Locke Lord LLP

Data Protection NEWSLETTER

June 2014

Locke Lord's Data Protection Newsletter provides topical snapshots of recent developments in the fast-changing world of data security in the United States and Europe. For further information on any of the subjects covered in the newsletter, please contact one of the members of our data protection team.

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

Patrick J. Hatfield
Partner, Austin, Texas
T: (512) 305-4787
phatfield@lockelord.com

Bart W. Huffman
Partner, Austin, Texas
T: (512) 305-4746
bhuffman@lockelord.com

Topics:

1. Ground-breaking ECJ Judgment in Google Case over "Right to be Forgotten"

On 13 May 2014 the Court of Justice of the European Union (the "ECJ") ruled that Google must remove from its search results links to websites containing inaccurate, inadequate and/or out of date personal information on its subjects, even where that information has been legally published by a third party (such as a newspaper). This is a landmark application of the so-called "right to be forgotten" under the Data Protection Directive 95/46/EC.

The case[1] involved a complaint by Mr Costeja Gonzalez, a Spanish national, that when his name was entered into the search engine of Google, links to articles in La Vanguardia newspaper from 1998 were generated, detailing the home repossession proceedings brought against him at that time. Mr Gonzalez, therefore, requested that the Spanish Data Protection Agency (AEPD) require Google to remove these search results, arguing that the information was entirely irrelevant as the proceedings had been fully resolved for a number of years.

In the ECJ's groundbreaking judgment, it held that people have the right to request links to *"inadequate, irrelevant or no longer relevant"* personal data to be removed. The judgment is somewhat unusual in that it represents a rare deviation by the ECJ from the Advocate General's (the "AG") opinion on this case produced on 25 June 2013. Although the ECJ is not bound by the AG's opinion, it is very unusual for the ECJ to deviate from it. The AG's opinion read that Google should not be considered a "data controller" for the purposes of the EU Data Protection Directive 95/46/EC (the "Directive"), and, furthermore, that the Directive did not establish a "right to be forgotten" which Mr Gonzalez could rely on against Google.

The EU Justice Commissioner, Viviane Reding, welcomed the court's decision, saying it was a *"clear victory for the protection of personal data of Europeans"*. Similarly, in response to this judgment, the UK Information Commissioner's Office ("ICO") released a supportive statement: *"We welcome the extent to which it upholds the data protection rights of individuals and confirms the powers of data protection authorities to enforce these."*

Noting the risk of this decision, however, *Bloomberg* reports how the ruling may open the floodgates for tens of thousands of requests to have legal, publicly available information about individuals taken out of a search index or links removed from websites. It is also the first time a search engine has been forced to remove a link to information legally published elsewhere on the internet.

In response to the decision, Google has already launched an online request form allowing Europeans to ask for personal data to be removed from online search results. Google explains in the form how they will assess each individual's request: *"When evaluating your request, we will look at whether the results include outdated information about you, as well as whether there's a public interest in the information—for example, information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials."*

Google have not clarified the timeframe for when links to this information will actually be removed, and the ICO have emphasised that this judgment does not mean the information itself will be removed, only the link to in search results.

As of 3 June 2014, Google has apparently received an astonishing 12,000 requests for the removal of personal data from its search results.

[1] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González

2. Facebook controversy over acquisition of fitness-tracking app Moves

Facebook's latest acquisition of Moves, an app that tracks its users' movements, has raised concerns after Moves changed its privacy policy 11 days after the acquisition, the *Guardian* reports.

The makers of Moves, Finnish company ProtoGeo, originally announced that it *"will continue to operate as a standalone app, and there are no plans to change that or commingle data with Facebook."* Reportedly, after the acquisition Moves changed its privacy policy to allow it to share user data with its parent company, Facebook.

Moves, which according to ProtoGeo has been downloaded more than 4 million times for iPhone and Android phones, tracks users' walking, running and cycling activity, as well as the locations they have visited every day. Users who consent to Moves storing that data may have concerns about Facebook now owning it, as it can now (for example) use its users' daily routines for targeted advertisements.

3. eBay hacked

In May this year it was announced that in February and March eBay fell victim to a mass cyber attack where personal data of its 145 millions users was hacked, *Reuters* reports. eBay has since urged its users to change their passwords, after it was discovered that names, phone numbers, passwords, email and home addresses were amongst the information hacked.

eBay's Global Marketplaces Chief, Devin Wenig, commented that initially eBay did not believe that its customers' personal data had been compromised, but after an extensive forensic investigation and discovering the extent of the cyber attack in May this year, eBay "moved swiftly to disclose" the breach.

No financial or other personal confidential information has been found to have been accessed. As such, eBay has made no announcements of plans to compensate its customers.

The Guardian reports that the ICO is looking into the cyberattack and eBay's handling of its customers personal data.

4. Gold stars for Apple, Facebook, Google, Microsoft, Twitter and Yahoo!

The Electronic Frontier Foundation's 2014 privacy report reveals how the policies towards governmental data requests of the world's biggest tech companies' rank. The nine highest ranking companies (out of the 24 companies reported on), which were awarded six stars each, included Apple, Facebook, Google, Microsoft, Twitter and Yahoo!

The 6 requirements used to credit these companies with a star include:

- possessing a warrant for content;
- informing users about governmental data requests;
- publishing transparency reports;
- publishing law enforcement guidelines;
- fighting for user's privacy rights in Congress; and
- fighting for users' privacy rights in courts.

The Guardian reports how Apple and Yahoo! in particular were praised as best improvers by the EFF, and Facebook has jumped from only 1 star in 2011 to full marks this year.

5. ICO issues report on data security threats

In May this year the ICO issued a new report on IT data security threats and best practices to be followed by online service companies. The ICO issued the report after their investigations into recent data breaches, leading to monetary fines, revealed common flaws in online security practices. The report highlights eight of the most common computer security vulnerabilities, including the storage of passwords.

The report focuses on the seventh principle of the UK's Data Protection Act: *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

The top eight vulnerabilities highlighted in the report, aptly titled "Learning from the Mistakes of Others" includes:

- a failure to keep software security up to date;
- a lack of protection from SQL injection;
- the use of unnecessary services;
- poor decommissioning of old software and services;
- the insecure storage of passwords;
- failure to encrypt online communications;
- poorly designed networks processing data in inappropriate areas; and
- the continued use of default credentials including passwords.

Amongst the many recommendations the ICO made in this report, the advice surrounding protection of passwords advised businesses to ensure passwords are subject to "hashing"[2] and "salting"[3] procedures, making it harder for hackers to decipher passwords.

[2] A hash function is a one-way method which converts a password into a hashed value. When a user first registers with a service and provides a password this is hashed and only this hash value is stored. When a user returns and enters their password, the hash is freshly calculated then compared with the stored hash. If the two hashes match, then the user can be authenticated.
[3] A salt in this context is a string of random data unique to each user. The salt is used by combining it with the user's password, then hashing the result. Having a unique salt for each user prevents an attacker from successfully checking for matches across all the hashes, in turn slowing the overall attack down.

6. Canadian PM nominates next Privacy Commissioner

On 28 May 2014 the Canadian Prime Minister, Stephen Harper, nominated Daniel Therrien as the next Privacy Commissioner of Canada. This nomination has yet to be approved by the Senate and House of Commons of Canada.

Therrien is currently Assistant Deputy Attorney General of the Public Safety, Defence and Immigration Portfolio at the Department of Justice, and will replace Chantal Bernier, who has been serving as Interim Privacy Commissioner since December 2013.

The Privacy Commissioner, as an Agent of Parliament, oversees compliance with both the Privacy Act, covering the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act, Canada's private sector privacy law.

7. iPhone and iPad users hacked and held to ransom

Many owners of iPhones and iPads in Australia and the UK have had their Apple devices hacked, shut down and have received ransom demands of 100 Australian dollars to unlock them.

The Find My Phone app is designed to help owners find and protect their data by locating their missing Apple device and allowing them to remotely shut it down if stolen. Ironically, this feature has been utilised by the hackers, identifying themselves as 'Oleg Pliss', to lock the device screens, refusing to unlock them until they receive the ransom monies in a PayPal account.

David Emm, from digital security firm Kaspersky Lab, is reported in the *Guardian* as saying: *"It seems likely that cybercriminals gained access to Apple ID credentials, for example by using phishing emails targeting Apple IDs…By using the credentials to access an Apple iCloud account, the attackers can enable the 'Find My iPhone' service".*

Apple, however, have released the following statement in response to the issue: *"Apple takes security very seriously and iCloud was not compromised during this incident. Impacted users should change their Apple ID password as soon as possible and avoid using the same user name and password for multiple services."*

Apple users who had previously set a security passcode were able to unlock their smartphones, whereas those who had not set a passcode could reset their device by connecting it to a computer and restoring it from an iCloud backup.

8. Spotify: latest cyber attack victim

It was revealed at the end of May this year that the music-streaming service Spotify, with 40 million users worldwide, is the latest major tech company to be hacked.

In a statement released by Spotify, the company assures its customers that their investigation into the attack shows that only one Spotify user's data has been accessed, which did not include any financial information, yet as a safety precaution they will be asking certain users to re-enter their username and password.

Spotify reassures: *"We have taken steps to strengthen our security systems in general and help protect you and your data – and we will continue to do so. We will be taking further actions in the coming days to increase security for our users."*

In response to the hack, Spotify have introduced a new app which is mandatory for Android users to install if they wish to continue using the service. Other app versions of Spotify, such as those for Windows, Mac, iPhone, iPad and Windows Phone will not be required to update the app.

Return to **TABLE OF CONTENTS**