Legal Information Management, 15 (2015), pp. 61–69

doi:10.1017/S1472669615000183

Is Someone Watching You? Data Privacy and Protection: Current Issues

Abstract: In this piece Jackie Fishleigh offers her views on the rather edgy and menacing world of data privacy and protection, focusing on developments during the last year. Her article provides a summary of the key issues that are currently being discussed and debated, including at BIALL's own annual conference which took place last year in Harrogate.
Keywords: internet; social media; privacy; data protection

A MODERN DAY FAUSTIAN PACT

While businesses used to ring-fence cyber security as something for their IT departments to deal with, more enlightened corporates are making it a senior management and, or, a firm wide issue with each employee taking personal responsibility. For each of us, as private individuals, there is the increasing and ongoing dilemma of whether and when to share – and when not to – in our personal lives. Recent research in the journal, Information Age[1], indicates that in four to five years any business not engaging in social media will not be taken seriously, while it is predicated that in eight to nine years individuals who do not have social media accounts may be regarded as untrustworthy. But, are the risks to reputation for a business and the loss of privacy or worse for the individual when things go wrong, really a price worth paying? As communications and information technology develops, the data footprint we leave reveals ever more about our identities and private lives. We should all be concerned as to who holds our data, and why, because our privacy can be compromised if our personal data is disseminated or misused. Like Faust, of the German legend, we are forced to make a trade-off between knowledge, and even power and wealth if we are lucky, and maintaining our integrity.

"RIGHT TO BE FORGOTTEN" – sparks debate on balancing freedom of expression and public interest with the right to privacy

This recent controversial ruling by the European Court of Justice (ECJ) upheld the right of Spaniard, Mario Costeja González who complained that searches on him still brought up out-of-date information about his repossessed house that had been put up for auction[2]. Service providers such as Google must now remove links to disputed references so that they do not appear if the name of the individual is searched. They also have to display a notice to the effect that something has been 'taken down' (though with no further information as to what). N.B. A request for the removal of a link to a story could come from someone who is not even its subject.

Reviewing and processing these requests will prove to be a massive administrative and technical challenge. Google is looking at the requests it receives and discussing them with a panel. If Google refuse a request to remove information, one can appeal to one's local court and local data privacy commissioner. With the internet constantly changing, the information in question may quickly be migrated to other websites.

There is now a form that can be completed in order to uphold one's 'right to be forgotten'. The complainant or their representative must provide proof of identity and state which links they wish to have removed. Solicitors are beginning to offer this as a standard feature of reputation management. According to Adrian Weckler, Technology Editor for Independent Newspapers (Ireland's largest newspaper group), who spoke at the BIALL Conference in June 2014, to date 40% of the requests to have links removed are from Germany.[3] Domestic law in both Germany and France are in line with the ruling. In general terms, Europe tends to be keen to protect privacy in comparison with America where free speech is embraced enthusiastically.

The ECJ ruling, mentioned above[4], makes clear that a search engine such as Google has to take responsibility as a 'data controller' for the content that it links to. Data protection lawyers said the ruling meant that Google could no longer be regarded legally as a "neutral intermediary". Jimmy Wales, co-founder of Wikipedia, referred to 'the right to be forgotten' as amounting to censorship[5]. Following this ruling, a news story from 1999 published in "The Independent" about a former head of the Law Society was removed from Google, according to Google itself[6]. The article about Robert Sayer's election as the new head of the Law Society said he described an individual who backed his rival as "a piece of dog turd on your shoe".

This was part of the first tranche of web stories (others concerned singer Kelly Osbourne, ex-Merrill Lynch boss Stan O'Neal, and a football referee involved in a controversial penalty decision[7]) to be removed from Google's search results, leading to accusations that Google was sabotaging the 'right to be forgotten' by deleting links to apparently 'harmless' news articles to stir up anger against what many saw as a form of censorship. Whether Google is trying to discredit the ruling or whether its actions are 'tactical' as the result of a decision that it is simply cheaper to say 'yes' to all these requests, is unknown. Privacy campaigners say that results that relate to the articles are in the public interest and should not be removed. Meanwhile, Ryan Heath, a spokesman for the European Commission's Vice-President Neelie Kroes, said that he could not see a "reasonable public interest" for the action, adding that the court ruling should not allow people to " Photoshop their lives"[8].

Around 70,000 requests for links to be removed have been made in the month of June (2104) alone, with more than 8,000 coming from Britain[9]. The BBC has also been swamped by requests to delete stories on its website. This has led to new guidance on 'unpublishing' content. David Jordan, BBC director of editorial policy and standards said, "Sometimes the people we feature in our news reports want the news about themselves to be erased so they can obscure the events they were involved in, or the comments they made to us and stop others finding them"[10]. The new guidance states that material on the BBC website is part of a "permanently accessible archive" and will not be removed or changed unless there are "exceptional circumstances". It adds the "removing online content, particularly news items, risks the accusation that we are erasing the past or altering history"[11].

EU DATA PROTECTION LAW to apply to non-European companies doing business in the European Single Market

The European Commission has ruled that data held by foreign companies such as Google, Facebook, Twitter and Microsoft will have to meet European privacy standards. This announcement, made in June, has proved to be highly contentious, according to Adrian Weckler[12].

FACEBOOK users may not 'like' the lack of legal protection

The Solicitors Journal reported online[13], on 8 July 2014, news of a plan for the Information Commissioner's Office (ICO) to probe Facebook's study of emotion which allegedly breached user privacy. The ubiquitous social network manipulated the newsfeeds of almost 700,000 UK users by monitoring how the stories influenced their mood in subsequent posts, sparking a furious backlash over invasion of privacy and data protection breaches, which the ICO are now investigating.

However, Michael Sandys, Partner and Head of Commercial at Jackson Canter Solicitors, has warned British people not to expect bringing successful legal claims as they must show that the social network has infringed its own user terms. "Privacy law in the UK is still in its infancy and remains undeveloped," he said. "In other countries, such as France, they have a much more robust system to protect the privacy of an individual."[14] "If Facebook has gathered data from what people post on newsfeeds which is not restricted by privacy settings then under UK legislation there is probably nothing a user can do unless it can show that there has been a breach of its terms of service regarding data use policy. If this can be established then there may be a potential claim by the user. However, assessing loss may not be easy."[15]

Article 8 of the Human Rights Act of 1998 states that people have a right to a private and family life, but this can only be applied to the Facebook study if certain conditions are met. "Whether data protection laws have been breached will depend on whether personal details have been used in the study, which Facebook has stated is not the case. Therefore, there is unlikely to have been a contravention of those laws unless specific personal data has been used." He continued: "If it can be shown that the messages which Facebook gathered for its project were posted to a profile which had its privacy settings turned up, those users would probably have a case. Their messages are only targeted at a specific and defined group of people and therefore there would be a reasonable expectation of privacy. This would be a good basis to build a case from."[16]

CREEPING MISOGYNY AND WORSE

BBC Newsnight presenter Kirsty Wark's unsettling BBC documentary "Blurred Lines: The New Battle of the Sexes", which was screened on 8 May 2014, made headlines with the comments it elicited from academic and journalist Germaine Greer. Greer claimed that online trolling was "setting the feminist cause back 40 years". This was a reference to the ordeal suffered by Caroline Criado-Perez who, having successfully lobbied to get Jane Austen on a UK bank note, received terrifying online abuse on Twitter. Isabella Sorley, 23, and John Nimmo, 25, were subsequently jailed for bombarding her with rape and death threats.

The programme included a moving speech from academic and TV presenter, Mary Beard, Professor of Classics at the University of Cambridge, who suffered internet abuse after appearing on Question Time, lamenting how "vile" online threats are "bad for female participation in the public sphere"(reported on BBC online, 23rd January 2013).[17] Many of the comments made about Question Time each week on Twitter are about how the female panellists look.

For the sake of her children Kirsty Wark had decided to embark on the gritty investigation of today's "anything goes" culture of laddishness which she felt had reached a

https://doi.org/10.1017/S1472669615000183 Published online by Cambridge University Press

tipping point where it had led to a new and darker inequality between the sexes. She felt this was worse than the "sexist Seventies" when she was a student. Much of this was due to the advent of the internet in her view.

On the day JK Rowling announced she had donated £1m to the 'Better Together' campaign, in relation to the Scottish independence debate, the author was subjected to online abuse and the Scottish detectives were called in to investigate. Rosamund Urwin, a London Evening Standard columnist, wondered whether we were seeing the answer to the 'Lord of the Flies' question: "how would we behave in a world with no laws and no leaders?" In her view, "we don't really need fiction to find that out. Because modern life offers its own case study: the internet. There, racism, misogyny, homophobia, sexual remarks, violent threats and irrational outrage are all part of the vernacular."[18]

If this sounds rather over the top, the Metro newspaper reported (on 2 July 2014) that laws preventing vengeful partners from posting sexually explicit pictures of their former lovers are being seriously considered. 'Revenge porn' can be defined as the unauthorised and malicious dissemination of intimate images (photographs or video) on the internet.

The Justice Secretary Chris Grayling told MPs that the government is "very open" to having a "serious discussion" about the issue after the summer recess[19]. So called 'revenge porn' is becoming more common. It causes huge harm to victims who feel degraded and humiliated. Some victims have ended up self-harming and even killing themselves.

This is an unquestionable misuse of private information and the courts are likely to be sympathetic to a claimant who has had their trust abused in such a fashion. A claimant's priority will be to secure the prompt removal of any images in the public domain. Website operators that do not remove images on notice are normally treated as defendants (although complications may arise if they are outside the jurisdiction). At present, legal redress is only possible if pictures are deemed a breach of copyright law, harassment or depict under 18 year olds. No specific offence covers revenge porn and there is pressure on the government to follow the lead of several other states and legislate.

SEARCH ENGINES

Phil Bradley's keynote address, given on 12 June 2014 at the 45th Annual BIALL Conference in Harrogate, reminded delegates of the increasing need to exercise caution online, as what you see is not necessarily the truth[20]. His example was a website called, "Martin Luther King – A True Historical Explanation" which on closer examination actually turned out to be a racist site. Even basic facts can be hard to establish. When Fidel Castro failed to comment on the death of his close ally Nelson Mandela in late 2013, rumours circulated that he himself had passed away. In the end Castro had to make a rare public appearance to prove he was still alive. This is not untypical as the internet does contain a myriad of extraneous, biased and inaccurate material, some of it disguised, some not. It is for this reason that there is a prohibition on juries using the internet and social media to research cases.

Phil Bradley also queried what "new" and "news" really meant these days in social media terms. With 24/7 news broadcasts there is no let-up in the constant stream of news which frequently turns out to be cobbled together from market research findings, trends revealed by surveys of all kinds and enhanced commentaries on already existing stories. Is 'news' today just what happened in the past hour?

This contrasts with my youth in the 1970s sitting down with the family to watch News at Ten presented by ITN anchor Reginald "Reggie" Bosanquet. Viewing this was quite a ritual and an event, and was how one learned what was really going on in the world – wars, elections and world economics and politics were standard fare. These days a vast range of famous faces from entertainment and the media pop up everywhere commenting at will on this issue and that with a view to seeking public attention. Celebrities may make points via social media to get a rise out of people and to raise their profiles. So can we still trust what we find via search engines?

Karen Blakeman informed us at her Pre-Conference Seminar (delivered on 11th June), entitled "The Brave New World of Free, Open Data and Open Access" (also held at the BIALL Conference referred to above), that "Hummingbird" was launched last autumn and represented the biggest change to Google search since 2001. It is a completely new search algorithm that affects 90% of all searches. It aims to understand what searchers really want and provide them with better answers. Google now examine the searcher's query as a whole and process the meaning behind it. This focus on context and the user's intentions aims to deliver more relevant results and better answers.

However, this type of personalisation which is being used increasingly by Google is not helpful to researchers as it filters potential hits based on their previous search history and location. This means that two users can perform an identical search and yet get different results. Phil Bradley recommended 'Duck Duck Go' in preference to Google as it does not track you, it does not personalise data and is a pure stream. We are constantly being tracked even when we sign out from Google apparently[21].

BROWSER FINGERPRINTING TECHNIQUES

There are a number of browser fingerprinting techniques around which track online users. Using special scripts they allow websites to uniquely identify and track visitors

https://doi.org/10.1017/S1472669615000183 Published online by Cambridge University Press

without the use of browser cookies or other similar means. 5.5% of the internet's 100,000 websites use these scripts. Canvas fingerprinting is the most well-known form of the technique and was originally described by researchers from Princeton University and KU Leuven University. 95 percent of these websites use canvas fingerprinting created by technology company AddThis. Rich Harris, Chief Executive of AddThis, says they began testing canvas fingerprinting as a possible way to replace "cookies" i.e. the traditional way that users are tracked, via text files installed on their computers[22]

DATA BABY PROJECT tracks the secret life of a mobile phone

As part of the *Data Baby project*, Channel 4 News created a fake, virtual identity to track its data and listen in to the stream of information flowing to and from the devices with which many of us spend our entire day. The 'baby' is called Rebecca Taylor, (one of most common names for women her age). She's 27, lives in London, likes photography, travel, music and uses all the popular social networks. The project which was launched on 6 March 2013 has revealed many disturbing truths including the fact that hundreds of thousands of messages phones are sent out every day, without us even knowing. Some of these messages are useful. They help our phones and apps stay connected and up-to-date. But some are giving away our location and our phones' unique identities to advertisers, who then use this information to target us. Apps were the main source of leakage and it so it is recommended that users read the terms and conditions carefully before signing up.

WE'LL JUST HAVE TO GET USED TO SHARING MORE

Netflix, the US company that provides on demand access to online movies, has claimed that we need to become accustomed to Netflix monitoring which films we watch (including the ones we are a bit embarrassed to admit we saw) and allow them to personalise the choice it offers us. This Faustian pact is worth it according to Netflix.

IDENTITY THEFT AND OTHER RISKS

The results of David Haynes' recent survey conducted as part of his PhD on risk and regulation of social media in the UK were published in the CILIP Update in June 2014[23]. 213 respondents ranked 12 risks. Identity theft came top of the risk list followed by strangers being able to see sensitive personal details, targeting by advertising, becoming a victim of fraud and discrimination by employer or potential employer.

Targeting by criminals (so they can burgle your house while you are away), friends and family or colleagues being able to see sensitive personal details, cyber-bullying or harassment (or stalking), and targeting by official bodies or security agencies were perceived to be less risky. More serious but perceived as perhaps (hopefully!) unlikely were extortion or blackmail, prosecution by authorities because of crime allegations and physical violence or kidnapping.

Respondents were also asked how effective they found current regulation for protecting users of online social networking services against risk. The overall message was that regulation was inadequate. When asked who should have primary responsibility for protecting personal data on online social networks 55% laid it at the door of online social network providers, with 26% users themselves, 13% government and others 7%.

WHAT'S IN A NAME?

Pseudonyms are frequently used on social media including the ubiquitous "anonymous". Even comments posted to The Lawyer website are mostly anons. I tend to think that the cloak of anonymity can bring out the worst in people but then again since I have a very unusual surname I can understand why people don't want to put out their real names and draw attention to themselves when they are easily traceable. Even those with common names are not safe. A John Smith, for example, could be in danger of being mixed up with a transgressor with the same or a similar name.

HALF OF CRIMES ARE NOW ONLINE

Former Cumbria Chief Constable Stuart Hyde said he was astonished to discover while researching social media and crime that the term Facebook was recorded 14,000 times in logs and records made by a single force's control room staff in 2011[24]. This rose to almost 19,000 in 2012 and more than 27,000 last year. Police forces are undergoing training to distinguish which of this avalanche of reported incidents are serious crimes which need to be given priority.

Rosamund Urwin quoted Chief constable Alex Marshall, who heads the College of Policing and says we have reached a tipping point: the majority of calls about harassment now involve online behaviour. Some of these complaints are silly — "X has de-friended me on Facebook," but others were in response to frightening abuse: rape threats, death threats[25]. Marshall's comments provoked all the predictable reactions. The onus was put on victims: they should "shrug it off" or develop "a thicker skin". Alternatively, they could leave social media, even though that means the "bile-spewing bullies" have won. There was the perpetual refrain too, "It's not real, it's just the internet."

And while there are occasional sanctions for criminal keyboard-bashers — a £624 fine for naming a rape victim, 12 weeks in prison for sending menacing tweets — people simply don't act as though it's a policed place. The virtual world is a "vituperative free-for-all."

https://doi.org/10.1017/S1472669615000183 Published online by Cambridge University Press

But it is real as Urwin pointed out, "Just because someone's threatening you on Facebook rather than in the pub, doesn't render it a joke or a dream. Your Twitter responses filling with abuse can feel like an intrusion into personal space. The effects can certainly be real too: think of the suicides linked to online abuse." She suggests that although it is essential police take online harassment seriously, the problem needs to be addressed more widely. Children should be taught in school about the law and the internet. Social media sites should ensure users actually see the terms of use and what constitutes illegal behaviour.

DO'S AND DON'T FOR THE INDIVIDUAL

Do's

Do make sure you understand and use the privacy settings on the various social media services. And educate others about them.

Don't s

Don't use obvious passwords such as password (!), dates of birth or 123456 – data breaches often occur when these weak/obvious/guessable passwords are used. Avoid giving out personal data to companies. Don't open unexpected e-mails from companies even if their websites look like the real one. This could be a phishing expedition to get your data and potentially your money.

CYBER ATTACKS, HACKING AND MALWARE

Arriving slightly late at Graham Cluley's session at Law Tech Futures 2014 held at the Queen Elizabeth Conference Centre in London on 25 March 2014, it felt like we were being briefed on the enemy before immediate deployment to a war zone. Graham explained how, in the past, computer viruses such as cascade and green caterpillar made it obvious when someone had got into a system with disruption to screen, 'ha ha ha' messages and the like. Now malware, i.e. software designed to take control and damage your computer or mobile device, does not announce its presence. It is stealthy and it is not done by teenagers from their bedrooms but is more likely to be carried out by government and intelligence agencies.

In one high profile example, Belgacom (a Belgium telecoms company) was hacked by the UK's surveillance agency GCHQ who wanted to monitor some of its customers referred to in a Reuters report on 13 December 2014.GCHQ has also been revealed to be regularly and indiscriminately intercepting communications both at home and abroad, including gathering webcam images from Yahoo messaging services.

These days hackers look for 'watering holes' and do 'drive by down loads'. They just need to know which websites you are interested in! They see where people congregate online rather like a naturalist observing rhinos at watering holes. There are also 'Zero day' threats which exploit a previously unknown vulnerability in a computer application, one that developers have not had time to address and patch. It is even possible to go somewhere legitimate online and get hacked without any trace of it being left behind!

Some political and financial criminals are interested in companies. Some anonymous hacker groups want to give law firms a bloody nose. Others are interested in celebrities or political figures. Graham said that "e-mail is inherently insecure" and malicious malware is infectious. 7 different law firms in Canada were hacked after a big minerals takeover deal fell through causing a lot of damage. In 2011 a Toronto law firm was hacked by what it assumed were dissidents but it turned out to actually be about the business itself. The hackers were looking for databases and sensitive information.

Rosamund Urwin said there is a "dytopian undercurrent" to the internet, referencing the Secret web, which is the dark side of web[26]. This is hidden and used mainly by criminals. There is even a so called "Silk Road" – an e-bay of cybercrime – which facilitates drugs sent through the post. There are subscriptions for sale to law firm information believe it or not! Former employees who leave acrimoniously can also turn nasty online. According to Graham Cluley when a woman at one law firm was dismissed, the IT department did not change all her passwords. A male friend of hers planted malware and stole all the employees' passwords at the law firm. He did not cover his tracks properly and was subsequently arrested.

BYOD (Bring Your Own Device), Drop box and iPhones form another cyber security minefield so maybe the battleground analogy does hold. 47% of work devices are also used for personal stuff. People connect their own devices to company networks. Oversight is needed as confidential e-mails can get on personal accounts and sensitive data can get put in drop-box (a free service that lets you bring your photos, documents, and videos anywhere and share them easily according to its own publicity.) Well maybe a bit too easily and with the wrong people if things go awry! Graham recommended we think of the much trumpeted Cloud as "somebody else's computer" since it results in companies losing a lot of control over their data.

USB sticks can lead to secrets literally being dropped on the floor. As for public Wi-Fi, the security risks are huge. A company's data and its clients' data can easily be compromised according to Ashley Norris's article on the Telegraph Online, entitled, "Cyber security: are cafes safe workplaces?" (23 July 2014)[27].

Graham Cluley recommended that VPN software should be used to encrypt confidential data. A VPN is a virtual private network, an isolated subset of the Internet that allows for much greater security and privacy without sacrificing the Internet's ability to connect far-flung PCs and users together. VPNs have lots of uses, such as telecommuting into a corporate network, secure collaboration with others – even on the other side of the world and –

https://doi.org/10.1017/S1472669615000183 Published online by Cambridge University Press

private browsing. With a VPN, you can surf the Web anonymously and securely, leaving no traces. 13% of Yahoo webcam involves nudity.

WHAT ACTION CAN BE TAKEN?: Here are Graham Cluley's top tips for companies:

1. Use Anti-virus software. Although it is not completely effective against a targeted attack. Keep up-to-date and informed about threats.
2. Secure transfer and sharing of files. Encryption is important. If a deal ends – withdraw access.
3. If system hacked and sensitive info is encrypted it doesn't matter because hackers don't have the passwords.
4. Must have different password for each website. Graham has a programme with all his on it. He just has one master password. Without this if you get hacked there can be a domino effect.
5. Best to have 2 step ID system – password and then short random sequence of numbers.
6. Use VPNs
7. Be aware of website vulnerabilities
8. Only store what you need to store. If you erase data, do it securely.
9. Get data loss protection.
10. Nothing is 100% trustworthy. Managing is not eliminating.

Hackers are not usually after law firms per se. The=danger is the damage to clients' cyber security when hackers target them via their law firms. Cyber criminals know that law firms do not all have the best possible security precautions in place to protect customer data.

PLC magazine has a very useful article on litigation risk and liability from companies. Put briefly:

> "Cyber security represents a risk to almost every business and the increasing sophistication of third-party attacks is being matched by increasing regulatory scrutiny, both at a domestic and EU level. Leaving aside damage to reputation and loss of trade, organisations should be aware of the significant litigation risk that arises out of such incidents, and that risk may increase if the EU proceeds to implement a mandatory reporting regime[28].

Apart from the regulatory ramifications of data theft, a company that suffers a successful attack of this nature may be liable to its customers or suppliers under:

- Breach of contract: specifically, breach of an express or implied term that customer data would be stored securely and with due care.
- Negligence: specifically, a failure to take reasonable security precautions when storing customer information.

One way to minimise the potential for claims of this sort is to ensure that the cyber security measures of the business comply with current best practice.

In 2012, the Department for Business, Innovation & Skills (BIS) published guidance as to how businesses could best protect themselves from cyber attack but a recent survey revealed that only 30% of large organisations had used the BIS material. For the time being, companies should make sure that their own security measures incorporate what BIS currently regards as best practice[29].

An entity that is regulated by the Financial Conduct Authority (FCA) will also need to take into account the need to comply with the FCA Handbook, which obliges regulated entities to take reasonable care to establish and maintain effective systems and controls for compliance with the regulatory requirements. A listed company will also need to consider its general obligations under the Listing Rules.

In addition, listed companies may have a duty to disclose cyber security breaches to the market under Disclosure and Transparency Rules (DTR) 2.2.1R[30], which provides that an issuer must notify a regulatory information service as soon as possible of any inside information which directly concerns the issuer unless DTR 2.5.1R applies. Any assessment as to whether the event of the breach constitutes inside information will depend on its severity and the nature of the business affected: theft of business critical intellectual property is very likely to be price sensitive, whereas a minor disruption to ancillary services for a short time may well not be.

An issuer that publishes (or dishonestly delays publishing) material that fails adequately to disclose cyber security events, minimises their impact or downplays their significance, may also face claims brought by investors under section 90A of the Financial Services and Markets Act 2000, as well as proceedings in tort."

The third annual study by PwC and Iron Mountain to discover how European mid-market companies perceive and manage information risk revealed a gap between stated commitments and practical action[31]. The authors of the report felt that this not only contributed to a greater exposure to information risks, it also restricted the extent to which mid-market businesses can effectively utilise their information as a valuable and, potentially, a market-distinguishing asset.

CYBER-TERRORISTS THREAT TO SECURITY

The Prime Minister, David Cameron, announced (in July 2014) a £1.1billion investment in the military to tackle new threats to national security. The Prime Minister says that spending on "intelligence and surveillance" equipment, such as drones, is a "national necessity" and that the armed forces must adapt to deal with "unseen enemies". Mr Cameron, warned readers of The Daily

https://doi.org/10.1017/S1472669615000183 Published online by Cambridge University Press

Telegraph, that Britain faces changing threats in the form of global terrorism and unseen cyber criminals who can target the country from abroad. We "cannot defend the realm from the white cliffs of Dover", he said[32].

INTERNATIONAL PERSPECTIVE

The latest issue of the journal, Privacy and Data Protection picks up on a number of global events in cyber security[33].

Brazil – Internet Bill of Rights

The Bill was approved by the Congress on 25th March 2014, and then signed into Law by the Brazilian's President, Dilma Roueff, on the morning of 23rd April during an event in Sao Paulo dedicated to Internet Governance. The Bill starts by setting out the foundations of internet usage in Brazil, which include respect for freedom of expression, the protection of privacy, data protection as legally set out and maintaining and guaranteeing net neutrality. The Bill sets out what rights and guarantees are ensured for Brazilian internet users. The data protection provisions of the Bill appear to anticipate the future overarching data protection framework in Brazil.

Portugal: Largest Fine Ever in Europe–What Can We Learn?

The Portuguese Data Protection Authority (DPA) recently took a high profile enforcement action. In Portugal and other EU countries where the data protection regulator has not issued guidelines on specific information security measures, the first considerations for organisations when deciding how to implement or update their information security systems are to define what personal data are being processed and why, and where they are being processed.

US: New York Court order Microsoft to comply with a search warrant

Meanwhile on 25th April 2014, a New York court ordered Microsoft to comply with a search warrant to disclose a large amount of content, contact, payment and other data relating to an email account hosted in Ireland. The decision sheds light on the views of certain members of the US judiciary towards sovereign jurisdiction and, in particular, the extent to which a US court should be able to compel the production of data stored in servers overseas–in this case, in Dublin. Post-Snowden, European distrust of US surveillance laws is at an all-time high."

Goldman forces Google to block private e-mail

In July 'The Independent' reported that Goldman Sachs was granted a court order in the US requiring Google to block an e-mail containing confidential information which it send out by mistake. A contractor, who was testing a system upgrade, mistook a Goldman corporate e-mail account (@gs.com) and accidentally sent it to a random Gmail (@gmail.com) account. The Wall Street banking giant complained that the content of the e-mail would "inflict a needless and massive privacy violation" and cause it "reputational damage"[34].

EMERGENCY DATA RETENTION AND INVESTIGATION POWERS BILL

According to the BBC, the legislation will force mobile and landline providers and ISPs to record and store details of their customers' phone calls, emails, text messages and other communications for 12 months. By 'data', the bill does not refer to the content of the communications but the context, e.g. who communicated with whom and when i.e. the metadata. This data still remains sensitive and can demonstrate a range of nefarious, or merely private, communications and behaviours. The retention and disclosure of this data represents a continuing threat to privacy if it is accidentally disseminated or misused.

The legislation is being introduced so "UK law enforcement and intelligence agencies can maintain their ability to access the telecommunications data they need to investigate criminal activity and protect the public", Downing Street said. The terrorist threat in Syria and the danger posed by paedophiles have been cited by David Cameron as ongoing risks. The bill has cross-party support, even though the text of the bill has not been published and the government has not stipulated precisely what "communications data" will cover, describing it only as "metadata" about communications, not their content. This definition has proved problematic before, as the two can often blur in online communications.

The Data Retention and Investigation Powers Bill will include a 'sunset clause', whereby the powers given by the act must be reviewed in 2016. Whether this will be a Snoopers' charter albeit a watered down one, or vital measure to fight criminals remains to be seen.

The real trigger for this bill was the impact of the European Court of Justice judgment of 8 April 2014 in the joined cases of C-293/12 Digital Rights Ireland and C-594/12 Seitlinger. That judgment found that the Data Retention (EC Directive) Regulation 2009 (SI 2009/859), which the UK had up to now relied upon for these powers, was unlawful[35]. This bill is a case of clinging on to powers whilst trying not to fall foul of the obligations imposed by European law. The bill means that the state retains the power to compel any company providing communications services to UK customers to retain data for a period of up to 12 months and comply with requests from the secretary of state for the interception of that data.

Shami Chakrabarti, director of human rights campaign group, Liberty, has criticised the emergency data

https://doi.org/10.1017/S1472669615000183 Published online by Cambridge University Press

retention bill as a deal stitched up by the party leaders behind closed doors resulting in "no privacy for us and no scrutiny for them"[36]. Having said that we are promised the following:

- A new Privacy and Civil Liberties Oversight Board established to scrutinise the impact of the law on privacy and civil liberties;
- Annual government transparency reports on how these powers are being used;
- A restriction on the number of public bodies, including Royal Mail, able to request communications data under the controversial Regulation of Investigatory Powers Act (RIPA).

THE FUTURE

The European Commission has been considering a new Data Protection Regulation. The 'Right to be Forgotten' was to be discussed as part of this but the recent decision of the CJEU has now pre-empted this. The Court ruling has effectively put the data subject's interests above those of internet users in the majority of situations. Whether the EU sees fit to redress the balance remains to be seen[37].

Footnotes

[1] *Information Age*, June 2014, p.1
[2] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Case number C-131/12
[3] The BIALL Conference held in Harrogate on 11th to 14th June 2014 featured three speakers. Their talks are referenced here in this article. The talks were: Bradley, "Phil. Data, data everywhere". Delivered on 12 June 2014; Weckler, Adrian. "The New Gold Rush". Delivered on 12th June 2014; Blakeman, Karen. "The Brave New World of Free, Open Data and Open Access". Delivered on 11th June 2014.
[4] op. cit. 2
[5] http://www.theguardian.com/technology/2014/jul/25/right-to-be-forgotten-google-wikipedia-jimmy-wales (accessed: 23 January 2015)
[6] http://www.telegraph.co.uk/technology/google/10945451/Google-asked-to-remove-over-250000-links.html (accessed: 23 January 2015)
[7] ibid
[8] http://www.independent.co.uk/life-style/gadgets-and-tech/news/right-to-be-forgotten-google-accused-of-deliberately-misinterpreting-court-decision-to-stoke-public-anger-9582985.html
[9] ibid
[10] ibid
[11] bid
[12] op.cit. 3
[13] http://www.solicitorsjournal.com/
[14] http://www.solicitorsjournal.com/news/personal-injury/claims-management/british-facebook-users-may-not-%E2%80%98like%E2%80%99-lack-legal-protection (accessed: 26 January 2014)
[15] ibid
[16] ibid
[17] http://www.telegraph.co.uk/culture/tvandradio/tv-and-radio-reviews/10817886/Blurred-Lines-the-New-Battle-of-the-Sexes-BBC-Two-review.html (accessed: 26 January 2014)
[18] Rosamund Urwin column, London Evening Standard Thursday 26th June 2014 "We must stop making light of online abuse"
[19] Ibid
[20] op.cit. 3
[21] op.cit 3
[22] Reported in the Tech Times, 27 July 2014
[23] David Haynes. Social Media and Risk. *CILIP Update*, June 2014
[24] Independent 25th June 2014: "Police fail to cope as half of crimes now go online" http://www.independent.co.uk/news/uk/crime/police-fail-to-cope-as-half-of-nonserious-crimes-now-originate-from-social-media-websites-9560836.html (accessed: 4 February 2015)
[25] http://www.standard.co.uk/comment/rosamund-urwin-we-must-stop-making-light-of-online-abuse-9564490.html (accessed: 4 February 2015)
[26] ibid
[27] http://www.telegraph.co.uk/sponsored/technology/4g-mobile/data-security/10983100/cyber-security-wifi.html (accessed: 4 February 2015)
[28] Simon Bushell, Gail Crawford and Tess Waldron. "Cyber Security: Litigation Risk and Liability". *PLC*, June 2014
[29] ibid
[30] ibid

https://doi.org/10.1017/S1472669615000183 Published online by Cambridge University Press

[31] The third annual study by PwC and Iron Mountain to discover how European mid-market companies perceive and manage information risk, 2014.
[32] http://www.telegraph.co.uk/news/uknews/defence/10965182/David-Cameron-pledges-1.1-billion-for-defence-to-fight-cyber-terrorists.html (accessed:4 February 2015)
[33] Privacy and Data Protection, 1 June 2014, *PDP* 14, 6
[34] http://www.independent.co.uk/news/business/news/goldman-sachs-wins-court-order-to-make-google-delete-confidential-email-sent-in-error-9581374.html (accessed: 4 February 2015)
[35] Dominic Crossley (Payne Hicks Beach). Privacy and/or security? First published online, and in print, in: *Law Society Gazette*, 11 July 2014
[36] ibid
[37] Dan Tench. Slipping the net. *New Law Journal*, 20 June 2014.

Biography

Jackie Fishleigh is Library and Information Manager at Payne Hicks Beach. She was President of BIALL in 2008–2009 and is a Fellow of CILIP. She is currently Chair of the Supplier Liaison Group of BIALL. Jackie recently spoke at both the PI and ARK Conferences on the topic of Big Data. Last autumn she also chaired the TFPL seminar on 'Data Protection and Privacy: Is it good to share?'.

Legal Information Management, 15 (2015), pp. 69–72

doi:10.1017/S1472669615000195

Current Awareness

Compiled by Katherine Read and Laura Griffiths at the Institute of Advanced Legal Studies

This *Current Awareness* column, and previous *Current Awareness* columns, are fully searchable in the *caLIM* database (Current Awareness for Legal Information Managers). The *caLIM* database is available on the Institute of Advanced Legal Studies website at: http://ials.sas.ac.uk/library/caware/caware.htm

The 'Cardiff Index to Legal Abbreviations' is available at http://www.legalabbrevs.cardiff.ac.uk/

CATALOGUING AND CLASSIFICATION

Gordon Dunsire 'RDA: Enabling Discovery of Content' (2014) October *CILIP Update* 36

Amy Hart, *RDA Made Simple: A Practical Guide to the New Cataloguing Rules* (Libraries Unlimited 2014)

COPYRIGHT

Jorgen Blomqvist, *Primer on International Copyright and Related Rights* (Edward Elgar 2014)

Susy Frankel and Daniel Gervais (eds), *The Evolution and Equilibrium of Copyright in the Digital Age* (Cambridge University Press 2014)

Alma Hales and Bernadette Atwell, *The No-nonsense Guide to Copyright in All Media* (Facet 2014)

Jingyi Li 'Copyright Exemptions to Facilitate Access to Published Works for the Print Disabled – The Gap Between National Laws and the Standards Required by the Marrakesh Treaty' (2014) 45 IIC 740

Marketa Trimble 'The Marrakesh Puzzle' (2014) 45 IIC 768