

David Navetta: 'Potential changes to the US breach notice risk landscape'

REPRINTED WITH PERMISSION OF CECILE PARK PUBLISHING
(February 2010)

www.e-comlaw.com
+44 (0) 20 7012 1380

CECILE PARK PUBLISHING

Editor Eduardo Ustaran
eduardo.ustaran@fw.com
Managing Editor Rita Di Antonio
rita.diantonio@e-comlaw.com
Associate Editor Jaya Tackopersadh
jaya.tackopersadh@e-comlaw.com
Editorial Assistant Asta Puraite
asta.puraite@e-comlaw.com
Subscriptions John Archer
john.archer@e-comlaw.com
telephone +44 (0)20 7012 1387
Sales and Marketing Karl Behrouz
karl.behrouz@e-comlaw.com
telephone +44 (0)20 7012 1384
Design Madeline Earnest
www.madeinearnest.com
Print The Premier Print Group

Data Protection Law & Policy is published monthly by Cecile Park Publishing Limited 17 The Timber Yard, Drysdale Street, London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093

© Cecile Park Publishing Limited.
All rights reserved. Publication in whole or in part in any medium, electronic or otherwise, without written permission is strictly prohibited. ISSN 1743-6605.

CECILE PARK PUBLICATIONS

E-Commerce Law & Policy

Monthly: launched February 1999
E-Commerce Law & Policy is a unique source of analysis and commentary on global developments in e-business legislation.
PRICE: £420 (£440 overseas).

E-Commerce Law Reports

Six issues a year: launched May 2001
The reports are authoritative, topical and relevant, the definitive practitioners' guide to e-commerce cases. Each case is summarised, with commentary by practising lawyers from leading firms specialising in e-commerce.
PRICE: £420 (£440 overseas).

E-Finance & Payments Law & Policy

Monthly: launched October 2006
E-Finance & Payments Law & Policy provides all those involved in this fast evolving sector with practical information on legal, regulatory and policy developments.
PRICE £520 (£540 overseas).

Data Protection Law & Policy

Monthly: launched February 2004
Data Protection Law & Policy is dedicated to making sure that businesses and public services alike can find their way through the regulatory maze to win the rewards of effective, well-regulated use of data.
PRICE £390 (£410 overseas / £290 Govt).

World Online Gambling Law Report

Monthly: launched April 2002
World Online Gambling Law Report provides up-to-date information and opinion on the key issues confronting the industry.
PRICE £520 (£540 overseas).

World Sports Law Report

Monthly: launched September 2003
World Sports Law Report is designed to address the key legal and business issues that face those involved in the sports industry.
PRICE £520 (£540 overseas).

DataGuidance

Launched December 2007
The global platform for data protection and privacy compliance.
www.dataguidance.com

Potential changes to the US breach notice risk landscape

The House of Representatives approved the new Data Accountability and Trust Act (DATA) on 8 December 2009. If passed, the Act would preempt many state breach notification laws and introduce a federal notification requirement. David Navetta, Founding Partner of the Information Law Group, discusses the potential impact of DATA on data breach policies and risk assessments for large and small companies in the US.

The Data Accountability and Trust Act (DATA) is a comprehensive federal data security law that explicitly preempts state law - including state breach notice laws passed in approximately 42 US states. If passed in its current form, it will likely have a significant impact on a substantial majority of companies handling personal information of US residents. The Act addresses three main areas:

- information security requirements for personal information in general;
 - information security requirements for personal information for 'information brokers'; and
 - breach notice obligations.
- This article focuses on the Act's breach notice obligations.

DATA's similarities to state breach notice laws

In many respects, DATA's breach notice obligations include the same or similar elements as the breach notice laws currently in place in approximately 42 US states. The following elements are common - but perhaps not exactly the same - in both DATA and many state breach notice laws:

- The person or entity that 'owns or possesses' personal information

has the primary obligation to notify the affected individuals.

- Third party agents and service providers maintaining or processing data on behalf of the data owner/possessor have an obligation to notify the owner/possessor of a security breach.
- Delay of notification is permitted if law enforcement determines that notification would impede a criminal or civil investigation.
- The primary means of notice is via written notification or by email - but only if email is the primary means of communication and the consent requirements of the E-SIGN Act (15 U.S.C. 7001) have been satisfied.
- Substitute notice is allowed under certain circumstances, including email notification, notice via a website and notification in print and broadcast media.
- Notice is required only if a risk of harm threshold has been met - DATA's harm threshold is higher than that in many state breach notice laws.
- Encrypted personal data may allow entities to avoid notice obligations, although DATA provides a 'presumption' of no harm rather than a strict encryption 'safe harbor'.
- Notification is triggered by unauthorized access to or acquisition of data in electronic form (note that some states' breach notice laws do apply to personal information in paper form).
- The definition of personal information is first name/initial and last name in combination with one or more data elements typically listed in state breach notice laws (e.g. social security number, driver's license/ID card or financial account/payment card number and required security/access code).

DATA's variations from state breach notice laws

If passed in its current form, the breach notice provisions of DATA will include some significant variations from most current state breach notice laws. Based on the preemption provisions in the Act, these differences could change the breach notice landscape relative to existing state laws:

- Notice must be provided within 60 days after the discovery of a breach of security (note that some states do impose specified deadlines for notice - the Florida notice deadline is 45 days).
- Notice must be provided to the Federal Trade Commission (FTC) in addition to affected individuals, and the FTC has the option, in its discretion, to post the notice letter on its website (note that many state laws require a notice to state Attorneys General).
- For breaches involving more than 5,000 affected individuals, notice must be provided without unreasonable delay to the major credit reporting agencies.
- The notices must include a toll-free number that affected individuals can call to receive information about the breach (e.g. a call center).
- The entity must offer affected individuals, free of charge, two years of credit monitoring services or access to their credit reports on a quarterly basis (although this requirement does not appear to apply to some payment card breach situations).
- Notice can be delayed if a federal national security agency determines that notification would threaten US national security.
- The risk of harm threshold provides that notice is required unless there is no reasonable risk of identity theft, fraud, or other unlawful conduct.
- Civil penalties of up to \$11,000 per violation are possible - with an

aggregate cap of \$5 million per breach of security - each failure to send the required notification is treated as a separate violation.

● The Act explicitly does not provide a private right of action (many states' breach notice laws don't provide a private right of action, although some are less explicit than others).

Analysis

DATA's breach notice obligations have the potential to significantly alter the breach notice landscape in the United States. This section explains some of the potential material impacts of DATA if passed in its current form.

Preemption

One of the most significant DATA impacts arises out of its preemption clause, which appears to fully preempt state law. Unlike the Health Insurance Portability and Accountability Act of 1996 (HIPAA), DATA does not preempt only those state laws that are 'less stringent' or 'contrary to' the Act. Rather, DATA 'supersedes any provision of a statute, regulation, or rule of a State...that expressly...requires notification to individuals of a breach of security resulting in unauthorized access to or acquisition of data in electronic form containing personal information.'

While a preemption analysis is beyond the scope of this article, one reason some would welcome a fully preemptive federal law is the desire for a single breach notice standard rather than 42 separate standards. Many personal information breaches involve the personal information from residents of more than one state - and for bigger breaches it is not unusual for residents of all 50 states to be impacted. This necessitates understanding and complying with the requirements

Unlike HIPAA, DATA does not preempt only those state laws that are 'less stringent' or 'contrary to' the Act. Rather, DATA 'supersedes any provision of a statute, regulation, or rule of a State...that expressly...requires notification to individuals of a breach of security'

of each individual state. In many cases, rather than undertake such an onerous exercise, many breached companies simply use a 'lowest common denominator' approach. Using this approach, if a breached company triggered notice obligations in a state with a low risk of harm threshold (e.g. a reasonable belief that personal information was acquired by an unauthorized person), it would simply provide notice to all the affected individuals (even in those states where the risk of harm threshold may not have been met). This could lead to 'over-reporting'. Assuming DATA provides for full preemption, it would eliminate the need to employ such an approach, and the notice trigger would be limited to single standard. Significantly, under DATA, as compared to many states, the triggering 'risk of harm' standard is relatively high.

However, there is one significant caveat with respect to preemption: the Act does not apply to every person or entity in the United States. Rather, DATA only applies to those entities over which the FTC has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act. As such, DATA would not appear to apply to financial institutions, insurance companies, governmental bodies or common carriers (e.g. telecommunications companies or transportation companies). Those entities would still be required to comply with state breach notice laws, even if DATA is passed.

Risk of harm

The trigger for state breach notice laws often comes down to the risk of harm posed to personal information by the security breach. On one end of the spectrum are those laws that are triggered by a reasonable belief of unauthorized access to personal information,

while others require a likelihood of 'harm' or 'misuse' of personal information. The following are examples of risk of harm triggers from various states:

● Arizona: 'personal information was or is reasonably believed to have been acquired by an unauthorized person';
 ● Colorado: 'the likelihood that unencrypted personal information has been or will be misused';
 ● Connecticut: 'personal information was or is reasonably believed to have been accessed by an unauthorized person'; and
 ● Florida: 'notice is not required if after reasonable investigation the person determines there is no reasonable likelihood of harm to customers'.

Assuming DATA is passed and fully preempts state laws, all of these competing standards would be eliminated. Instead, notice would be required only if the breached entity determines there is a 'reasonable risk of identity theft, fraud or other unlawful conduct'. This risk of harm standard arguably falls on the higher end of the spectrum. For example, in the case of a lost laptop, without evidence that the laptop fell into the hands of wrongdoers, there may not be a reasonable risk of identity theft, fraud or unlawful conduct. In contrast, if the notice trigger was a reasonable belief of unauthorized acquisition, notice to affected individuals of the missing laptop might be required. The overall impact of this change is likely to be less reporting of breaches for two reasons:

● it eliminates the need to engage in a 'lowest common denominator' approach and decreases 'over-reporting'; and
 ● the risk of harm standard in DATA is relatively higher than many states.

It follows further that, for companies that only conduct

SECURITY BREACH

business with residents in those states with low harm thresholds, the relative chance of having to provide notice of breach may be decreased under DATA.

Enforcement

While the trigger for DATA may be relatively higher, the enforcement provisions of the Act could act as a counterbalance. Even though the Act does not provide for a private right of action, it does provide for potentially significant civil penalties in the event the Act is not complied with. Under the Act, the FTC can impose civil penalties of up to \$11,000 per violation, and each failure to send the required notification to an affected individual is treated as a separate violation. However, civil penalties are capped out at \$5 million per breach of security.

In practice, these penalties are likely to encourage breached companies to make very careful decisions about whether the Act was triggered by a breach of security. In particular, a company that makes the wrong call with respect to DATA's risk of harm trigger and fails to report a breach, may be liable for significant 'per person' penalties. The deterrent impact of these fines and penalties will be influenced by the aggressiveness of the FTC's enforcement practices. If the FTC actively looks for unreported breaches in order to bring enforcement actions or establishes processes for affected individuals to report suspected personal information breaches, the deterrent effect of the civil penalties is likely to increase. Moreover, the potential

civil penalties are more likely to impact smaller and medium-sized companies, as they will have relatively more to lose if they fail to provide the required notice.

Additional 'multiplier expenses' under DATA

With state breach notice laws, the typical expenses to achieve compliance include attorney fees to analyze the laws, forensic expenses to determine what happened in the breach and whether personal information was impacted, as well as costs to prepare and send the mailings (e.g. paper, printing, envelopes and postage). The mailing costs represent a 'multiplier expense' – there is a cost ranging from approximately \$0.10 to \$2 per mailing sent to each affected individual. For larger breaches, mailing costs can add up quickly and often outstrip attorney fees and forensic expenses. None of this has changed under DATA. DATA, however, adds two new 'multiplier expenses' to the mix that are not present in state breach notice laws. Firstly, companies that must notify under DATA are also obligated to provide a toll-free number for affected individuals who wish receive additional information about the breach. For smaller breaches it may be possible to handle these phone inquiries 'in house', but for larger breaches it may be necessary to retain a third party call center to handle the breaches. Third party call center services can cost \$0.50 to \$1 per affected individual. Again, when multiplied by tens of thousands or millions of individuals, these expenses can become significant.

Secondly, DATA requires the breached entity to offer credit protection services. Breached entities can choose one of two options: free consumer credit reports from at least one of the major credit reporting agencies available on a quarterly basis for two years, or credit monitoring services available for two years. These expenses, especially for larger breaches, can be astronomical.

The magnitude of the potential expenses that arise out of a breach covered under DATA represent a major change from state breach notice laws. Ironically, they also may encourage companies to avoid reporting breaches in order to avoid substantial expenses, acting as a counter-force to the civil penalties under the Act.

David Navetta Founding Partner
Information Law Group
djn@davidnavetta.com

SIGN UP FOR FREE E-LAW ALERTS

Data Protection Law & Policy provides a free alert service. We send out updates on breaking news, forthcoming events and each month on the day of publication we send out the headlines and a precis of all of the articles in the issue.

To receive these free e-law alerts, register on www.e-comlaw.com/updates.asp or email erika.joyce@e-comlaw.com