, or, (b) in violations of the consent requirements, the number of individuals for whom the entity failed to consent as required under such title, whichever is greater.<sup>33</sup> The maximum total liability for any related series of such violations is \$3 million. Penalties for “knowing or repetitive” violations shall be enforceable by the FTC as unfair or deceptive acts or practices, and state attorneys general also may bring civil actions.

### **DO-NOT-TRACK**

While Do-Not-Track has a more limited scope than the CPBRA, it would bring to the business of collecting personal information by online service providers under federal regulation. The CPBRA calls for rules requiring users’ consent to online tracking, but does not specifically authorize a universal opt-out. Do-Not-Track directs the FTC to establish standards for implementing a mechanism by which an individual can “simply and easily” indicate whether the individual prefers to have personal information collected by providers of online services, (including providers of mobile applications and services)” and rules to prohibit, with certain exceptions, collecting personal information on individuals who express via such a mechanism a preference not to have such information collected.<sup>34</sup> Regardless of the individual’s preference, the FTC rules must allow for collection and use of personal information to the extent (1) necessary to provide a service requested by the individual, so long as the information is “anonymized or deleted upon the provision of such service,” or (2) the individual receives “clear, conspicuous and accurate notice” and “affirmatively consents to such collection and use.”<sup>35</sup> Violation of such rules shall be deemed an unfair and deceptive act or practice in violation of the FTC Act.<sup>36</sup>

Like the CPBRA, enforcement of Do-Not-Track lies exclusively with the FTC and the state attorneys general. The latter are empowered to bring civil actions in federal district court to enjoin violations of the FTC rules, compel compliance with such rules, obtain damages, restitution or other compensation on behalf of residents adversely affected by a violation, or obtain civil penalties.<sup>37</sup> The civil penalties are calculated at up to \$16,000 times the number of days the person is not in compliance with the rule, with the total amount of penalties against such person not to exceed \$15 million for all such civil actions.

Unlike the do-not-call law, which allows people to avoid telemarketing calls, Do-Not-Track does not empower people to stop receiving online ads. Instead, the bill allows users to avoid receiving certain targeted ads, but those ads presumably will be replaced with untargeted ones.

The bill appears to be aimed at ensuring that ad networks respect the new browser-based do-not-track headers that have appeared since December 2010, when the FTC called for online companies to create

---

<sup>33</sup>*Id.* at §404(a).

<sup>34</sup>Do-Not-Track, §2(a).

<sup>35</sup>*Id.*, §2(b).

<sup>36</sup>*Id.*, §3(a).

<sup>37</sup>*Id.*, §3(b)(1).

a universal mechanism for consumers to opt out of all online tracking. Since then various companies such as Microsoft and Apple have announced new do-not-track headers which users can activate to communicate that they do not want to be tracked, (only a few ad networks thus far have promised to honor them). While law currently appears not to require companies to respect browser-based headers, some have suggested that refusing to do so might be considered an unfair practice under the FTC Act.

Industry standards currently call for ad networks to notify consumers about behavioral targeting and allow them to opt out of receiving targeted ads, but they do not require that companies follow do-not-track headers. The Direct Marketing Association claims the present industry-run program of hosting host opt-out pages where users can express a preference to avoid targeted ads can effectively inform consumers about online ad practices and allow them to choose whether they want targeted ads. It argues that a new law regulating behavioral targeting or the directing of ads to users based on the sites they have visited could “send the wrong signal to the public—which is that there’s something inherently wrong with these practices.”<sup>38</sup>

Consumer groups, on the other hand, such as the Center for Digital Democracy, Consumers Union and Electronic Frontier Foundation, are behind Rockefeller’s bill.<sup>39</sup> Lee Tien, senior staff attorney at the EFF, says the group believes the measure can help preserve civil liberties online. Tien says that most online activity is covered by the First Amendment and should not be subject to surveillance by either the government or private companies. “It is speech, it is reading, it is associating with others,” Tien says. “All of that needs to be protected.”

## Conclusion

With many other issues, especially fiscal and health-oriented, occupying the main focus of Congress and the White House in 2011, there is no assurance that either the CPBRA or Do-Not-Track will reach a final vote this year. In the view of the author, the two bills will eventually be combined and Do-Not-Track will be somewhat softened. While India is suddenly emerging as a leader in national privacy regulation, we await the First Coming of a comprehensive U.S. regime.

*Denis Rice is a co-author of PRIVACY AND SECURITY COMPLIANCE AND LITIGATION IN CALIFORNIA (CEB 2010) and has written and spoken extensively on privacy and data security, including in Bangalore, Berlin, London, Monterey, and for the Practising Law Institute. He is founding chair of the California State Bar Cyberspace Law Committee. A member of the ABA's Science and Technology Section and Committee on Cyberspace Law, he is listed in Best Lawyers in America in five categories, including Information Technology. In 2009 the State Bar Business Law Section gave Mr. Rice its Lifetime Achievement Award.*

---

<sup>38</sup>Wendy Davis, *Do-Not-Track Bill Introduced in Senate*, Online Media Daily (May 9, 2011) at [http://www.mediapost.com//?fa=Articles.printFriendly&art\\_aid=150148](http://www.mediapost.com//?fa=Articles.printFriendly&art_aid=150148).

<sup>39</sup>*Id.*

## Managing Security Risks in Business Associate Agreements

By Michael R. Overly, Chanley T. Howell, R. Michael Scarano



*Newspapers and trade journals feature a growing number of stories detailing instances in which organizations have entrusted their most sensitive information and data to a vendor or other business partner only to see that information compromised because the vendor failed to implement appropriate*

*information security safeguards. Worse yet, those same organizations are frequently found to have performed little or no due diligence regarding their vendors and have failed to adequately address information security in their vendor contracts, in many instances leaving the organizations without a meaningful remedy for the substantial harm they have suffered as a result of a compromise. That harm may take a variety of forms: damage to business reputation, loss of business, potential liability to the data subjects, and regulatory and compliance issues. Recent studies by the Ponemon Institute have shown that on average a company will pay \$202 per record compromised and, in the aggregate, an average of \$6.6 million if they experience a security breach.*

Those organizations, entities and individuals that provide health care services possess extremely sensitive and valuable information about patients, including both health and financial information. In today's business and legal environment, health care providers must be far more careful when entering into vendor relationships in which patient-identifiable information will be placed at risk. The Health Information Technology for Economic and Clinical Health Act and its implementing regulations (the "HITECH Act") strengthen the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA") by imposing stringent new fines for violations and adding a wide range of new requirements. For example, the HITECH Act requires providers to notify patients, the government and, in some cases, the media of certain security breaches involving their "unsecured" protected health information ("PHI").

The Department of Health and Human Services (HHS) has published guidance indicating that PHI can be properly "secured" if it is encrypted or destroyed in accordance with HHS guidelines. If PHI is "secured" then it is not subject to the security breach notification requirements. However, it is virtually impossible to maintain PHI in an encrypted state when it is in "use," i.e., being created, viewed, modified, etc. As a result, from a practical perspective, at any given moment providers will have significant PHI at risk of a security breach triggering the notification requirements.

Health care providers frequently hire vendors, referred to as business associates, to perform services involving PHI, including services that require the business associate to create, view or modify PHI. Such

PHI is also subject to the HITECH Act security breach notification requirements. However, if a business associate has a security breach that triggers the notification requirements, that business associate's sole obligation under the HITECH Act is to notify the provider. The obligation to notify affected patients and to take other required action remains with the provider. There could be significant costs associated with security breach notification, including, but not limited to, the cost of creating and sending out the required notifications and responding to queries and complaints from affected patients, as well as the costs to implement mitigation steps, such as free credit report monitoring. There may also be costs associated with negative publicity and investigation and enforcement action by the HHS Office of Civil Rights or other agencies. Absent contractual provisions that address allocation of liability for costs associated with security breach notification requirements, a provider will likely find itself liable for all costs connected to security breaches of PHI that was under the control of a business associate.

HIPAA and the HITECH Act contain requirements providers must follow when contracting with business associates, including contractually binding their business associates to implement security measures to protect PHI. However, providers are not legally required to monitor a business associate's contractual or statutory compliance with HIPAA and the HITECH Act. Although business associates are directly subject to the HIPAA Security Rule under the HITECH Act, as noted above, much of the risk and liability associated with security breaches remains with the providers. As a result, in this new environment, providers should take a more regimented approach to security to further mitigate risk. The recommendations in this article are intended to reduce the likelihood of security breaches by ensuring that business associates are obligated to provide "best practice" protections for handling PHI.

In this article, we discuss three tools providers can immediately put to use to substantially reduce the information security threats posed by their business associates, ensure proper due diligence is conducted and documented, and provide remedies in the event of a compromise. Those tools are: (1) the Due Diligence Questionnaire; (2) key contractual protections; and (3) the use in appropriate circumstances of an Information Security Requirements Exhibit. Whenever a business associate will have access to an organization's network, facilities, PHI or other sensitive or valuable data, one or more of these tools should be used.

Use of these tools will enable a provider to achieve a number of important goals:

- Reduce the risk of security breaches that trigger notification requirements under the HITECH Act and minimize potential liability. As noted above, costs arising out of security breaches and associated with security breach notification can be substantial. In addition to investigations by OCR or other government agencies, security breaches could result in actions by state attorneys general.
- Protect valuable assets of the provider. In many instances, a provider's proprietary and confidential information is *the* most important asset of the company (e.g., new service lines,

future marketing activities, prospective transactions, trade secret information, source code, etc.). Such information in the hands of a competitor could result in material harm for the provider. For publicly traded providers, a compromise of corporate data may result in shareholder suits against the officers of the corporation for failure to exercise reasonable business judgment in protecting that information.

- Create contractual remedies for providers in the event of a security breach by a business associate.
- Establish the provider has used due diligence in protecting PHI and its information systems. In the event of a compromise, the tools will assist the provider in documenting its efforts to minimize risk.
- Protect the provider's reputation and avoid the public embarrassment associated with a security compromise.

#### **Due Diligence: The First Tool**

Providers may conduct some form of due diligence before entrusting business associates with PHI or with access to their systems. However, the due diligence is often done informally, in a non-uniform manner, and is not clearly documented. In very few instances is the outcome of that due diligence actually incorporated into the parties' contract. This ad hoc approach to due diligence may no longer be appropriate or reasonable in the context of today's business and regulatory environment. To help to ensure proper documentation and uniformity of the due diligence process, especially for high risk arrangements, providers should consider developing a standard "Due Diligence Questionnaire" for prospective business associates to complete. Areas covered by the questionnaire would include: corporate responsibility, insurance coverage, financial condition, personnel practices, information security policies, physical security, logistical security, disaster recovery and business continuity, and other relevant issues.

Use of a standardized questionnaire has a number of significant benefits:

- It provides a uniform, ready-made framework for due diligence.
- It ensures an "apples-to-apples" comparison of business associate responses.
- It ensures all key areas of diligence are addressed and none are overlooked.
- It provides an easy means of incorporating the due diligence information directly into the parties' contract. That is, the completed questionnaire can be attached as an exhibit to the final business associate agreement, which will be executed along with the underlying services agreement.

From the outset, business associates must be on notice that the information they provide as part of the due diligence process and, in particular, in response to the Due Diligence Questionnaire, will be (i) relied upon in selecting the business associate; and (ii) incorporated into and made a part of the final business associate agreement, together with the underlying services agreement between the parties. To be most effective, the questionnaire should be presented to potential business associates at the earliest possible stage in the relationship. It should be included as part of all relevant RFPs or, if no RFP is issued, as a stand-alone document during preliminary discussions with the business associate.

Key areas for the Due Diligence Questionnaire include the following:

- *The business associate's financial condition.* Is the business associate a private or public company? Can the provider obtain copies of the most recent financial statements? Financial condition may not appear to be a critical factor for information security purposes, but the possibility a business associate may file bankruptcy or simply cease to do business while in possession of a provider's most sensitive information presents a substantial risk, especially in today's current economic environment. In such instances, it may be difficult, if not impossible, to retrieve the data and ensure it has been properly scrubbed from the business associate's information systems.
- *Insurance coverages.* What types of coverage does the business associate have? What are the coverage limits and other terms? Is the coverage claims made or occurrence based? Does the business associate's insurance cover liability related to privacy violations or security breaches?
- *Corporate responsibility.* Are there any criminal convictions, recent material litigation, instances in which the business associate has had a substantial compromise of security, or been investigated for privacy violations, etc.?
- *Subcontractors.* Will the business associate require the use of any subcontractors or affiliates in the performance of its services? Will the business associate use subcontractors or affiliates outside the United States? Where are the subcontractors and affiliates located? What types of services will they provide? What information, if any, of the provider will be sent to these entities? Transmission of PHI to contractors or subcontractors located outside the United States has been identified as creating unique risk. Such entities will not be subject to U.S. court jurisdiction. There have been highly publicized reports of situations where PHI was potentially subject to unauthorized disclosure, including an instance in which a non-US based contractor threatened to publish such PHI if it did not receive payments.
- *Organizational security procedures.* What are the business associate's information handling policies? Does it have a dedicated information security team? Is there an incident response team? What are the business associate's information security practices with contractors

and agents (e.g., due diligence, requiring non-disclosure agreements, specific contractual obligations relating to information security, etc.)?

- *Physical Security.* What physical security measures and procedures does the business associate employ?
- *Encryption.* Does the business associate use appropriate encryption technologies to protect PHI and other sensitive information?
- *Destruction.* Does the business associate destroy PHI and other sensitive information through appropriate methods, such as shredding paper, film or other hard copies, and clearing, purging or destroying electronic media in accordance with HIPAA requirements?
- *Technological Security.* Does the business associate have appropriate access controls and logging / audit trail capabilities? Does the business associate use system access control on its systems to limit information access to only those of its personnel who are specifically authorized?
- *Special Issues for Software Developers.* If the business associate is a software developer, what are its development and maintenance procedures? What security controls are used during the development lifecycle? Does the business associate conduct security testing of its software? Does the business associate maintain separate environments for testing and production? Does the business associate license code from third parties for incorporation into its products? If so, what types of code?
- *Policies.* If PHI is at risk, does the business associate have an information security policy and privacy policy? What is the revision history of its policies? Are there any instances where the business associate has had to report a significant breach of security?
- *Contingency Plans.* What are the business associate's business continuity/disaster recovery plans? When was its last test? When was its last audit? Were there any adverse findings in the audit? Have deficiencies been corrected? What is the revision history of its plan? What security procedures are followed at the recovery site?

### **Key Contractual Protections: The Second Tool**

In the overwhelming majority of engagements, the underlying services contract entered into between a provider and its business associates has little or no specific language relating to information security. At most, there is a passing reference to undefined security requirements set forth in the business associate agreement and a basic confidentiality clause. Of course, the business associate agreement should contain language requiring the business associate to comply with HIPAA, including a requirement to "implement reasonable and appropriate administrative, physical and technical

safeguards to protect the confidentiality, availability and integrity” of PHI. However, today’s best practices in business associate contracting suggest far more specific language is required. Moreover, the personnel responsible for negotiating the underlying services agreement are often not those charged with negotiating the business associate agreement. As a result, there is often a disconnect between the risks to PHI implicated by the types of contemplated services and the terms to protect such PHI, as well to protect the provider, in the business associate agreement. Providers should consider inserting very specific language into underlying agreements referencing information security provisions in the business associate agreement and clearly incorporating such agreement into the underlying services agreement. The underlying services agreement and the business associate agreement should be read together to ensure that ambiguities related to information security are eliminated, e.g., confidentiality provisions in the underlying agreement that could be interpreted to apply to PHI, which conflict with the terms of the business associate agreement.

Providers will likely have to amend their business associate agreements following the issuance of a final HITECH rule which is expected to set forth specific requirements for such amendments. Many providers have already done so based on provisions in the HITECH statute and proposed rule. Although providers are well advised to make the changes discussed in this article sooner rather than later, these mandated amendments will present a critical opportunity to more comprehensively address information security. In addition to other provisions that must be inserted under the HITECH Act, the following protections related to information security should be considered for inclusion in relevant business associate agreements:

### Warranties

In addition to any standard warranties relating to how the services are to be performed and authority to enter into the underlying services agreement, the following specific warranties relating to information security should be considered for business associate agreements:

- A warranty requiring the business associate to comply with “best industry practices relating to information security;”
- A warranty of compliance with the provider’s privacy policy in accessing, using and disclosing PHI;
- A warranty against sending PHI to offshore subcontractors or affiliates, unless specifically authorized to do so by the provider; and
- For those arrangements in which the Due Diligence Questionnaire has been completed, a warranty stating that the business associate’s responses to the Due Diligence Questionnaire, which should be attached as an exhibit to the contract, are true and correct.

### Address Specific Information Security Obligations

In addition to the provisions relating to the business associate's compliance with the HIPAA Security Rule, and generalized language relating to the business associate's obligations to take all reasonable measures to prevent unauthorized uses or disclosures of PHI and to report all breaches or potential breaches of security to the provider, consider addressing more specific information security obligations. Consider, where appropriate, inserting specific language requiring the business associate to secure and defend its information systems and facilities from unauthorized access or intrusion, to participate in joint security audits, to periodically test its systems and facilities for vulnerabilities, to use appropriate encryption and access control technology where applicable, and to use proper methods and techniques for destruction of PHI to render such PHI "secure," as set forth in the HHS guidance.

### Indemnity

Consider including, along with general indemnity language, a specific provision requiring the business associate to hold the provider harmless from claims, damages, and expenses incurred by the provider resulting from a breach of the business associate's security. That is, the business associate should protect the provider from lawsuits and other claims that result from the business associate's failure to adequately secure its systems. In the past, indemnity provisions were often negotiated out of business associate agreements. However, in light of the heightened enforcement environment, including the authority conferred upon state attorneys general to bring civil actions against providers, decisions to forego indemnification should be reevaluated in light of the risk under each business associate arrangement.

### Responsibility for Costs Associated with Security Breach Notification

As noted above, there could be significant costs associated with security breach notification, including costs related making the required notification, as well as costs associated with negative publicity and governmental investigation and enforcement action. Consider inserting provisions into the business associate agreement that require the business associate to pay for all costs associated with security breach notification requirements if a security breach occurs with PHI in the control of the business associate.

In addition to the business associate agreement, other provisions impacting information security in the underlying services agreement should be evaluated as follows:

### Limitation of Liability

Most software/services agreements, and many other services agreements have some form of "limitation of liability" – a provision designed to limit the type and extent of damages the contracting parties may be exposed to. It is not uncommon to see these provisions disclaim the business

associate's liability for all consequential damages (e.g., lost profits, harm to the provider's reputation, etc.) and limit all other liability to some fraction of the fees paid. These types of provisions are almost impossible to remove from most underlying services agreements, but it is possible to require the business associate to exclude from the limitations those damages flowing from the business associate's breach of the business associate agreement, including breaches related to information security obligations. Without these exclusions, the contractual protections described above would be essentially illusory. If the business associate has no real liability for breach of privacy or confidentiality because the limitation of liability limits the damages the business associate must pay to a negligible amount, the providers contractual protections are rendered meaningless.

### Confidentiality

The business associate agreement is the venue for protecting the privacy and security of PHI. However, a fully-fleshed out confidentiality clause should be the cornerstone for information security protections related to non-PHI in every underlying services agreement. The confidentiality clause should be broadly drafted to include all information the provider desires to be held in confidence. Specific examples of protected information should be included (e.g., source code, proprietary care plans, marketing plans, new product information, trade secrets, financial information, etc.). Although the term of confidentiality protection may be fixed – for, say, five years -- ongoing, perpetual protection should be expressly provided for valuable information, such as trade secrets of the provider. Requirements that the provider mark relevant information as “confidential” or “proprietary” should be avoided. These types of requirements are unrealistic in the context of most arrangements. The parties frequently neglect to comply with these requirements, resulting in proprietary, confidential information being placed at risk. It will be important to read the confidentiality provision carefully in conjunction with the protections for PHI under the business associate agreement to ensure there is no ambiguity.

### **Information Security Requirements Exhibit: The Third Tool**

The final tool in minimizing business associate information security risks is the use of an exhibit or statement of work to specifically define the security requirements relevant for a particular transaction. For example, engagements in which PHI or other highly sensitive information will be entrusted to a business associate may require the business associate to observe strict practices in its handling of the information. For example, the information security requirements exhibit may prohibit the business associate from transmitting the provider's information over internal wireless networks (e.g., 802.11a/b/g) or from transferring that information to removable media that could be easily misplaced or lost. The exhibit may also contain specific requirements for use of encryption and access control technology, decommissioning hardware and storage media on which the provider's information was stored to ensure the information is properly scrubbed from the hardware and media. Other specific physical and technological security measures should be identified as relevant to the particular transaction.

## CONCLUSION

Providers are presented with unique risks when they entrust PHI and their proprietary and confidential information to their business associates. Those risks can be minimized by employing the tools discussed in this article: appropriate and uniform due diligence, use of specific contractual protections relating to information security, and use -- where relevant -- of exhibits or other attachments to the agreement detailing unique security requirements to be imposed on the business associate.

*Michael R. Overly ([moverly@foley.com](mailto:moverly@foley.com)) is a partner in the Los Angeles office of Foley & Lardner LLP and a member of the firm's Information Technology & Outsourcing Practice Group. His practice focuses on drafting and negotiating technology-related transactions. He publishes a monthly, free e-mail newsletter regarding recent developments in technology law. Subscriptions can be obtained by sending an e-mail request to the above address.*

*Chanley T. Howell ([chowell@foley.com](mailto:chowell@foley.com)) is a partner in the Jacksonville office of Foley & Lardner LLP and a member of the firm's Information Technology & Outsourcing Practice Group. His practice focuses on drafting and negotiating technology-related transactions, and counseling clients on records and data management issues.*

*Mike Scarano ([mscarano@foley.com](mailto:mscarano@foley.com)) is a partner in the Del Mar office of Foley & Lardner LLP. He is Vice Chair of the firm's Health Care Industry Team and Co-chair of its Health Information Technology Work Group. His practice focuses on advising health care providers on HIPAA compliance and other regulatory issues.*

## Elephant in the Room: The Potential for Data Breach Statutory Damages

By Paul Paray



*While some data breach victims will eventually sustain an ID theft, it is generally acknowledged that the vast majority will not. Accordingly, the direct damages sustained by ID theft victims are not very helpful in a class action – there are just not enough plaintiffs to excite class action attorneys. Over the years, plaintiffs' class action counsel have spent many hours trying to create a damages theory that would actually be common to all victims of a data breach event. The two theories that have gotten the most class action traction are based on "fear of ID theft" or "lost time and effort" allegations. Unfortunately – for plaintiffs' counsel, that is – neither theory really fits the bill.*

### Damages Based on the "Fear of ID Theft"

Plaintiffs' class action counsel chasing down data breach events have generally been unsuccessful in pursuing claims based solely on the "fear of identity theft" or related incidental damages. Although *Ruiz v. Gap, Inc.*<sup>1</sup> instructs us there may be an outside chance of surviving a motion to dismiss, a defendant's summary judgment motion will eventually kill any claim brought by those who have not actually sustained theft of their identities. In effect, an actual incidence of ID theft – which after a breach can take quite a while to happen – has become the *de facto* precursor to compensable damages.

Despite what some plaintiffs' counsel have said after the standing ruling in *Krottner v. Starbucks*,<sup>2</sup> nothing has really changed this dynamic. In fact, as shown in *Ruiz* and other cases cited below, *Krottner* is not even the first court to rule federal standing exists for "fear of identity theft" claims.

By way of background, employees at Starbucks sued the company after the October 29, 2008 theft of a laptop computer containing "names, addresses, and social security numbers of approximately 97,000 Starbucks employees." *Id.* The trial court had previously dismissed the case, finding that Washington law doesn't recognize a cause of action where the only financial damage is "risk of future harm." The trial court also found insufficient facts to carry an implied contract claim.

In a pair of rulings issued last month, the Ninth Circuit agreed with the lower court and affirmed dismissal of the action<sup>3</sup> given that, under Washington law, "actual loss or damage is an essential element" of a negligence claim. This opinion on the merits was not approved for publication.

It is the standing ruling<sup>4</sup> – which was actually approved for publication – that has excited some in the data breach litigation business. The Ninth Circuit ruled plaintiffs had Article III standing given that

<sup>1</sup> <http://www.scribd.com/doc/32496484/Ruiz-v-Gap-9th-Cir-Apr-12-2010>

<sup>2</sup> Nos. 09-35823 and 35824 (9<sup>th</sup> Cir. , Dec. 14, 2010), <http://www.ca9.uscourts.gov/datastore/opinions/2010/12/14/09-35823.pdf>

<sup>3</sup> <http://www.scribd.com/doc/45306889/Krottner-v-Starbucks-No-09-35823-9th-Cir-Dec-14-2010-Memo>

"'generalized anxiety and stress' as a result of [a data breach] is sufficient to confer standing". It is very important to note that the court, quoting from *Equity Lifestyle Props., Inc. v. County of San Luis Obispo*,<sup>5</sup> recognized as a threshold matter that "[t]he jurisdictional question of standing precedes, and does not require, analysis of the merits." In other words, with jurisdictional standing you can reach the federal courthouse but once inside, you still need to prove your case – something plaintiffs here were unable to do given they lost at the district court level and on appeal.

In reaching its decision, the Ninth Circuit cites to cases on both sides of the issue. *Compare Doe v. Chao*,<sup>6</sup> (suggesting that a plaintiff who allegedly "was 'torn . . . all to pieces' and 'was greatly concerned and worried' because of the disclosure of his Social Security number and its potentially 'devastating' consequences'" had no cause of action under the Privacy Act, but nonetheless had standing under Article III) and *Pisciotta v. Old National Bancorp*,<sup>7</sup> (holding that plaintiffs whose data had been stolen but had not yet been misused suffered an injury-in-fact sufficient to confer Article III standing) with *Lambert v. Hartman*,<sup>8</sup> (although plaintiff's actual financial injuries resulting from the theft of her personal data were sufficient to confer standing, the risk of future identity theft was "somewhat 'hypothetical' and 'conjectural.'").

Looking to exploit its Pyrrhic victory, plaintiffs' counsel deftly uses the December 15, 2010 standing decision to solicit Starbucks employees<sup>9</sup> who may have actually sustained an ID theft:

[We] received a favorable precedential opinion from the United States Court of Appeals for the Ninth Circuit in *Krottner v. Starbucks Corporation*, No. 09-35823. In the opinion, the Ninth Circuit judges held that plaintiffs whose personal information had been stolen, but not misused, had standing to bring their case in federal court. The opinion held on the facts before it that the increased risk of future harm from identity theft was a credible enough treat [sic] to provide an injury-in-fact for Article III standing...

If you have any information regarding the Starbucks data breach, or if you believe you have been affected by the data breach and would like to discuss your rights and interests in this matter, please contact our Washington D.C. office.

### **Damages Based on "Lost Time and Effort"**

Thankfully (for defendants), there is no compelling precedent that expressly recognizes negligence or contract damages derived *solely* from the time and effort spent to remediate an alleged

---

<sup>4</sup> <http://www.ca9.uscourts.gov/datastore/opinions/2010/12/14/09-35823.pdf>

<sup>5</sup> 548 F.3d 1184,1189 n.10 (9th Cir. 2008, <http://www.leagle.com/xmlcontentlinks.aspx?gfile=548%20F.3d%201184>

<sup>6</sup> 540 U.S. 614, 617-18, 624-25 (2004).

<sup>7</sup> 499 F.3d 629, 634 (7th Cir. 2007).

<sup>8</sup> 517 F.3d 433, 437 (6th Cir. 2008).

<sup>9</sup> [http://www.finkelsteinthompson.com/featured\\_cases/finkelstein\\_thompson\\_llp\\_receives\\_favorable\\_appellate\\_opinion\\_in\\_data\\_breach\\_case.php](http://www.finkelsteinthompson.com/featured_cases/finkelstein_thompson_llp_receives_favorable_appellate_opinion_in_data_breach_case.php)

wrongdoing. Although mitigation damages are sometimes awarded in addition to other damages such as damages generally never rest as the sole measure of damages in either a negligence or contract setting. This general rule manifests as the “economic loss rule” in some jurisdictions (used to bar recovery in negligence when the only loss is pecuniary) or is simply bolted on to the concept of damages in other jurisdictions.

Seeking to resolve a “lost time and effort” argument made by plaintiffs in a very public data breach context, on November 24, 2009, Judge D. Brock Hornby, the federal district judge in Maine presiding over the Hannaford Brother data breach litigation, certified the following question to the Maine Supreme Court:

In the absence of physical harm or economic loss or identity theft, do time and effort alone, spent in a reasonable effort to avoid or remediate reasonably foreseeable harm, constitute a cognizable injury for which damages may be recovered under Maine law of negligence and/or implied contract?<sup>10</sup>

On September 21, 2010, the Maine Supreme Court answered this question in the negative. Relying on longstanding law, Maine’s highest court responded to Judge Hornby without equivocation: “[Maine case law] does not recognize the expenditure of time and effort alone as a harm.”<sup>11</sup> Rejecting a “mitigation of damages” argument that would elevate expended time and effort to the status of a compensable legal injury, the court ruled, “[u]nless the plaintiffs’ loss of time reflects a corresponding loss of earnings or earning opportunities, it is not a cognizable injury under Maine law of negligence.” And, quoting the lower court, given that “the time and effort expended by the plaintiffs here represent ‘the ordinary frustrations and inconveniences that everyone confronts in daily life’” damages were also not available under the implied contract claim.

Although other courts have made passing comments regarding the relevance of “lost time” as a sole measure of damages, the Maine Supreme Court decision is the only decision on all fours within a data breach context. *Id.* (“In other cases, a passing mention of loss of time without adequate facts to demonstrate how those damages were being measured is insufficient to persuade us that the expenditure of time and effort alone is a harm recoverable in negligence.”)<sup>12</sup>

Even if a future court found these damages standing alone somehow compensable, there exists another barrier that would likely stymie future class certification motions relying on this damages

---

<sup>10</sup> *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 671 F. Supp. 2d 198, 201 (D. Me. 2009), [http://www.med.uscourts.gov/Opinions/Hornby/MDL/MDL1954\\_2009\\_11\\_24\\_ORDER7.pdf](http://www.med.uscourts.gov/Opinions/Hornby/MDL/MDL1954_2009_11_24_ORDER7.pdf).

<sup>11</sup> *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492 (Me. 2010).

<sup>12</sup> *Citing Kuhn v. Capital One Fin. Corp.*, No 05-P-810, 2006 WL 3007931, at \*3 (Mass. App. Ct. Oct. 23, 2006); *Freeman v. Missouri Pac. Ry. Co.*, 167 P. 1062, 1063-65 (Kan. 1917)).

theory -- courts would have a tough time finding an efficient means of determining on a class-wide basis the value of a plaintiff's "time and effort". Although courts have recognized that the need for individualized proof of damages is not *per se* an obstacle to class certification, the measure of a plaintiff's relative "time and effort" would likely not predominate any data breach putative class.

To the extent such thorny class certification issues would possibly resolve differently among the federal circuits, the U.S. Supreme Court may soon add some needed clarity. On December 6, 2010, the Court agreed to review the April 27, 2010 decision by the U.S. Court of Appeals for the Ninth Circuit granting class certification in the massive Wal-Mart sexual discrimination case.<sup>13</sup> "Petition for writ of certiorari to the United States Court of Appeals for the Ninth Circuit granted limited to Question I presented by the petition. In addition to Question I, the parties are directed to brief and argue the following question: "Whether the class certification ordered under Rule 23(b)(2) was consistent with Rule 23(a)." (emphasis added).

Although named plaintiffs in the *Wal-Mart* case "waived any claim for compensatory damages, forfeiting the rights of individual class members to recover damages authorized by Congress solely in order to facilitate class treatment", an important commonality ruling remains likely given the Court specifically requested that the parties brief the applicability of Federal Rule of Civil Procedure 23(a).<sup>14</sup> One way or the other, the Supreme Court's decision in *Wal-Mart* will impact the class action landscape – including the potential landscape surrounding breach class action suits.

### **Data Breach Class Action Suits -- Will the Floodgates Ever Open?**

It may not arrive this year or next but the time will likely eventually come when class actions are routinely certified after a significant data breach. As discussed above, these future certified class actions will not likely derive from courts applying a new and improved "fear of" or "lost time" damages theory. Moreover, this shift certainly won't happen using a newly varnished claim theory based on lost chattel, conversion, or a constructive bailment.

### **Statutory Damages in Data Breach Class Action Suits**

Over the years, plaintiffs' class action counsel have utilized their jet flyover time trying to create a claims theory that would be common to any victim of a data breach event. For the reasons set forth above, theories based on a "fear of ID theft" or "lost time and effort" have not withstood scrutiny in a class action setting – nor will likely in the future. So, what exactly is the damages theory that will someday clog the class action dockets of judges around the country?

In the same way state breach notification statutes jump started data breach litigation, aggressive legislative bodies will again likely lead the way. It appears as if the only real significant liability threat

---

<sup>13</sup> See [Dukes v. Wal-Mart Stores, Inc.](#), 603 F.3d 571 (9<sup>th</sup> Cir. 2010), [cert. granted, Wal-Mart Stores, Inc. v. Dukes](#), 178 L. Ed. 2d 530 (2010).

<sup>14</sup> See [Petitioners Brief](#) at 35, dated January 20, 2011.

to those companies sustaining a data breach is the advent of statutory damages – damages that would ensue with or without any showing of real harm to a plaintiff. No matter how small the statutory amount per breach victim, such statutes will not only open up the class action floodgates – they will literally blow them wide open. Although there is no such law on the books right now, companies need to remain diligent and prepare for the day when the first statutory damages law is enacted.

Maybe there is some level of poetic justice in the fact that the volcanic state of Hawaii – by virtue of S.B. 728 or a watered down version of S.B. 728 – may become the first state to expressly provide for such damages.<sup>15</sup> After all, the potential business impact is much like a volcano erupting. Before getting to Hawaii’s newly introduced bill – which on February 11, 2011 was voted by a standing committee to be held from the full house for further consideration<sup>16</sup> – it might be helpful to reference a potential framework for statutory damages using two laws that are decades old and a more recent law that already acts as an ID theft prevention statute.

### **The Video Privacy Protection Act of 1988 (VPPA)<sup>17</sup>**

On December 17, 2009, a class action Complaint<sup>18</sup> was filed against Netflix, Inc., alleging that Netflix “perpetrated the largest voluntary privacy breach to date.” According to the Complaint, Netflix knowingly and voluntarily disclosed the video purchases of approximately 480,000 Netflix subscribers when Netflix provided to contest participants data containing over 100 million subscriber movie ratings and preferences. When launching its contest, Netflix stated that all provided data was anonymized and that the subscribers’ movie ratings were given tokenization numbers, *i.e.*, “numeric identifier unique to the subscriber” rather than any actual personal data.<sup>19</sup> The Complaint alleges researchers were able to identify individual subscribers by cracking Netflix’s anonymization process.<sup>20</sup>

Among other claims, plaintiffs brought suit under VPPA seeking statutory damages. VPPA generally prohibits any “video tape service provider” from “knowingly disclosing the personally identifiable information concerning any customer of such provider” (18 U.S.C. 2710(b)). According to EPIC,<sup>21</sup> this law “stands as one of the strongest protections of consumer privacy against a specific form of data collection.” In addition to other VPPA damages that may be awarded, VPPA provides for “actual damages but not less than liquidated damages in an amount of \$2,500.” (18 U.S.C. 2710(c)(2)(a)).

---

<sup>15</sup> [http://www.capitol.hawaii.gov/session2011/Bills/SB728\\_.pdf](http://www.capitol.hawaii.gov/session2011/Bills/SB728_.pdf)

<sup>16</sup> [http://www.capitol.hawaii.gov/session2011/lists/measure\\_indiv.aspx?billtype=SB&billnumber=728](http://www.capitol.hawaii.gov/session2011/lists/measure_indiv.aspx?billtype=SB&billnumber=728)

<sup>17</sup> [http://www.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00002710----000-.html](http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002710----000-.html)

<sup>18</sup> [http://www.wired.com/images\\_blogs/threatlevel/2009/12/doe-v-netflix.pdf](http://www.wired.com/images_blogs/threatlevel/2009/12/doe-v-netflix.pdf)

<sup>19</sup> *Id.* at Paragraph 32(b)).

<sup>20</sup> *Id.* at Paragraph 37.

<sup>21</sup> <http://epic.org/privacy/vppa/>

On March 19, 2010, the case was dismissed pursuant to a confidential settlement between the named plaintiffs and Netflix.<sup>22</sup> For some reason – maybe due to Federal Rules of Civil Procedure 23(a) concerns given the choice of plaintiff representative or an offer too good to pass up – plaintiffs’ counsel chose to resolve this suit prior to seeking certification of the class. Although it would have been interesting to see how this privacy statutory damages suit resolved itself via motion practice, the case remains noteworthy given legislative bodies may look to it to see how quickly class action suits can resolve themselves when faced with statutory damages.

### **Song-Beverly Credit Card Act of 1971**<sup>23</sup>

This California law protects consumers from merchants who request personal data during a credit card transaction – in essence, a very old privacy statute. A recent California Supreme Court case, *Pineda v. Williams-Sonoma Stores, Inc.*,<sup>24</sup> applied basic statutory construction rules to this statute and found that “personal identification information concerning the cardholder” includes a person’s ZIP code. What is noteworthy about the case is not the result as much as it is the fact it has immediately created a significant spike in class action “privacy” suits.<sup>25</sup>

This increase in class action suits (which will obviously abate a bit after retailers modify their checkout policies) results from a court’s ability to now award statutory civil penalties up to a maximum \$250 for the first violation and \$1,000 for subsequent violations – all because a cashier asks for a ZIP code during checkout. Although technically not a privacy ruling (this case is a statutory construction 101 case), it definitely helps move the ball towards a statutory damages goalpost.

Unless the California Legislature decides to clarify the statute in light of *Pineda*, this decision stands as a very low threshold both for what may constitute “personal identification information” pursuant to state law and for what sort of minor privacy transgression merits a statutory damages award. And, if the California Legislature decides not to change the statute, it will signal that potential mega-class action suits are not something that will prevent future legislatures from enacting privacy laws with much more bite. Although decided *prior* to *Pineda*, a Ninth Circuit decision referenced below picks up the ball from *Pineda* and moves it much further down the field when it comes to sanctioning mega class actions involving privacy indiscretions.

### **Fair and Accurate Transaction Act of 2003 (FACTA)**<sup>26</sup>

Among other things, FACTA provides consumers with a very important anti-ID theft protection. Specifically, the law provides that, “no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration

<sup>22</sup> <http://docs.google.com/gview?url=http://docs.justia.com/cases/federal/district-courts/california/candce/5:2009cv05903/222519/14/0.pdf?1269975532&chrome=true>

<sup>23</sup> <http://www.leginfo.ca.gov/cgi-bin/waisgate?WAIISdocID=81928212795+5+0+0&WAIISaction=retrieve>

<sup>24</sup> <http://blog.digitalriskstrategies.com/is-geo-data-a-new-privacy-battleground/>

<sup>25</sup> <http://www.law.com/jsp/ca/PubArticleFriendlyCA.jsp?id=1202482142062>

<sup>26</sup> <http://www.ftc.gov/os/statutes/031224fcra.pdf>

date upon any receipt provided to the cardholder at the point of the sale or transaction.” (15 U.S.C. § 1681c(g)(1)). A willful failure to comply with these requirements allows for statutory damages “in an amount equal to the sum of any actual damages sustained by the consumer as a result of the failure or damages of not less than \$100 and not more than \$1,000.” (15 U.S.C. § 1681n(a)(1)(A)).

In *Zaun v. J.S.H. Inc. of Faribault d/b/a Long John Silver's – Mall of America*,<sup>27</sup> the court dismissed a class action complaint based on a violation of the above FACTA requirement (no willfulness) but recounts other FACTA class action cases able to withstand a motion to dismiss. All of those cases may have pushed the privacy statutory damages envelope but the case that provides the most ammunition for a full frontal assault is *Bateman v. American Multi-Cinema, Inc.*<sup>28</sup> In *Bateman*, the Ninth Circuit flat out rejects defendant’s argument that “minor” privacy transgressions should not be able to morph into a class action potentially totaling \$290 million in statutory damages – 290,000 credit card receipts in violation of FACTA. In reaching its conclusion, the court in *Bateman* reasons:

In the absence of such affirmative steps to limit liability, we must assume that Congress intended FACTA's remedial scheme to operate as it was written. To limit class availability merely on the basis of ‘enormous’ potential liability that Congress explicitly provided for would subvert congressional intent.... Here, AMC did not argue before the district court that the potential \$ 290 million liability would put it out of business, nor did it submit any declarations, documents, or other evidence demonstrating that such liability would be ‘ruinous.’

The court in *Bateman* also recognized that “the civil liability provisions were added in order to assist consumers in ‘protect[ing] their privacy.’”<sup>29</sup> To that end, “[a]llowing consumers to recover statutory damages [deters] businesses from willfully making consumer financial data available, even where no actual harm results.” *Id.* The full impact of this case remains to be seen given that it has not yet been resolved – the Ninth Circuit remanded for further findings on the class certification motion.

Recognizing the potential adverse business impact of this case, the US Chamber of Commerce has fought hard to reverse the ruling.<sup>30</sup> Although there is an apparent dispute among the Circuits that should be fodder for a cert grant and it is not uncommon for the Ninth Circuit to get overturned by the Supreme Court, the *Bateman* decision may never land in the Supreme Court. More importantly, it is far from clear what direction the Supreme Court would take if it even heard the case.

---

<sup>27</sup> 2010 U.S. Dist. LEXIS 102062 (D. Minn. Sept. 28, 2010), [http://courtops.org/wp-content/uploads/2010/10/FCRA\\_wrongslip\\_10113334299.pdf](http://courtops.org/wp-content/uploads/2010/10/FCRA_wrongslip_10113334299.pdf)

<sup>28</sup> 623 F.3d 708 (9<sup>th</sup> Cir. 2010) (*en banc* petition pending), *reversing, Bateman v. American Multi-Cinema, Inc.*, 252 F.R.D. 647 (C.D. Cal. 2008). <http://www.ca9.uscourts.gov/datastore/opinions/2010/09/27/09-55108.pdf>

<sup>29</sup> *Id.* (quoting S. Rep. No. 103-209, at 6 (1993)).

<sup>30</sup> <http://www.chamberlitigation.com/sites/default/files/cases/files/2010/Bateman%20v%20American%20Multi-Cinema,%20Inc.%20%28NCLC%20Brief%29.pdf>

Where does this trilogy of laws and resulting privacy class actions leave us? For one, they can be perceived as a solid vote in favor of the viability of class actions suits tied to privacy-related statutory damages. After all, these three privacy laws providing for statutory damages have withstood class action scrutiny without any subsequent limiting legislative changes – even though such laws can readily be amended to curtail the availability of class actions. Second, they demonstrate courts have no problem remedying minor individual privacy infractions with massive class actions. Third, and most importantly, they provide concrete examples for future legislatures who may want to address the typical data breach scenario – compromised privacy rights yielding little actual harm.

As succinctly put by the court in *Bateman*, “[t]he need for statutory damages to compensate victims is plain. The actual harm that a willful violation of FACTA will inflict on a consumer will often be small or difficult to prove.” Couple the above trilogy with the fact that there are other “privacy-related” laws that provide for statutory damages and there exists the workings of a potential framework.<sup>31</sup>

### **Hawaii’s S.B. 728<sup>32</sup>**

After the University of Hawaii’s latest data breach took place this past October<sup>33</sup> – its third significant breach in under one year’s time – Hawaii’s state legislature chose to get on the offensive. On January 21, 2011, S.B. 728 was formally introduced, including the following language:

If a judgment is obtained by the plaintiff, the court shall award the plaintiff a sum of not less than \$ [yet to be determined] or threefold damages sustained by the plaintiff, whichever sum is greater, and reasonable attorney's fees and costs. Damages sustained by the person shall include actions taken to mitigate injury from future identity theft, including actual or future purchase of credit report monitoring and identity theft insurance.

Given that two of three committees have recently held the bill,<sup>34</sup> it is not clear where this is all heading. It may be the case that the February 8, 2011 hearing which yielded significant opposition from the business community<sup>35</sup> transformed the bill into a political hot potato that is now potentially DOA. Although Pearl Harbor analogies are obviously premature, the opening salvo remains cleanly fired from Hawaii.

It is the California legislature that, not surprisingly, may eventually again lead the way. A California bill introduced on February 8, 2011, S.B. 208<sup>36</sup> requiring restitution payments from criminal defendants to their ID theft victims, states that “the immediate preservation of the public peace, health, or safety

---

<sup>31</sup> See e.g., [Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC](#), 08-civ-4810 (S.D.N.Y. Dec. 22, 2010) (awarding statutory damages for a violation of the [Stored Communications Act](#), 18 U.S.C. § 2707).

<sup>32</sup> [http://www.capitol.hawaii.gov/session2011/Bills/SB728\\_.pdf](http://www.capitol.hawaii.gov/session2011/Bills/SB728_.pdf)

<sup>33</sup> <http://uhwo.hawaii.edu/idalert>

<sup>34</sup> [http://www.capitol.hawaii.gov/session2011/lists/measure\\_indiv.aspx?billtype=SB&billnumber=728](http://www.capitol.hawaii.gov/session2011/lists/measure_indiv.aspx?billtype=SB&billnumber=728)

<sup>35</sup> [http://www.capitol.hawaii.gov/session2011/Testimony/SB728\\_TESTIMONY\\_CPN-EDT\\_02-08-11.pdf](http://www.capitol.hawaii.gov/session2011/Testimony/SB728_TESTIMONY_CPN-EDT_02-08-11.pdf)

<sup>36</sup> [http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb\\_0201-0250/sb\\_208\\_bill\\_20110208\\_introduced.pdf](http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0201-0250/sb_208_bill_20110208_introduced.pdf)

within the meaning of Article IV of the Constitution” includes ensuring that “an identity theft victim can monitor their credit report and repair his or her credit at no cost to him or her.” This is the sort of constitutional spin (albeit a necessity here to get the bill fast tracked) that might finally make statutory damages – which are *de facto* punitive – a reality. Until that sad day arrives, companies are well advised to continue to update their various policies to comply with applicable security standards<sup>37</sup> and continually test their internal controls as well as bolster their defenses<sup>38</sup> by deploying reasonable security measures.<sup>39</sup>

*Paul E. Paray, Esq. is a commercial litigator with over 15 years experience resolving complex claims. Paul is a member of the New York, New Jersey, and District of Columbia Bars and has spoken and written extensively on the management of digital risk. He can be reached at [paule@paray.com](mailto:paule@paray.com).*

---

<sup>37</sup> <http://blog.digitalriskstrategies.com/new-ma-data-protection-law-impacts-companies-around-the-country/>

<sup>38</sup> <http://blog.digitalriskstrategies.com/pc-world-self-encrypted-drives-set-to-become-standard-fare/>

<sup>39</sup> <http://blog.digitalriskstrategies.com/regulatory-and-judicial-enforcement-of-reasonable-security/>

## Committee Co-Chairs' Message

Dear ISC Members:

On February 12-13 of this year, our committee held a pre-RSA meeting in San Francisco attended by a number of committee members. This meeting covered topics such as FTC enforcement actions, security research, COICA, health care disclosure requirements, business partner security questionnaires, in-house legal defensibility perspectives, reducing risk and increasing resilience, and robotics liability. We want to thank Foley & Lardner LLP for use of their offices. Our next meeting semi-annual schedule will be announced soon.

Also, keep an eye posted for upcoming webinar announcements that we create or host from time to time.

Finally, we continue to ask that you share your knowledge and experience with your fellow professionals and committee members by writing an article for this periodical. Our next issue (Autumn 2011) will come out in September. That is it for now. We look forward to seeing you at our next in-person meeting or on our next webinar.

David Navetta and Kathryn Coburn, ISC Co-Chairs