dataprotectionlaw&policy

FEATURED ARTICLE
02/09

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

US: Challenges facing privacy framework

Within days of taking office, President Obama's Administration issued its Technology agenda - emphasising the importance of technology in advancing competition - and its Homeland Security agenda - which includes policy objectives to protect information networks in the US. David Fagan and Lisa Bress, Associates at Covington & Burling LLP, examine the challenges facing the Administration as regards the US's short-term data protection legal framework.

The Obama Administration's approach to cybersecurity and data protection, like so many other areas, is the subject of keen interest among lawmakers and observers both in the United States and abroad. This interest is owed in part to the fact that, like so many other areas, the Obama Administration has suggested that it intends to pursue change in the US government's policies and laws with respect to securing personal data. The new President is not alone in championing this position; in the months leading up to the new Administration, prominent third party studies and federal regulators advocated many proposals that the White House has since formally adopted as policy objectives. Nevertheless, there remain significant challenges to any meaningful shift in the US data protection legal framework in the near term.

There is little doubt about the Obama Administration's desire to promote policies that advance the efficient and safe use of technology. President Obama's own affinity for technology is widely known, and he campaigned on a promise of making cybersecurity a priority within his administration. To that end, within days of taking office, the Administration issued its 'Technology' agenda, along with other issue-oriented objectives. The agenda emphasizes the importance of technology in advancing competitiveness and contributing to fundamental problems like energy efficiency, controlling healthcare costs, and maintaining public safety. At the same time, the Administration issued its Homeland Security agenda, which includes a series of policy objectives to protect US information networks.

Together, the Technology and Homeland Security agendas set out the Administration's vision for prioritizing the protection of personal data, including the networks and systems on which such data resides. The Administration has pledged to '[s]trengthen privacy protection for the digital age and harness the power of technology to hold government and businesses accountable for violations of personal privacy'. More concrete than this rhetorical pledge to protect privacy, the President appointed Melissa Hathaway, a former Bush administration official, as a Senior Director to the National Security Council, to review the government's cybersecurity efforts. There has been wide speculation that Hathaway eventually will become National Cyber Advisor reporting directly to the President with responsibility for federal agency policy and the development of a national cyber policy. The Administration also has pledged to '[i]nstitute a common standard for securing [personal] data' and 'require companies to disclose personal information data breaches'. While this pledge stops short of explicitly promising to regulate cybersecurity and the protection of personal data, the strong implication is that such regulation may be pursued.

In a December 2008 report addressing Social Security Numbers and the risk of identity theft, the US Federal Trade Commission (FTC), which has taken the lead in regulating and enforcing information security practices with to the protection of consumer information, recommended the adoption of national data security standards that 'would be implemented in rulemaking by federal agencies that oversee entities that routinely use and transfer sensitive consumer information'. The FTC also encouraged Congress to adopt legislation that would establish a national data breach notification standard. Earlier the same month, the US think tank - the Center for Strategic and International Studies (CSIS) - released a prominent report containing cybersecurity recommendations for the President. The report - which was authored by two members of the House of Representatives, a leading technology industry security officer, and a retired US Air Force General - specifically advocated for a national cybersecurity czar and greater federal regulation.

Part of the impetus for the focus on greater federal leadership and oversight in the protection of personal data and the network systems stems from the fact that at the federal level, there is no single law requiring the protection of information systems or personal data. Rather, there are selected sector-specific privacy and data security laws, such as laws governing health information and financial institutions. In the absence of any broader law, the FTC, relying on its authority to regulate unfair and deceptive trade practices, has sought to regulate information security through a series of enforcement actions

against companies that have suffered large security breaches or whose information security practices were inconsistent with statements in privacy policies provided to consumers. Nearly a dozen states have also adopted specific information security laws (including quite detailed regulations in Massachusetts), and 44 States have enacted laws requiring notice to state residents in the event of a breach affecting personal information. In addition, various industry groups have drafted self-regulatory principles - the Payment Card Industry Data Security Standard (governing cardholder data) - that may have the force of law when they are applied by contract between parties.

The question, then, is whether the Obama Administration can realistically pursue a federal mandate in the cybersecurity and data protection area. There are at least four obstacles.

First, there is no consensus on exactly what such a law should look like. Industry and consumer protection groups differ on significant issues such as whether the law should prescribe - or at least suggest - the use of certain technologies, such as encryption technologies. There also are broad differences among key stakeholders over the appropriate scope of any obligation to notify consumers in the event of a security breach (i.e., the appropriate standard to trigger such a notice obligation), and which federal agency should enforce such information security standards and/or a breach notice obligation.

Second, there is no clear leader among federal agencies in the area of cybersecurity and the protection of personal information. The FTC has staked its ground to the protection of consumer interests. The Department of Homeland Security (DHS) is responsible for protecting the nation's infrastructure and, in that vein, has sought out its own leadership position on cybersecurity issues. (In one of her first actions on the job, Secretary Janet Napolitano issued a directive to her staff asking for information about DHS's authority and responsibility to protect government and private sector domains. DHS may well cede ground in the cybersecurity area if a White House office of cybersecurity is eventually created.) Within the Department of Commerce, the National Institute of Standards and Technology last month issued recommendations, directed primarily at government agencies, for effectively safeguarding personally identifiable information. Other federal agencies also have a stake, based on the industries that they oversee.

The Administration has pledged to '[s]trengthen privacy protection for the digital age'

Against this backdrop, the FTC and the CSIS reports issued in December each advocated developing federal standards that can be distilled through sector-specific federal agencies. This is a sensible approach, but it glosses over the challenge of coordinating an inter-agency process to develop the standards in the first instance.

Third, there are similar complexities in Congress. Each of the last two Congresses introduced multiple pieces of legislation that would have established a federal data security regime, and similar legislation already has been introduced in the Congress that seated last month. The Senate Judiciary, Commerce, and Banking committees and the House Energy and Commerce, Financial Services, and Judiciary committees all have pursued their own versions of the legislation over the last several years, with the result being that the legislation has never received a full vote in either chamber and, instead, has died amidst committee jurisdictional differences. While there have been recent signs that the Energy and Commerce committee could ascend to a leading position on data security issues in the House, the jurisdictional picture remains murky and there has been no clear indication from Congressional leadership that the jurisdictional differences of the past will be conclusively remedied this year.

Fourth, and most important, there are many other, more pressing policy priorities for the Obama Administration and Congress. While this is likely to be an active legislative year, it is difficult to envision federal data security legislation and regulation receiving much attention in the short term.

This is not to discount the prospects of federal legislation and/or regulation in the data protection space over the next year. President Obama has a clear public mandate behind his agenda, and the convergence of a majority-elected Presidency and a same-party Congress provides this Administration with advantages not held by any other in decades. There also is the possibility that if additional States begin to press for increasingly specific or technical data protection statutes like Massachusetts, industry may become more vocal in its support for national standards. But, at this point, there remain more reasons for skepticism with respect to anticipating any significant near-term changes in the US data protection regime.

David Fagan Associate
Lisa Bress Associate
Covington & Burling LLP, Washington
dfagan@cov.com
lbress@cov.com

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.
ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.
A twelve month subscription is £420 (overseas £440) for twelve issues and includes single user access to our online database.

e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.
Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.
A twelve month subscription is £420 (overseas £440) for six issues and includes single user access to our online database.

data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.
DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently.
Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.
A twelve month subscription is £390 (public sector £285, overseas £410) for twelve issues and includes single user access to our online database.

world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.
Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.
Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.
A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.
Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction,domain names,ticketing and privacy are subjects that have featured in WSLR recently.
Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.
A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

priority order form

FAX +44 (0)20 7729 6093
CALL +44 (0)20 7012 1380
EMAIL dan.towse@e-comlaw.com
ONLINE www.e-comlaw.com
POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND

☐ Please enrol me as a subscriber to **e-commerce law & policy** at £420 (overseas £440)
☐ Please enrol me as a subscriber to **e-commerce law reports** at £320 (overseas £440)
☐ Please enrol me as a subscriber to **data protection law & policy** at £390 (public sector £285, overseas £410)
☐ Please enrol me as a subscriber to **world online gambling law report** at £520 (overseas £540)
☐ Please enrol me as a subscriber to **world sports law report** at £520 (overseas £540)

All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.

Name			
Job Title			
Department		Company	
Address			
Address			
City		State	
Country		Postcode	
Telephone		Fax	
Email			

1
Please **invoice me** Purchase order number
Signature Date

2
I enclose a **cheque** for the amount of
made payable to *'Cecile Park Publishing Limited'*

3
Please debit my **credit card** VISA ☐ MASTERCARD ☐
Card No. Expiry Date
Signature Date
VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information.
Please tick here if you would like to hear from other companies about products or services that may add value to your subscription. ☐