Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

INTERNATIONAL EDITION

APRIL 2016

IN THIS ISSUE

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:

Natasha Ahmed
Associate
London
+44 (0) 20 7861 9048
nahmed@lockelord.com

Jeffrey Kung
Counsel
Hong Kong
+852 3465 0680
jkung@lockelord.com

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Karen L. Booth
Associate
Hartford
860-541-7714
karen.booth@lockelord.com

Alan D. Meneghetti
Partner
London
+44 (0) 20 7861 9024
ameneghetti@lockelord.com

Bart W. Huffman
Partner
Austin
512-305-4746
bhuffman@lockelord.com

Charles M. Salmon
Associate
Austin
512-305-4722
csalmon@lockelord.com

John F. Kloecker
Of Counsel
Chicago
312-443-0235
jkloecker@lockelord.com

Philippa Townley
Associate
London
+44 (0) 20 7861 9041
ptownley@lockelord.com

The Panama Papers and Implications for Cyber Security in Law Firms

What seems like a long time ago now, in 2011 PricewaterhouseCoopers (PwC) warned that "there is no question that law firms are among the companies being targeted by cyber criminals." Despite this, many law firms believed (or just did not feel the risk significant enough) that they were unlikely to be the target of a cyber-attack. In the same 2011 report, PwC reported that "a number of law firms believe they were too small or obscure to warrant the interest of professional hackers," and Legal Week have also reported that law firms are far less likely (to the order of 35%) to have a response plan in place for cyber-attacks than non-legal professionals (a slightly better 52%).

The issue of cyber-security at law firms has been brought to the fore in recent weeks due to two significant data breach incidents which have targeted the legal sector.

In March 2016 New York security firm Flashpoint issued a statement to 48 prestigious law firms warning them that they had been targeted by a Russian cyber-criminal (known as "Oleras"). New York firm Cravath Swaine & Moore (which also has an office in London) confirmed that its systems had been breached the previous summer.

Just a few weeks later news emerged of a major document leak from the off-shore Panamanian-based law firm Mossack Fonseca. This is the biggest document leak in history – bigger than the 2010 Wikileaks and the 2013 Edward Snowden disclosures combined. More than 11.5 million documents – or 2.6 terabytes of data – were leaked to German newspaper Süddeutsche Zeitung, which went on to share the leaked information with the International Consortium of Investigative Journalists. The fallout from the leak is significant and continues to bring headline news on a near-daily basis: so far, Iceland's prime minister Sigmundur Gunnlaugsson resigned after his family was accused of concealing millions of dollars in an offshore account; Uruguayan lawyer Juan Pedro Damiani resigned from his role as an ethics judge at FIFA, and FIFA president Gianni Infantino has been accused of signing off a contract entered into by two businessmen who have been accused of paying millions of dollars in bribes to South American football officials; on Tuesday 5th April and Wednesday 6th April, David Cameron and Downing Street confirmed that the prime minister does not benefit from any offshore funds, and on Thursday 7th April the prime minister revealed that he had owned shares in Blairmore Holdings, an offshore fund set up by his father. The UK Prime Minister, as well as various other ministers in the UK, have now made public their tax returns. And the repercussions continue on a daily basis.

Founding partner of Mossack Fonseca, Ramon Fonseca, has been quoted as saying of the Panama Papers leak that "This is not a leak. This is a hack."

Whether a leak or a hack, these recent stories raise concerns about the ability of law firms to protect themselves and their clients' data from data breaches.

In April 2015, the UK Law Gazette reported that in 2014 the Information Commissioner's Office (the ICO, which is the UK's national data protection authority) investigated 173 law firms for potential breaches of the UK Data Protection Act 1998. The ICO has noted that data breaches reported by solicitors and barristers increased by 32% from 2013/2014 to 2014/2015, and accounted for 4.5% of all reported breaches. In its 2015 Annual Law Firms' Survey, PwC reported that 62% of the law firms reviewed had reported being the victim of cyber-attack(s), which represents an increase of nearly 20% from 2014 (45% of law firms reviewed had reported a cyber-attack(s) in 2014).

Why are law firms being targeted by cyber-attackers?

Cyber-attackers attack companies, including law firms, to obtain information for a variety of reasons, including economic (or industrial) espionage, insider trading, holding the victim to ransom, making fraudulent purchases and of course for ideological causes. In the case of the Oleras hack, reports have stated that the hackers were seeking insider information in relation to confidential, undisclosed mergers and acquisitions in order to use this information for insider trading. In 2012, an Anonymous offshoot, "AntiSec," hacked a Washington law firm claiming to have done so in order to expose "rich and powerful oppressors." So why go for law firms? The Law Society of England and Wales believes it is because "law firms are particularly attractive sources of information." Law firms are often considered to be "soft targets," providing easier access to confidential information about businesses than those businesses themselves due to the fact that, for the most part, they have relatively lax security systems in place.

What can law firms do to protect themselves against data breaches?

The ICO, the Law Society of England and Wales, and the English Solicitors Regulation Authority (the SRA) all recognize the increased threat of cyber-attacks to law firms and have each published guidance setting out practical steps that can be taken to improve security. The Law Society has set up a page dedicated to providing advice to lawyers and law firms on how to avoid cyber-attacks, and the SRA has published a document dedicated to highlighting cybercrime risks to law firms and also its latest Risk Outlook report, both of which provide practical advice for legal practitioners.

The ICO has also published some "top tips" to help lawyers keep the data they handle secure:

- Keep paper records secure. Do not leave files in your car overnight and do lock information away when it is not in use.
- Consider data minimisation techniques in order to ensure that you are only carrying information that is essential to the task in hand.
- Where possible, store personal information on an encrypted memory stick or portable device. If the information is properly encrypted it will be virtually impossible to access it, even if the device is lost or stolen.
- When sending personal information by email consider whether the information needs to be encrypted or password protected. Avoid the pitfalls of auto-complete by double checking to make sure the email address you are sending the information to is correct.
- Only keep information for as long as is necessary. You must delete or dispose of information securely if you no longer need it.
- If you are disposing of an old computer, or other device, make sure all of the information held on the device is permanently deleted before disposal.

For UK firms, a cyber-attack could reveal a breach of a law firm's obligations to the SRA as well as under the Data Protection Act 1998, and is likely to result in damage to a firm's reputation and its client relationships (both past, current and potential), loss of business, and a huge investment in time and resource to remedy the breach. In light of this and recent events, it is time for firms which have not already done so to assess their data breach risks and put in place appropriate security measures as a business priority.

Two Significant Privacy and Data Protection Developments for the Insurance Industry

Recent action by the National Association of Insurance Commissioners (NAIC) could eliminate the requirement to issue redundant annual privacy notices under certain circumstances, while imposing new and onerous data security and breach notification obligations, as further described below.

Efforts to Streamline GLBA Privacy Notices

As we reported here, the federal Gramm-Leach-Bliley Act (the GLBA) was amended effective December 4, 2015, eliminating the requirement for annual GLBA privacy notices under certain circumstances. The GLBA, however, does not preempt state laws that provide greater protection of consumer privacy rights. Therefore, the GLBA amendments presumably did not override state insurance law requirements for annual privacy notices, which had been promulgated to comply with the requirements of the GLBA as originally enacted, and are now more protective than the amended GLBA requirements.

At the NAIC spring meeting on April 4th, the NAIC Privacy Disclosure (D) Working Group approved a draft bulletin available here, and considered amendments to the Model Privacy of Consumer Financial and Health Information Regulation available here, which would implement the GLBA amendments. Both the draft bulletin and proposed amendments to the model regulation are pending approval by the NAIC and action on the state level. It will be up to individual states to adopt an amended privacy regulation and/or to issue a bulletin following the NAIC's proposal to allow eligible insurers the relief provided under the GLBA amendments.

Issuance of Preliminary Draft Insurance Data Security Model Law

The NAIC Cybersecurity (EX) Task Force recently released a preliminary working and discussion draft of an Insurance Data Security Model Law available here (the Draft Model Law). While praiseworthy in its effort to provide uniformity for data security and breach notification requirements among the states, at least with respect to the insurance industry, the Draft Model Law clearly needs further development, input and revision, or it may do more harm than good.

The Draft Model Law has received significant industry criticism, including at a Task Force meeting held April 4, 2016, and via a letter submitted by about a dozen trade associations. Criticism of the Draft Model Law includes concern with the fact that the draft would authorize regulations that could vary from state to state, thereby undermining uniformity, and would create a private cause of action. With respect to breach notification, the Draft Model Law includes an onerous five calendar day requirement for notification to the commissioner (which would mean the commissioner of each jurisdiction), and further authorizes each commissioner to review and comment on the draft consumer notification letter prior to issuance and prescribe the level and duration of consumer protection required. At a minimum, the Draft Model Law would require that the breached entity offer and pay for at least 12 months of identity theft protection for affected consumers.

Fourth Circuit Affirms CGL Duty to Defend for Medical Records Breach

The Fourth Circuit Court of Appeals has affirmed a Virginia federal district court's summary judgment ruling for the insured under a commercial general liability (CGL) policy, finding that the insurer had a duty to defend a third-party lawsuit alleging failure to properly secure electronic storage of medical records. *Travelers Indemnity Co. v. Portal Healthcare Solutions, LLC*, No. 14-1944 (4th Cir. Apr. 11, 2016). A copy of the appellate court's unpublished opinion is available here.

Glen Falls Hospital contracted with the insured, Porter Healthcare Solutions, LLC, for the electronic storage and maintenance of the hospital's confidential medical records. Two patients discovered that when they searched for their names in an online engine, the first result was a direct link to their Glen Falls medical records. The patients brought a class action lawsuit alleging that Portal failed to safeguard their confidential medical records. Portal sought coverage under two Travelers CGL policies. The policies cover "electronic publication of material" that, depending on the policy year, either "gives unreasonable publicity to" or "discloses information about a person's private life." Travelers brought an action in the Eastern District of Virginia seeking a declaration that it is not required to defend Portal in the class action lawsuit, on grounds that the underlying suit did not allege a covered publication under the policies. *See Travelers Indem. Co. of America v. Portal Healthcare Solutions, LLC*, 35 F. Supp. 3d 765, 767-68 (E.D. Va. 2014).

On the parties' cross-motions for summary judgment, the district court granted Portal's motion, holding that "exposing material to the online searching of a patient's name does constitute a 'publication' of electronic material" for purposes of the Travelers policies. *Id.* at 770. Addressing Travelers' argument that no third party was alleged to have viewed the records, the district court said that the definition of "publication" did not hinge on third-party access – but rather occurs when the information is "placed before the public." *Id.* at 770-71. The court proceeded to find that in addition to publication, the public availability of records also satisfied the second requisite for coverage, *i.e.*, that the public availability of records was "unreasonable publicity" and disclosed information about the patient's private life. *Id.* at 771-72. The district court therefore found that Travelers had a duty to defend under the policies (the court did not address whether the policies would cover any potential judgment or settlement against Portal).

The Fourth Circuit affirmed, commending the district court for its "sound legal analysis." The appellate court adopted the district court's reasoning that the third-party lawsuit alleged conduct which, "if proven, would have given 'unreasonable publicity to, and disclosed[d] information about, patients' private lives,' because any member of the public with an Internet connection could have viewed the plaintiffs' private medical records during the time the records were available online" (Slip Op. at 7).

The Fourth Circuit's ruling starkly illustrates that the issue of coverage for data breach lawsuits under CGL and other traditional policies is by no means settled. The decision joins a collection of varying results on this issue that depend heavily on the particular facts of each case, the policy language and jurisdiction.

Global Sweep Exercise to Examine the Privacy Transparency of IoT Devices

Consumers are increasingly using connected devices and smart technology that store information that can be connected to a person. This raises a number of issues, including privacy, security, software licensing and compliance with data protection legislation.

On April 11, 2016 the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) joined a global Privacy Sweep (sweep) exercise to examine privacy transparency relating to the Internet of Things (IoT) devices such as smart electricity meters, Internet-connected thermostats and wearables. Just as IoT brings new business opportunities, it raises new legal issues as devices compile an unprecedented volume and variety of personal data.

The PCPD is one of 29 of the Global Privacy Enforcement Network (GPEN) "privacy enforcement authorities" members who selected a type of device most appropriate for their jurisdiction. Hong Kong chose to examine how fitness bands produced in Hong Kong collect and use personal data, and how the device users are kept informed of privacy-related matters.

The GPEN has grown from 13 privacy enforcement authorities in 2010 to 59 authorities across 43 jurisdictions in 2015, with plans to further expand across Africa, Asia and South America.

Mr. Stephen Kai-yi Wong, Privacy Commissioner for Personal Data, Hong Kong said that "Many IoT devices increasingly include functions such as tracking fitness and health, which means more personal data elements are being collected and shared across apps and other devices without the knowledge or consent of the consumers. It is important for companies engaged in these activities to make known to the consumers their personal data policies and practices, types of personal data they hold and how the data is used."

The sweep exercise is expected to provide findings on the challenges and impact of privacy and data protection on IoT devices in general, and more specifically on fitness bands, the results of which will be made public in the third quarter 2016.

Concerns identified during the sweep may result in follow-up work to broaden awareness of data privacy rights and responsibilities, such as public education and promotion, outreach to organizations and/or enforcement actions.

Going for Broke(r) – Broker Named in Cyber Coverage Litigation

A subplot is brewing in the policy limits dispute between a data breach victim and its cyber insurer – is a specialty broker that worked with the independent agent in placing the policy liable for claims against the agent? In *New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's*, No. 2:16-cv-00061 (E.D. La.), the insured hotel filed a claim for $3 million in losses arising from a 2013 cyberattack. The insurer denied coverage as to losses in excess of $200,000, asserting that the limit in an endorsement for "payment card industry fines" applied to all claims arising from the cyberattack. (*See* Testing the Limits - Cyber Coverage Litigation (Feb. 23, 2016).)

In the original complaint, the insured sued the both the insurer and the independent agent that procured the policy. The complaint alleges that full policy limits of $3 million should be available to cover the insured's losses. As to the agent (Eustis Insurance, Inc.), the complaint alleges that the agent is liable for breach of contract and negligent failure to procure coverage. According to the insured, if the insurer's interpretation of the endorsement is found to be correct, then the agent "did not use reasonable diligence to place the insurance requested, as the insurance is limited to only $200,000 in coverage for fraud recovery, operational reimbursement, and case management fees resulting from a cyberattack, whereas the full policy limit is $3 million."

On March 28, 2016, the agent filed a third-party complaint against the broker, R-T Specialty, LLC, which the agent contends it relied on in procuring the policy. The agent alleges that it "had no experience in procuring cyber insurance policies," and "relied on the expertise of R-T Specialty to procure the cyber coverage requested by Hotel Monteleone." The third-party complaint asserts that in the event damages are awarded against the agent, then R-T Specialty is wholly liable for those damages.

Although the case is in the early stages and the allegations are unproven, *Hotel Monteleone* is a reminder that the parties in a cyber coverage lawsuit can include not only the insured and insurer, but also a broad range of brokers and other advisors. The evolving case law, variation in policy language, increasingly costly breaches and shifting landscape of regulatory and PCI fines will continue to raise the stakes in cyber-related coverage litigation and provide incentives to seek compensation from the widest possible scope of parties.

ICO Issues Highest Fine for "Staggering" 46 Million Nuisance Calls

The UK data protection regulator, the ICO, has issued its largest ever fine on the company behind 46 million automated nuisance calls. Prodial Ltd, a lead generation firm, has been fined £350,000. The maximum fine which the ICO is entitled to levy under the UK's Data Protection Act 1998 is £500,000.

The automated calls played recorded messages relating to payment protection insurance (PPI) claims. Over 1,000 people have complained to the ICO about these repeated calls at all times of the day and night that often failed to provide an opt-out option.

The ICO has reported that Prodial Ltd was operating out of a residential property in Brighton and hiding its identity, making it hard for people to report these calls. Moreover, an investigation has found that Prodial never obtained the required consent to contact people through the means of Internet phone lines – which allows companies to make enormous numbers of recorded marking calls cheaply. It is illegal to contact people in this way without specific consent.

Information Commissioner Christopher Graham has delivered the following very clear message in response to Prodial's illegal invasion of people's privacy:

> This is one of the worst cases of cold calling we have ever come across. The volume of calls made in just a few months was staggering.
>
> This was a company that knew it was breaking the law. A company director admitted that once the ICO became involved, the company shut down. That stopped the calls, but we want to send a clear message to other firms that this type of law-breaking will not pay. That is why we have handed out our highest ever fine.
>
> No matter what companies do to try to avoid the law, we will find a way to act.

ISO Data Call Reflects Ongoing Efforts to Shape Cyber Underwriting Standards

Efforts continue to gather data and standards on which to base cyber underwriting decisions. On March 11, 2016, the Insurance Services Office, Inc. (ISO) issued a voluntary cyber insurance data call to collect detailed premium and loss information from insurers.

The ISO data call joins other recent initiatives to create common standards to evaluate cyber risks. For example, the National Association of Insurance Commissioners recently required insurers writing theft or cybersecurity insurance to report claims, premiums and other details. The Department of Homeland Security has a Cyber Incident Data and Analysis Working Group which seeks to gather pertinent information. And in January 2016, Risk Management Solutions, Inc. (RMS) and AIR Worldwide (a unit of Verisk Analytics, as is ISO), with support from a number of insurers and reinsurers, released common data elements and practices for maintaining cyber risk data (*see* A Common Standard for Evaluating Cyber Risk (Feb. 23, 2016).)

The ISO call is intended to address three "areas of concern" in the cyber insurance market: lack of aggregated data for pricing, silos of data across different industry sectors and rate filings based on actuarial judgment. The data call contains 268 fields relating to a wide scope of information including policy types, SICs, deductibles, limits, losses and defense costs and other coverage and loss characteristics.

What remains to be seen is whether the nature of cyber risks – rapidly evolving, difficult to quantify and potential exposure to exponentially scalable damages – lends itself to the same data collection techniques that the industry has used for decades to evaluate other risks. It is also an open question whether limits on the number of personnel with the requisite expertise to meaningfully evaluate cyber risks – currently commanding premium compensation in private sector technical fields – will restrict the capabilities of rating agencies and other data aggregators to stay within striking distance of the next major cyber peril.

Revised Uniform Fiduciary Access to Digital Assets Act Provides Important Procedures for Dealing with Digital Assets Following a Death

In addition to posing significant emotional and life challenges, a death almost always gives rise to a number of practical and legal tasks to be attended to by family and friends of the deceased. Traditional assets and obligations are typically dealt with through the long-developed areas of law of trusts and estates. Legal means to appropriately handle digital assets of a decedent are, of course, not fully developed. Yet digital assets are of ever-increasing importance as most of an individual's records are stored – not in a closet or safe – but within password-protected online or electronic accounts. Important questions arise as to how those accounts should be handled after death, including who should have access to and who may exercise control over those accounts. Even access to information associated with "traditional" accounts increasingly requires access to at least a decedent's email account.

The National Conference of Commissioners on Uniform State Laws has attempted to address the issues in the form of a uniform law, recently revised as the Revised Uniform Fiduciary Access to Digital Access Act (Revised UFADAA; a comparison chart reflecting differences between the Revised UFADAA and the original is available here). The Revised UFADAA provides an authorization framework for legal fiduciaries and data custodians (a provider that actually maintains or stores digital assets of a decedent pursuant to an agreement) to address the needs of fiduciaries to access online accounts, gather assets, and protect the wishes of the deceased and the interests of the deceased's beneficiaries. This framework is centered on consents and directions provided by a decedent during life. Consistent with the federal Stored Communications Act, the Revised UFADAA imposes heightened requirements for disclosure of or provision of access to the contents of electronic communications.

The Revised UFADAA sets forth various procedures and protections for custodians, including methods for seeking to limit required disclosures, immunity for good faith compliance and provision for recovery of reasonable administrative costs.

The law has been enacted or introduced in the state legislatures of 28 different states as of the time of this writing. Individuals managing the estate of someone close to them, or seeking to simplify matters for their own beneficiaries, may wish to determine the status of UFADAA in their home state and take appropriate measures to clarify their wishes regarding the post-death treatment of digital assets.

GDPR Legislative Process is Complete: EU Parliament Gave Final Approval on 14 April 2016

The EU Council and the European Parliament have officially adopted their final position on the General Data Protection Regulation (GDPR) after more than four years of negotiations. The regulation, which was approved and passed by the European Parliament on 14 April, updates and modernises the principles of the 1995 Data Protection Directive (95/46/EC), aiming to give European citizens control of their personal data and create a high, uniform level of data protection across the EU that is fit for the digital age. The GDPR will enter into force 20 days after it is published in the Official Journal of the European Union and will be directly applicable in the same way across all the Member States of the EU 2 years thereafter (in other words, in about May/June 2018).

A compromise was agreed with the European Parliament on 15 December 2015. On 8 April 2016, the Council adopted its position at first reading, which paved the way for the European Parliament's vote in second reading at its plenary session and adoption on 14 April 2016. This has finally completed the legislative process for the GDPR.

The new rules include provisions on:

- a right to be forgotten (which confirms the position adopted by the Court of Justice in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*);
- "clear and affirmative consent" and "explicit" to the processing of private data by the person concerned;
- a right to transfer your personal data to another service provider;
- the right to know when your personal data has been hacked or a breach has occurred in relation to your personal data;
- ensuring that privacy policies are explained in clear and understandable language; and
- stronger enforcement and fines up to the greater of 4% (or euro 20 million) of a firm's total worldwide annual turnover, as a deterrent to breaking the rules.

Jan Philipp Albrecht (Greens, DE), who steered the legislation through Parliament, has given the following statement on the final adoption: "The general data protection regulation makes a high, uniform level of data protection throughout the EU a reality. This is a great success for the European Parliament and a fierce European 'yes' to strong consumer rights and competition in the digital age. Citizens will be able to decide for themselves which personal information they want to share."

Albrecht added: "The regulation will also create clarity for businesses by establishing a single law across the EU. The new law creates confidence, legal certainty and fairer competition."

Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Chicago | Dallas | Hartford | Hong Kong | Houston | Istanbul | London | Los Angeles | Miami | Morristown
New Orleans | New York | Providence | Sacramento | San Francisco | Stamford | Tokyo | Washington DC | West Palm Beach