Analysis of PRISM and other surveillance programs – Part Two

In recent months the media has been revealing more about previously clandestine data gathering and surveillance methods used by the National Security Agency (NSA) in its efforts to combat terrorism. The new information has led welcome debate over the proper scope of the NSA's authority and oversight, and calls for reform. Despite an unprecedented public defense by the NSA itself, as well as President Obama and the Department of Justice, the revelations have raised a host of questions, confusion and conflicting assertions about what the NSA is doing. Part One of this article explored the legal underpinnings of the NSA programs and discussed the proposals for reform of the NSA's legal authority now pending before Congress. In Part Two of this article, Alex Lakatos and Matt Bisanz, Partner and Associate at Mayer Brown LLP respectively, address why the NSA's overreaching authority is of dubious effectiveness when it comes to keeping America safe, but may be a real threat to USA businesses.

Preventing terrorism

Questionable effectiveness

It is questionable whether PRISM or the phone records program ever stopped any terrorist plots. USA officials have cited only two cases as having been discovered exclusively by searching those records; one involving some San Diego men who sent $8,500 to Al Qaeda-linked militants in Somalia and another involving identification of communications that tied a person in Colorado with plans to bomb the New York City subway system. But critics say credit for Colorado case should go to British Intelligence, not the NSA. The Obama Administration meanwhile defends what appears to be a flimsy record with generalities - calling NSA programs 'critical tools in protecting the nation from terrorist threats.'

But Senators Mark Udall and Ron Wyden, who both serve on the USA Senate Select Committee on Intelligence, have released a joint statement 'refuting claims that phone record collection by the intelligence community has thwarted attacks against the United States', stating: 'In our capacity as members of the Senate Select Committee on Intelligence, we have spent years examining the intelligence collection operations that have been secretly authorized under the USA Patriot Act. Based on this experience, we respectfully but firmly disagree with the way that this program has been described by senior administration officials. After years of review, we believe statements that this very broad Patriot Act collection has been *a critical tool in protecting the nation* do not appear to hold up under close scrutiny. We remain unconvinced that the secret Patriot Act collection has actually provided any uniquely valuable intelligence. As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.'

Their analysis is in line with the statement of J. M. Berger, an author and terrorist analyst: "[A] lot of people have wishes or hopes of turning the whole internet into a smart computer that can figure out where the terrorists are. Maybe that's possible someday - I don't know. You can't just plug something into the internet and have a list of names come out and start monitoring everybody on that list. You need a good deal of complicated curation. But when you can do that, it can be a very powerful and effective tool."

Part of the problem is that sophisticated terrorists who pose the greatest threat typically steer clear of electronic communications. Osama Bin Laden and deceased al Qaeda Iraqi leader Abu Musab al Zarqawi, for example, used a complex network of couriers instead of risking exposure to the intelligence agencies' omnipresent electronic tracking programs.

Poor use of resources

Beyond the lack of a track record, PRISM and the phone records program may actually be counterproductive, because their fire hose of output may distract law enforcement from better leads. Congressman Rush Holt said: "[T]he idea of the Fourth Amendment [which protects against warrantless searches and seizures] is not to get in the way of law enforcement and intelligence, but rather to see that they do a good job by having to prove at each step of the way that they know what they're doing, that they're not off running down hunches and going off on wild goose chases and witch hunts."

Even collecting very basic data on every phone call or email can result in databases that are so large that it becomes increasingly difficult to sort and review the information in a meaningful way. As an analogy, if you know there is a needle in the haystack, you can find it very easily using a magnet, but if you do not know whether you are looking for a string, needle, or stick, you will never be able to sort every straw of hay to find what you need. The Administration claims that such

large sets of data are needed to properly understand how individual pieces relate to each other, but in 2011, according to Snowden's disclosures, the intelligence agencies quietly discontinued a then-secret program that collected email metadata on Americans - 'to' and 'from' information, not content - because it was not yielding much value.

Harm to foreign relations

The NSA's overreaching programs alienate friends and allies that USA relies upon for help in the war on terror. Even America's staunchest allies are uneasy, at best, about the NSA's intelligence programs.

German Chancellor Angela Merkel grew up in the East German police state and expressed diplomatic 'surprise' at the NSA's activities. She knows how the Stasi collected thousands of jars of fabric from citizens, just in case one of them later double-crossed the state and their scent was needed for detection dogs. She vowed to raise the issue of the NSA's expensive surveillance programmes with President Obama at the G8 meetings. The Italian Data Protection Commissioner added to the debate by saying that the NSA's programs would 'not be legal' in his country. British Foreign Minister William Hague faced heated challenge in Parliament for his Government's participation in the NSA programs, notwithstanding that the UK intelligence service accepts partial funding from the NSA. Prime Minister David Cameron faced unprecedented defeat in Parliament when he asked the UK to join with the USA in relying on USA-collected intelligence, as the basis for military intervention in Syria.

All of this backlash may cost the USA help from allies that is critical to its efforts to protect against terrorism. A Congressional Research Service Report titled 'US-EU Cooperation Against Terrorism' published on 4 September 2013, explains "some challenges persist in fostering closer US-EU cooperation [in the fight against terror… Notably] EU worries about US data protection safeguards and practices [are an obstacle that has] been further heightened by the public revelations in June 2013 of US National Security Agency surveillance programs."

With ever increasing concern about the NSA conduct, and rising protests against the NSA activities in Europe, arguments that storing data in the EU may not do the trick may be too little, too late

Harm to USA economic interests

There is yet another problem with the NSA's controversial programs, one that often is overlooked amidst heated debate that, justifiably, focuses on civil liberties and homeland security. Namely, that NSA overreaching (or even the perception of overreaching) can put USA technology companies at a competitive disadvantage. This risk is particularly acute for USA cloud service providers (CSP) and those that rely upon USA CSPs. Anecdotal evidence suggests that USA CSPs (or even vendors that use USA CSPs) may be losing business to their non-USA competitors, who are seen as keeping data farther from the USA government's prying eyes. For example, a Cloud Security Alliance Survey on Government Access to Information published in July 2013 reported that 56% of non-USA responders were less likely to use cloud services in light of the Snowden's revelations, and 10% claimed to have cancelled projects that would have used USA cloud servers, and about a third of USA responders said that the Snowden incident makes it harder for them to conduct business outside the USA.

According to Reuters, sources including technology executives in Europe hope that 'the scandal may prove a turning point for the region's young cloud computing industry.' Reuters further reports that European companies such as telecoms groups Orange and Deutsche Telekom are trying to exploit the concerns as they build their own cloud businesses.

Caspar Bowden, an independent privacy advocate and Microsoft's Chief Privacy Adviser from 2002-2011, said that before the Snowden leak, the big USA cloud companies had been largely able to quell fears about data security with savvy public relations, but "the headlines [about PRISM] will change all that. The nationality of the company and the location of the data do make a difference."

John Engates, RackSpace Chief Technology Officer, said: "Are people concerned about doing business in the USA and what the USA could do with their data? The answer is yes. It's something as a country we need to figure out, how to allay some of the fears about data moving through the USA. That's partly why people are gravitating toward the idea of private clouds that you can run in other countries."

These concerns, however, should be understood in context. The USA is still the largest and most dominant player in the provision of cloud services, with many of formative companies based in, and most sophisticated services originating from, the USA. And significant new business from customers new and old, including customers from Europe and Asia, continue to roll into the USA market.

Solutions for USA industry

Still, the NSA is making life harder for USA CSPs. What should they do?

First, USA companies should

explain that the perception of keeping data in the EU will keep it safe from prying eyes does not always comport with reality. Through programs like PRISM and Upstream, the USA Government is able to obtain data that relates to international communications, either by receiving the data from the participating companies or (perhaps) even directly from tapping of international telecommunications cables. There are recent allegations that the NSA hacked the Brazilian state-run oil company Petrobras and intercepted billions of emails and calls to Brazilians. And, moving data to the EU certainly does not shield it from EU authorities, who - to less fanfare and perhaps less extensively - do snooping of their own, sometimes even at the behest of their USA counterparts. These arguments, however, are likely to be unheard over the chorus of outrage at the USA government's past actions. With ever increasing concern about the NSA's conduct, and rising protests against NSA activities in the EU, arguments that storing data in the EU may not do the trick may be too little, too late.

Second, USA companies can market more technologically secure solutions. Tien Tzuo, founder of Zuora, which sets up payments and billing for cloud software service providers, concludes that "[t]here's a sense that there needs to be a new breed of technologies to give a little bit more control of their private information back to consumers. And I think we're going to see a lot of innovation in that area over the next few years." Many cloud providers, such as Amazon Web Services (AWS), the cloud services arm of Amazon.com, provide tools for its customers to encrypt data they store. And Apple has segregated users' fingerprint data in its latest iPhone 5S release to keep it off of Apple's own cloud offering. Other companies may choose to outsource some data, while keeping the most sensitive materials (such as human resources, trade secrets) in house. None of these current solutions are foolproof; encryption may interfere with smooth business operations or be cracked with NSA decryption tools, Apple's segregation may be overcome via remote access, and even in-house solutions are still at risk to disloyal employees. But, they are at least attempts at innovation.

Third, this economic concern may persuade some in Congress who are not swayed by civil liberties arguments to make more serious reforms to limit what the NSA can do. It is a well-known reality of American politics that money talks and few have as much money to lose as the industries that make, run, and use cloud computing technology. USA technology businesses who are not already doing so (many are) should make sure their voices are heard on this issue, so that Congress and the Obama Administration appreciate fully the impact of failure to achieve meaningful reform and genuinely change perceptions at home and abroad.

Alex Lakatos
Partner
Mayer Brown LLP
alakatos@mayerbrown.com

Matt Bisanz
Associate
Mayer Brown LLP
mbisanz@mayerbrown.com

The authors would like to thank Jeffery Taft, Partner at Mayer Brown LLP, for his assistance with this article.

Comment

A francophone BCR model to boost African data protection

The Association of French-speaking Data Protection Authorities (AFAPDP), consisting of 15 countries, recently proposed a BCR-style data transfers model between member states as part of their efforts to improve the standard of data protection in less mature regimes. Recently, Africa has seen a flurry of developments, from Morocco's approval of Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), to new privacy laws in Niger and Gabon. Floriane Leclercq, the French Data Protection Authority's (CNIL) representative at the AFAPDP, comments on the AFAPDP's mission and how African data protection law is shaping up.

French-speaking African countries have begun to establish data protection laws and authorities – this is a persistent and encouraging trend for the strengthening of individual rights and the rule of law. As of June 2013, seven French-speaking African countries have an authority tasked with the protection of personal data and bills are being drafted in six French-speaking African countries. In this area of law, French-speaking countries are ahead of the English-speaking countries. In addition to these national initiatives, regional organizations such as the Economic Community of West African States (ECOWAS) and the African Union (AU) have taken over the protection of personal data. On 16 February 2010, ECOWAS adopted a Supplementary Act on the protection of personal data for direct application in 15 countries. The AU is currently preparing a draft convention which contains a section is devoted to the protection of personal data.

The mission of the AFAPDP is to promote the adoption of laws protecting personal data and the establishment of national institutions for the protection of personal data while respecting the needs and traditions of each country. The AFAPDP offers assistance to States and local authorities to develop an expertise in the protection of personal data, based on the experience of members of its network authorities.

The AFAPDP began an internal consultation on our francophone Binding Corporate Rules in the past few months, which is still in progress. At the beginning of this project, we were pursuing two main objectives:

- better supervision – protection and facilitation – of data transfers between French-speaking countries, and
- standardisation of principles and practices between French-speaking authorities.

Our working group chose to propose one supervisory tool first: the francophone Binding Corporate Rules, inspired by the European tool of the same name, because it already works and has proven its worth. However, as this project is in connection with the international context (the data protection reforms currently under discussion in the European Union and other enforcement initiatives such as the Global Privacy Enforcement Network (GPEN) and the APEC Cross-Border Privacy Enforcement Arrangement (CPEA) and the International Enforcement Group), a few discussions and months are still necessary to reach an adequate level of awareness and expertise in the French-speaking community.

In general, there is a growing interest in African states to enact legislation to protect personal data in accordance with international standards.

- The first driving force is a political one: the right to protection of personal data is an excellent indicator of democracy. The law recognises new rights and installs a new independent authority to protect fundamental freedoms. Moreover, the state itself is subject to supervision by the data protection authority. In Tunisia, the protection of fundamental rights, including the right to protection of personal data, is in line with the context of politics and digital revolution. The law reform, proposed by the National Personal Data Protection Authority (INPDP) in June 2012, would be a way for the Tunisian Government to show its commitment to strengthening democratic accountability and public confidence and validate the principle of a digital revolution and freedom of expression.
- The second driving force is economic one: the right to protection of personal data is involved in the construction of a legally secure digital economy likely to attract foreign investment. In Morocco, the adoption of the law of protection of personal data and the establishment of an authority to protect personal data with powers of authorisation and control shows the government's commitment to strengthen the legal transparency and provide an attractive framework for digital companies creating jobs in key sectors such as international finance, remote services companies, and telecommunications.

On 6 June 2013, the Moroccan government adopted a bill approving Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Ratification would make Morocco the second non-member country of the Council of Europe to be party to the Convention. The Council of Europe, the Moroccan data protection authority (DPA) and the AFAPDP did a lot to support the ratification. The Moroccan DPA hopes that the ratification will lead to amendments of the Moroccan law - it needs to be lightly modified to reinforce the DPA's ability to enforce the law, its financial and functional independence, and ability to recruit its own staff.

Floriane Leclercq
Data Protection Project Manager at the AFAPDP

Intelligent data migration: ten techniques for best practice

With ever increasing data volumes, archives contain tremendous amounts of valuable and worthless information. Whether by changing circumstances or bad design, many legacy archives make it almost impossible to gain a true understanding of their contents. Dr Jim Kent, CEO, EMEA and Head of Investigations at Nuix, explains techniques organisations can use to speed up data migration.

Many organisations have hundreds of terabytes of data stored in legacy archive systems. Due to the technical limitations of these systems, it is often difficult to search and analyse their contents for eDiscovery, data minimisation or risk management purposes.

As a result, many organisations are looking to migrate the contents of legacy archives to newer platforms or cloud services. However, the same factors that limit our ability to understand the contents of archives also make it very difficult and time consuming to move them.

In addition, data migration is an opportunity to leave behind old, duplicated and otherwise space-filling data. However, organisations also lack a thorough and legally defensible process for assigning value to data – they simply don't know where to start.

Did archives solve problems, or create them?

Since email archives first arrived in their current form, organisations have purchased some form of disk archive. Archive vendors primarily target large companies in highly regulated sectors such as financial services, pharmaceuticals and healthcare, and large government agencies. These organisations have huge data volumes and strict compliance rules about retaining it.

Over the past decade, archives addressed these organisations' need to retain data for the required period. However, they generated a host of new problems, including:

- bloating, such as retaining data indiscriminately with no thought of its value or retention period;
- slow and unreliable searching;
- slow data extraction, where archives' built-in interfaces for extracting data were not designed for high volume – often they could only work with one file at a time;
- obsolete platforms, where many archive systems that were once common became unsupported.

The challenges of archive migration

Facing these challenges, many organisations decide the best option is to migrate the archived data to a modern platform or an outsourced or cloud service. Cloud services, for example, usually cost less than running storage hardware in-house, or simply make it someone else's problem to manage!

However, organisations often migrate all their data to a new archive or cloud service. This indiscriminate approach does not solve many of the problems with the original archive, such as the large volume of content that has no business value or contains risks. It merely defers these issues for as long as the migration takes.

Furthermore, because of the limitations of archives' extraction interfaces and the sheer scale involved, many migration vendors still claim it is impossible to transfer large volumes of data in less than a year.

Ten techniques

A faster, more efficient approach would be to migrate only the email messages that have business value or that the organisation must retain for compliance. This requires advanced migration technologies that can directly access the data in the source archive, bypassing the built-in interface, and create a complete and in-depth index. With this index, organisations can identify, retain and deal with any information that presents a risk and leave behind redundant, and trivial data to be decommissioned with the old archive.

High-risk data remediation

Archives often contain both high-risk and high-value information. One very serious risk is the prevalence of customers' identity or financial details stored without appropriate security in emails and attachments. These are often the result of employees making 'convenience copies' of this data, for purposes such as working from outside the office.

While indexing the contents of an archive, it is possible to identify and extract items containing high-risk information such as credit card and national identity numbers. Organisations can also isolate messages and attachments containing lists of 'hot words' and other high-risk items that are unique to their business. The organisation's risk team can review and act on even these items before the migration process begins.

Search macros and legal hold

Most organisations have a number of employees subject to litigation or regulatory inquiry. In many organisations, there are a few individuals who frequently appear in litigation or regulatory requests—also known as 'frequent flyer' custodians. One of the first steps in many archive migration projects is to isolate these custodians' data for preservation or legal hold purposes.

Organisations can pre-filter the

cecilepark PUBLICATIONS

Informing the legal industry since 1999

dataprotectionlaw&policy

Data Protection Law & Policy is essential reading for busy professionals operating in the data protection and privacy sphere. Written by experts for experts, this monthly journal delivers razor-sharp analysis and insights on the legal and regulatory topics on the horizon.

Launched in 2004, *Data Protection Law & Policy* has been on the cutting-edge of reporting, mapping out the developments in the internet domain, the evolving role of the data privacy professional, and the global shifts in policy and legislation.

dataprotectionlaw&policy

Regulation

Case Law

Data Breach & Data Security

Data Transfers & Outsourcing

Social media

Cloud computing

Online Privacy

Mobile Apps

Sectorial changes including in health and banking

"*Data Protection Law and Policy* gets to the heart of data privacy hot topics and considers them in a practical and pragmatic way. This is particularly useful as data privacy is a dynamic subject where interpreting the requirements of data privacy laws is fundamental to the role of a responsible data controller"

- Sue Taylor, Senior Data Privacy Manager Leading Financial Services Company

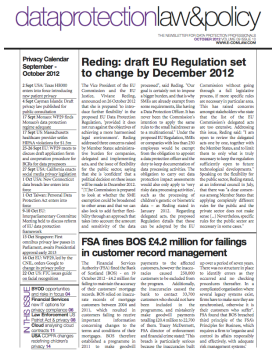
cecilepark PUBLICATIONS

Informing the legal industry since 1999

Big data - Social gaming - Mobile payments

In a world that changes everyday: six legal journals to guide you through the complex global marketplace

Data Protection Law & Policy


dataprotectionlaw&policy

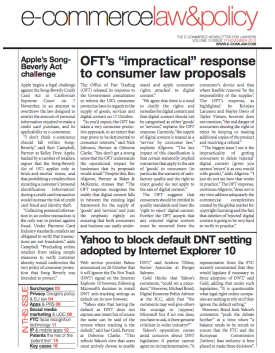
Privacy Calendar September October 2012

Reding: draft EU Regulation set to change by December 2012

FSA fines BOS £4.2 million for failings in customer record management

- Global privacy regulations
- Privacy compliance
- Data acquisition
- International data transfer

E-Commerce Law & Policy


e-commercelaw&policy

Apple's Song-Beverly Act challenge

OFT's "impractical" response to consumer law proposals

Yahoo to block default DNT setting adopted by Internet Explorer 10

- E-Commerce regulation
- Distance selling
- Social media
- Piracy

E-Commerce Law Reports

bi-monthly


e-commercelawreports

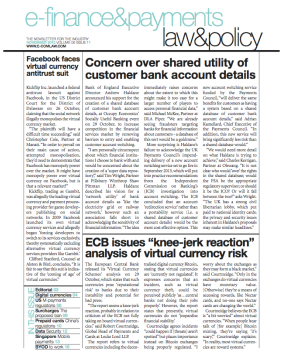
Key cases include:

- Online contracting
- Distance selling
- Defamation

Why...

- **Razor-sharp analysis of global legal issues**
- **Editorial board of experts**
- **Exclusive features & interviews**
- **Essential information: timely news**
- **In-depth analysis and expert commentary**
- **Unrestricted access to the online archive**

E-Finance & Payments Law & Policy


e-finance&payments law&policy

Facebook faces virtual currency antitrust suit

Concern over shared utility of customer bank account details

ECB issues "knee-jerk reaction" analysis of virtual currency risk

- E-payments
- Global regulatory regimes
- SEPA
- Virtual currency

World Online Gambling Law Report


worldonline gamblinglawreport

Singapore to regulate online gambling

Greece issues ultimatum to unlicensed online operators

Unauthorised tribal gaming offering in Canadian province

- Global gambling regulation
- Payment processing
- Social gaming
- Advertising

World Sports Law Report


worldsportslawreport

CJEU approves action against Sportradar

Calls for investigation as UCI supports Armstrong sanction

European Commission considers ban on athletes betting on sport

- Player contracts
- Broadcasting rights
- Sponsorship
- Anti-doping

To request a complimentary copy or for details on how to subscribe

Contact David Guati: +44 (0)20 7012 1387 / david.guati@e-comlaw.com

Visit our website:
www.e-comlaw.com

Head Office UK Cecile Park Publishing, 17 The Timber Yard, Drysdale Street, London N1 6ND
Tel: +44 (0)20 7012 1380

Find us on:

contents of the source archive to ensure they migrate all data relating to these custodians to the new archive or to another repository immediately after processing.

Deduplication

Archives apply multiple techniques to minimise the volume of information they store, including data compression and 'single instancing', a form of deduplication. However, single instancing has several limitations, such as ignoring identical items received in different mailboxes at slightly different times.

Creating a cryptographic hash value for each item makes it possible to deduplicate identical items from a single custodian's data, even when there are multiple copies across multiple email servers or archives. In some cases it may also be legally defensible to remove duplicates across multiple users or an entire data set.

Age-based culling

Migration offers an opportunity to cull data based on its age. Any data past its retention period, unless it is on legal hold, can simply be left behind in the old archive.

Archive metadata, such as the date each item was created, last accessed and last modified, provides further insights into the value of the data. For example, is it worth keeping copies of a company newsletter no-one has accessed in more than five years?

Size-based culling

Examining archived data by file size is another way to achieve a quick win. For example, an organisation could examine a list of the largest email messages and attachments that were past their retention date and that no one had accessed.

With today's technology, archive owners can use a series of logical techniques to minimise the volume of data they must migrate to the new platform, reduce target storage costs, mitigate business risks and complete migrations in weeks, not years

Distribution and auto messages

Automated email notifications are another large pool of low-value data, particularly because they are often sent to multiple recipients or distribution lists. Understanding whether these messages have value requires consultation with end users but often yields substantial results. It builds user engagement with the migration process because employees can see how it can help them work more productively. It also increases employees' comfort with the ideas of deleting data and broader information governance, which is critical to these projects' success.

Email subject value analysis

Another powerful technique is to group archived items across all user mailboxes by subject line or title. Across an entire archive with hundreds of millions or billions of items, this technique can identify millions of messages that have no business value.

For those messages that are more ambiguous (such as 'FW:Hey' or 'Re:Re'), information managers can manually review a random sample. If a 5% sample of all messages with the subject 'Fw:Fw:Fw' yields nothing but innocuous content, such as jokes, it would be quite reasonable to leave this content behind in a migration.

Spam and trivial data

Email gateways generally remove the worst examples of unsolicited commercial email before they reach user inboxes. However, employees often choose to receive bulk emails such as news updates and marketing messages. These messages have value to the user, at least initially, but their worth rapidly diminishes over time.

Deciding which of these messages to remove is, again, a consultative process. A complete index makes it relatively easy for information managers to isolate messages by a combination of sender, the domain the messages were sent from and keywords such as 'golf', 'lunch', 'weekend' or 'pizza.'

Predictive coding

Predictive coding, mostly used in eDiscovery, has a role to play in archive migration. Predictive coding creates a statistical model that uses word frequency to automatically separate documents into two categories. This is very similar to the way spam filters work.

A predictive coding model might be useful to sort email messages into buckets such as 'valuable' and 'trivial' or to identify specific types of information such as contracts or customer feedback forms.

Near-duplication and clustering

Although the deduplication technique I discussed earlier is more powerful than archives' single instancing, there are categories of duplicates it will not catch. Near-duplicate technology gets around this problem by comparing the similarly of text between items using a technique called 'shingling'.

With any item that is particularly valuable, or definitely not valuable, near-duplication can identify clusters of documents that contain similar text – another fast way to categorise large volumes of data.

Migrations in weeks

With today's technology, archive owners can use a series of logical techniques to minimise the volume of data they must migrate to the new platform, reduce target storage costs, mitigate business risks and complete migrations in weeks, not years.

Dr Jim Kent
CEO, EMEA and Head of Investigations
Nuix

Privacy after death: analysing the position on the deceased's emails

Prior to the widespread adoption of electronic mail, obtaining access to a beloved one's personal documents after his or her death was a fairly straight-forward process. The executor of the estate would, consistent with any specific instructions in the decedent's will, be authorised by a court of law to have banks and postal offices open the decedent's safety deposit boxes to determine their contents and aid with the administration of the estate. Frederick M. Joyce and Tiffany M. Nichols, Chair of Telecom Group and Associate at Venable LLP respectively, explores a recent Massachusetts appeals case, *Ajemian v. Yahoo! Inc. 7 May 2013*[1], involving a request by a deceased man's relatives to access his Yahoo! email account, which was denied by Yahoo!, analysing the difficulty of balancing electronic privacy with the rights of those claiming a legitimate reason to access online content.

Background facts

Around August-September of 2002, Robert Ajemian opened a Yahoo! email account for his brother John; Robert intended that the two access and share the account as co-users. Yahoo!'s Terms of Service and Privacy Policy (TOS) at the time when the account was first opened gave it the right to terminate a password and discard account content for any reason, in its sole discretion.

In August of 2006, John was struck and killed by a motor vehicle. At the time of his death, Yahoo!'s TOS included a clause excluding any third-party beneficiaries to the agreement and terminating any right of survivorship to Yahoo! email accounts. There was no evidence that this change in policy was ever communicated to the decedent or his brother.

Beginning shortly after John's death, Marianne and Robert Ajemian, siblings of the decedent, tried repeatedly to gain access to their brother's email account. Initially, they sought access in order to obtain the email addresses of John's friends to notify them of his death and memorial service. Subsequently, the plaintiffs (by then appointed as co-administrators of decedent's estate) sought the emails to help identify and locate assets and administer the decedent's estate.

Although Yahoo! initially agreed to turn over the information, provided the family produced a copy of John's birth and death certificates and other documentation, it later refused them access to the account or its contents, relying on the Stored Communications Act, 18 U.S.C. §§ 2701 et seq. (2006).

Yahoo! interpreted that law to prevent it from disclosing decedent's emails, even to the administrators of his estate. Subsequent negotiations led the parties to a partial resolution, requiring Yahoo! to produce 'all subscriber records and email header information, not to include email content,' which Yahoo! produced pursuant to the judgment.

Probate court decision

The co-administrators then filed a second complaint in Probate Court seeking the contents of the emails on the grounds that they were the property of John's estate and property of Robert as co-owner of the account. The probate judge dismissed the complaint on the grounds that the Yahoo! forum selection clause in the TOS required that any lawsuit be brought in California. The probate judge also concluded that res judicata barred the co-administrators from bringing their claim in a Massachusetts court, but not in a California court.

Appeals Court decision

The Appeals Court of Massachusetts (Norfolk division) determined that there was a failure in the record as to whether the forum selection clause had been 'reasonably communicated and accepted' by the email account users; therefore, Yahoo! had not met its burden of proof with respect to its contract claims. Further, since the co-administrators were not signatories to the Yahoo! contract, the court determined that it would not be reasonable to enforce the forum selection clause against them.

With respect to jurisdiction over this dispute, the Appeals Court favoured Massachusetts over California. The Appeals Court held that since John was domiciled in Massachusetts at the time of his death, 'Yahoo! [had] offered nothing to suggest that jurisdiction over assets of his estate [should be] anywhere other than Massachusetts.'

The Appeals Court did not reach the question of whether Yahoo! was required to keep the emails confidential under the Stored Communications Act.

The Court noted that Yahoo!'s request that the Probate Court's decision be affirmed under the Stored Communications Act had been raised only in a footnote and did not 'rise to [the] level of argument acceptable for appellate review.' The judgment was reversed and the matter remanded to the Probate Court for further proceedings consistent with the appellate opinion.

Email assets – property of an estate?

Recent news of apparent widespread electronic snooping by the USA government has heightened concerns that internet service providers guard and protect their customers' electronic communications. On the other hand, in a world where most people in developed nations communicate and engage in commerce largely via electronic means, cases like Ajemian v. Yahoo! highlight the often legitimate interests of non-governmental entities in gaining access to someone else's electronic communications.

Under Massachusetts law, as with most states, upon a person's death, that person's real and personal property passes to their devisees or heirs. Further, the decedent's personal representative has the right and responsibility to take control of the decedent's assets to the extent necessary to handle the administration of the estate. While it is unclear from the Appeals Court decision whether the decedent had a valid will upon his death, this dispute might have occurred with or without a will, given uncertainties under Massachusetts law as to whether email should be deemed property of an estate.

Yahoo! somewhat half-heartedly relied on the Stored Communications Act to deny the co-administrators access to the decedent's email records. Nevertheless, privacy rights are generally understood to cease upon a person's death and, personal effects such as letters and pictures that traditionally pass to heirs are just as likely as emails to contain personal information. The real concern for email service providers lies with potential liability for unauthorised disclosure to 'bad guys,' not family members, of

[T]he family's public policy interest in administering the estate outweighed Yahoo!'s inchoate interests in protecting the privacy of a deceased customer

private and protected electronic communications.

One lesson to be learned from this case is that the drafters of wills may need to focus their attention on the central importance of electronic assets. Still, it could be another generation until the phrase 'personal effects' is recognised to include all of one's electronic communications and electronic documents.

In the meantime, courts will continue to struggle with this tension between electronic privacy rights and the legitimate interests of a decedent's estate administrators. As shown in this case, contract law provides only a partial solution, and may be part of the problem. Although 'a common law cause of action for invasion of privacy may cease upon death, general freedom of contract principles suggest that it may still be possible to create a contractual right of privacy which is effective to protect private information of deceased individuals.'[2]

However, if a contract is deemed unlawful or contrary to public policy, it is unenforceable. Absent some record evidence that the decedent intended Yahoo!'s privacy policy to be binding on his estate, the Appeals Court likened Yahoo!'s privacy policy to a contract of adhesion, the kind a majority of internet users fail to read[3]. Consequently, the family's public policy interest in administering the estate outweighed Yahoo!'s inchoate interests in protecting the privacy of a deceased customer.

A change in venue, or even a change in email service provider, may have led to a different outcome. For instance, Indiana, Connecticut, Rhode Island, and Oklahoma have adopted laws granting estates certain property rights in the electronically stored communications of decedents. At the same time, many email service providers have policies in place that would have allowed the plaintiffs access to the decedent's emails. Absent changes in federal or state electronic privacy laws, these types of probate court disputes may become increasingly common.

Frederick M. Joyce
Chair, Telecom Group
Venable LLP
rjoyce@venable.com

Tiffany M. Nichols
Associate
Venable LLP
tmnichols@venable.com

1. Ajemian v. Yahoo, 987 N.E.2d 604 (Mass. App. Ct. 7 May 2013)
2. Jonathan J. Darrow & Gerald R. Ferrera, '*Who Owns a Decedent's E-Mails: Inheritable Probate Assets or Property of the Network?,*' 10 N.Y.U. J. Legis. & Pub. Pol'y 281, 314 (2006-2007) at 314 (citing Willard Packing Co. v. Javier, 899 A.2d 940, 947 (Md. Ct. Spec. App. 2006); State v. Pleva, 456 N.W.2d 359, 362 (Wis. 1990)).
3. See Tyler G. Tarney, '*A Call for Legislation to Permit the Transfer of Digital Assets at Death,*' 40 Cap. U. L. Rev. 773, 778 (Summer 2012) (citation omitted).

Analysing the new Protection of Personal Information Bill

The South African Parliament passed - on 22 August 2013 - the Protection of Personal Information (POPI) Bill. POPI was introduced in August 2009 by the South African Cabinet and represents South Africa's first comprehensive data protection legislation. POPI is expected to come into force before the end of the year. *Data Protection Law & Policy* interviewed Advocate Mthunzi Mhaga, Spokesperson for the Department of Justice and Constitutional Development, to learn more about the new Bill.

To what extent does the final version differ from the 2009 Bill?

The final version of the Bill differs in a few respects from the 2009 version. For example:

- Chapter 5 of the Bill aims to regulate the establishment of an Information Regulator and the amendments that to the Chapter were aimed at strengthening the provisions concerned in order to ensure that the Regulator will be established as an independent statutory authority. The Bill further aims to amend the Promotion of Access to Information Act 2000 (Act 2 of 2000), in order to establish the Information Regulator as a functionary that may consider complaints against decisions that have been taken by public or private bodies in respect of requests for access to records of the bodies concerned. The complaints procedure provided for in the Promotion of Access to Information Act 2000, will be amended as follows:

(i) Insofar as certain public bodies are concerned, the compulsory internal appeal procedure will be retained. A party who is aggrieved by a decision of a relevant authority will be granted an option to either submit a complaint to the Information Regulator or to approach a court for appropriate relief.

(ii) A party who is aggrieved by a decision by the head of a private body will be able to either submit a complaint to the Information Regulator in respect of the decision concerned, or to approach the court for appropriate relief.

- The 2009 version of the Bill reflected provisions dealing with the requirement that responsible parties (parties who process personal information) should notify the Information Regulator that they process personal information and the requirement that they should obtain prior authorisation from the Information Regulator before they process certain categories of personal information. The provisions dealing with notification were aimed at regulating matters associated with the requirement, such as, the particulars to be included in the notification, exemptions and the criminalisation of any failure on the part of a responsible party to notify the Information Regulator. However, the provisions dealing with notification were omitted from the final version of the Bill.

The provisions dealing with prior authorisation which were retained, among others, require that a responsible party must obtain authorisation from the Information Regulator before any processing if the responsible party plans to, among others, process personal information for the purposes of credit reporting or transfer special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

What are the most important features of the law?

- The Bill aims to introduce eight internationally accepted information protection principles, namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. Special provisions have also been included in the Bill with the view to the protection of special (sensitive) personal information of data subjects and the personal information of children.
- An independent statutory authority, namely the Information Regulator, will be introduced that will be responsible for monitoring the implementation of the new Protection of Personal Information Act and the Promotion of Access to Information Act 2000.
- Enforcement of the Bill will be through the Information Regulator by means of a system of notices, as a first step, where conciliation or mediation has not been successful. The Information Regulator is also empowered to assist data subjects in claiming compensation from responsible parties where the manner in which they process personal information is not in line with the requirements of the Bill and such processing has caused damage to the data subjects concerned.
- The Bill further aims to follow a flexible approach in terms of which industries will be allowed to develop codes of conduct in accordance with the conditions (principles) for the lawful processing of personal information. Codes of conduct will assist in the practical application of the conditions for the processing of personal information in specific sectors. Provision is made for codes of conduct to be issued for specific sectors by the Information

Regulator and may even make provision for adjudicators to be established in terms of such codes to be responsible for the supervision of the processing of personal information in those specific sectors.

- The Bill also aims to make provision for the protection of data subjects' rights insofar as unsolicited electronic communications and automated decision making are concerned. The Bill also provides that personal information may not be transferred to countries that do not ensure an adequate level of information protection. This prohibition is subject to certain exceptions, for example, where a data subject consents to the transfer of his or her personal information or where the transfer is necessary for the performance of a contract between the data subject and the responsible party.

When enacted, will the Law see a dramatic shift for South African business and foreign businesses wishing to operate in South Africa?

The Bill emanates from the South African Law Reform Commission's report on privacy and data protection. The Bill aims, in harmony with international standards, to give effect to the right to privacy, by introducing measures to ensure that the personal information of an individual (data subject) is safeguarded. The Bill also aims to balance the right to privacy against other rights, particularly the right of access to information and to generally protect important interests, including the free flow of information within and across the borders of South Africa. Therefore, it should be noted that, in view of international trends and expectations, the Bill will contribute substantially towards South Africa's future participation in the information market as a country which could be regarded as providing adequate information protection by international standards.

[I]n view of international trends and expectations, the Bill will contribute substantially towards South Africa's future participation in the information market as a country which could be regarded as providing adequate information protection by international standards

When do businesses operating in South Africa have to comply with the law?

Responsible parties will have to comply with the provisions of the Bill as soon as it is implemented. However, the Legislature has decided to introduce a transitional arrangement in order to accommodate those responsible parties who are not in a position to comply fully with the provisions of the Bill upon implementation thereof. Clause 114 of the Bill, for instance, provides that all processing of personal information must, within one year after the implementation of the clause, comply with the provisions of the Bill.

Has the Information Protection Regulator been nominated? When is this expected?

The members of the Information Regulator have not been nominated yet. The Bill was only recently approved by Parliament and must, in terms of section 79 of the Constitution of the Republic of South Africa, 1996, be referred to the President for the President to assent to and sign the Bill. A Bill assented and signed by the President becomes an Act of Parliament and, in the present case, will take effect on a date to be determined by the President. In this regard the provisions of clause 41 of the Bill should also be noted, which prescribes the procedure for the appointment of the members of the Regulator which, among others, involves Parliament.

What are the maximum sanctions?

Chapter 11 of the Bill deals with offences and penalties. The Chapter creates offences such as obstruction of the Regulator (clause 100), breach of confidentiality by a person acting under the direction of the Regulator (clause 101), obstruction of the execution of a warrant (clause 102), the failure to comply with an enforcement notice (clause 103) and offences by witnesses (clause 104).

Two additional offences, apart from those mentioned above, that were included in the introduced version of the Bill, were created, namely unlawful acts by responsible parties in connection with account numbers (clause 105) and unlawful acts by third parties in connection with account numbers (clause 106). The Legislature has also introduced a provision, namely clause 109 of the Bill, which aims to empower the Information Regulator to impose administrative fines upon responsible parties instead of being prosecuted for having committed offences in terms of the Bill.

Advocate Mthunzi Mhaga
Spokesperson for the Department of Justice and Constitutional Development

Data transfers to the cloud: avoiding the pitfalls of export control rules

Use of cloud computing in the business sector is fast becoming the norm, offering increased flexibility, reduction of costs and a stronger interconnection of businesses within the competitive global markets. However, export control mechanisms are often overlooked when transferring data in the cloud, with severe sanctions for violations. Dr Philip Haellmigk and Florian Foerster, Associate and Trainee Solicitor respectively at Bird & Bird, outline the requirements businesses using the cloud should be aware of, as well as how to avoid falling foul of these provisions.

In the context of cloud computing, the issues of data protection and security of information stored within the cloud have been intensely discussed. However, businesses pay too little attention to the significant export control implications in the context of cloud computing. Most businesses have a misleading understanding of what actually constitutes an export and fail to recognise that export control mechanisms are intrinsically linked to the access and transfer of data in the cloud. This pitfall has to be avoided as sanctions for breaches of the legal requirements are draconic: the sanctions comprise, among others, imprisonment and unlimited fines for the corporations and individuals. Businesses that want to use cloud computing models are therefore well advised to take export control laws seriously.

Applicability to cloud computing

Export control regulations are applicable to cloud computing in several situations:

- If the cloud provider is located abroad, then the process of IT outsourcing to a cloud is subject to export control regulations.
- Moreover, the cloud providers themselves may wish to store the data received, for example for financial reasons; with a sub-contractor in a third country with a more favourable IT cost structure. This is usual business practice as 'borderless' data traffic, in particular, is an integral part and advantage of cloud computing.
- In cases where the cloud provider's head office is in the UK but data is being accessed from abroad, the external access leads to an (indirect) data transfer abroad. Whether or not the data is actually being accessed remains irrelevant. The sole possibility that data may be accessed entails export control obligations.
- Setting up an in-house private cloud that is only accessible by company employees at all foreign locations is also subject to export control regulations. Often businesses misjudge the significance of export control regulations to the transfer of intra-company data. Therefore, one often hears the following statement: "It's all internal, it all stays within the firm!" This point of view is wrong. From an export control perspective the intra-company exchange of data is very relevant. Since in this case, data also ends up abroad irrespective of whether the data recipient is a colleague or a third person.

EU export control regulations

The most important European instrument is Council Regulation (EU) No 428/2009 of 5 May 2012, regarding a community regime for the control of exports, transfer and brokering of dual-use goods (the Dual-Use Regulation) which includes an annex with dual-use items that require export licences (the so-called Dual-Use List). The Dual-Use List not only comprises physical goods, but also technology, data and data processing programmes developed or required for such goods. The export of dual-use items also applies to the transfer of software or technology by way of electronic media (facsimile, telephone, e-mail). This includes the provision of software and technology in electronic formats to legal and natural persons outside of the EU.

Embargoes

Currently there are EU embargoes against 26 countries, however an EU Member State may impose further national restrictions against an embargoed country (as the UK in relation to Iran) or embargo an additional country (as the UK in relation to Argentina).

Sanctions

Compliance in the field of export control law is not just a moral question of company philosophy or a nice, but unnecessary variation of compliance.

Criminal and civil penalties

It is a criminal offence to export goods (including technology and data) which are controlled or subject to sanctions and embargo regime without a licence from the appropriate authority. Civil and criminal penalties may be imposed both on companies and individuals, depending on the nature of the breach. In the UK, the maximum criminal penaltiy is up to ten years imprisonment. In Germany, the maximum imprisonment is 15 years. Enforcement has become a priority in the UK and Germany, with a number of recent criminal prosecutions against both corporations and individuals. Furthermore, corporations and individuals can face unlimited fines.

Denial of license

A further consequence of an illegal data transfer that impacts export businesses is that authorities may revoke export licenses that have already been granted. Furthermore, the relationship with the authorities may be damaged to the effect that future export license applications are denied.

Reputational damage

Finally, the commercial and reputational consequences of being subject to an investigation or enforcement action must be considered. Commercial relationships with suppliers and customers can be impacted and prosecutions can attract high levels of negative publicity.

Compliance measures

European businesses ought to check whether the EU and national regulations of export control law apply to its business prior to the use of in house cloud computing; irrespective of which model is to be implemented.

Perform an audit

Does the IT to be outsourced contain any sensitive data regarding legal export control? Has this data been recorded in the respective lists of goods (EU Dual-Use List, national military goods list)?

Instruct employees

Providing that the IT to be outsourced contains sensitive data in regards to legal export control, the employees must be informed. Furthermore, the employees should be provided with work and process instructions for the intra-corporate handling regarding export of such sensitive data. In addition, it has to be stipulated which employee (centrally) is responsible for exchange and maintaining contact with the authorities (applications for authorisation, general questions etc.). On the whole, it has to be ensured that on all corporate levels the required export control compliance structures are being implemented (starting with the person responsible and going all the way up to the management level).

Often businesses misjudge the significance of export control regulations to the transfer of intracompany data

Examine the cloud provider

Legal export control compliance does only work if the cloud provider is also willing to observe the export control regulations. Therefore, it has to be clarified with the respective cloud provider in which countries its IT infrastructure is located or which sub-suppliers are situated in which countries (for example, checking 'embargoes').

Secure contractual protection

Finally, the companies should secure themselves contractually against the cloud provider and its handling of outsourced data since they lose most of the control over this data by outsourcing it. However, the company remains responsible for the export of the data and its further fate. Therefore, the cloud computing contracts should contain export control clauses which ensure that the cloud provider promises to observe the respective export control regulations when providing services. If existent, the legal department should be implicitly consulted and/or external legal advice should be obtained.

Dr Philip Haellmigk, LLM
Associate
Solicitor (England & Wales)
Rechtsanwalt (Germany)
Lic. en Droit (France)
Bird & Bird
philip.haellmigk@twobirds.com

Florian Foerster
Trainee Solicitor
Bird & Bird
florian.foerster@twobirds.com

Revised OECD Guidelines

The Organisation for Economic Co-operation and Development (OECD) published - on 9 September 2013 - revisions to their Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the Guidelines). The revisions represent the first update to the original 1980 version, which became the first set of internationally agreed privacy principles. *Data Protection Law & Policy* has put together a roundtable of comments from privacy experts across the globe to provide a truly international perspective on this development.

Jennifer Stoddart, Privacy Commissioner of Canada, Chair of the Privacy Expert Group reviewing the OECD Guidelines:
The updated Guidelines are notable in two respects:

- Firstly, there is a greater focus on the concept of accountability. While accountability remains one of the key principles defined in the Guidelines, the revised Guidelines provide greater clarity on implementing accountability, including direction on establishing a privacy management programme within an organisation. The updated Guidelines also introduce the concept of breach notification. Organizations should notify privacy enforcement authorities of significant privacy breaches, and, in cases where a breach may adversely impact individuals, organizations should inform the affected individuals as well.
- Secondly, there is a new focus on the global dimension of privacy. In an environment where data flows freely across borders, greater interoperability between jurisdictions is necessary. Member countries should establish national privacy strategies reflecting a coordinated approach across all of government. Privacy enforcement authorities must have adequate powers, resources and technical capacity to effectively enforce the privacy laws in their respective jurisdictions.

My Office was pleased to have contributed to the review process. We have long believed that accountability is the driving force behind privacy management.

We have also seen first-hand the fruitful results that have grown out of increased international cooperation and collaboration.

The OECD Council's adoption of the revised Privacy Guidelines is an important milestone for the global privacy community and an excellent starting point for organizations in countries without privacy legislation. The original Guidelines and its Basic Principles served as a foundation for the development of the Canadian PIPEDA in the late 1990s.

Christopher Wolf, Partner at Hogan Lovells and Director of the Privacy and Information Management Group
I was a member of the OECD Volunteer Group of privacy experts asked to consult on the Guidelines, and I am truly pleased with the final product. The practical focus on a risk management approach to protecting privacy makes great sense and is the only realistic option in a data-laden economy. I also strongly endorse the need for greater efforts to address the global dimension of privacy through improved interoperability.

The Guidelines recognize the strategic importance of privacy requires a multifaceted national strategy co-ordinated at the highest levels of government. I also am pleased to see the emphasis on privacy management programs to serve as the core operational mechanism through which organizations implement privacy protection. The inclusion of a provision on data security breach notification is a reflection of the contribution this US-originated concept has made to the protection of privacy.

Cédric Burton, Senior Associate at Wilson Sonsini Goodrich & Rosati
The main privacy principles stay untouched, which demonstrates that common global trends are currently emerging and becoming the bedrock of data protection globally. The revised guidelines also build on the various existing data protection regimes by cherry-picking obligations and concepts that have proven to be working well in some regions of the world and are now widely recognised as key privacy principles globally.

Some aspects of the OECD privacy guidelines have been modernised such as the rules on trans-border data flows and the security requirements, but one of the major improvement is the focus is on accountability, privacy management programs and on how privacy protections are concretely implemented within organisations. This demonstrates a shift from a rather bureaucratic approach to a more practical one.