SLAUGHTER AND MAY

BRIEFING
JANUARY 2015

Data encryption: increasing confidence in the internet

The use of algorithms to convert information into unreadable cipher text is not a new phenomenon and yet recently encryption has become a frequent headline item, not just in the tech industry but also in the mainstream press. The relationship between users, encryption and the law is not always a comfortable one. By examining two recent developments in the world of encryption, this briefing considers whether encryption is a useful tool for the legislator or a potential thorn in its side.

RANKING SIGNALS – LEGAL IMPERATIVE?

In August, Google announced that it has started to use HTTPS as a light-weight ranking signal in its search algorithm.[1] By incentivising the use of encryption, Google's stated ultimate goal is to keep everyone safe on the web. Following the shockwaves of the Google v Spain decision[2], however, is Google's latest move fuelled less by a desire to protect its users from the threat of cybercrime and more by the need to protect itself from the potentially unpredictable reach of data privacy laws?

Given the costs of the Google v Spain decision[3], Google could be forgiven for taking a highly conservative approach to compliance risk mitigation. In its hotly debated decision, the European Court of Justice ('ECJ') held that by finding information (including personal data) placed on the internet by third parties, indexing and storing that information and making it available to internet users according to a particular order of preference, Google must be a data controller within the meaning of the Data Protection Directive 95/46/EC (the "**Directive**"). Article 17(1) of the Directive dictates that data controllers must implement appropriate technical and organisational measures to protect personal data. Is this a clue as to the real reasons for Google's latest encryption announcement?

Whilst Google has taken this legislative requirement on board in other areas of its business (such as its recent encryption decision in relation to its iCloud Storage)[4], it cannot be the case that Google is deemed to be a data controller of personal data while it sits on the relevant third party website. Controller responsibilities are only triggered when Google processes, indexes and stores elements of that data for its own purposes. Although a legislative imperative seems unlikely to be behind Google's pro-privacy move to prioritize encrypted websites, the reputational impact of the publicity surrounding the ECJ's decision is likely to have been a contributing factor.

Looking beyond the requirements of the data protection legislative regime, Google's decision to reward encryption must be seen as a commercial, business-orientated choice rather than an entirely public-spirited move. As noted in the European Commission's publication "Digital Agenda for Europe", Europeans will not engage in ever more

1 http://googlewebmastercentral.blogspot.co.uk/2014/08/https-as-ranking-signal.html
2 Case C-131/12 – Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.
3 Critics outraged as Google removes search results about top UK lawyer and US banker", *Independent*, 3 July 2014 – "the US firm reported receiving more than 41,000 in the four days following the ruling".
4 http://googlecloudplatform.blogspot.co.uk/2013/08/google-cloud-storage-now-provides.html

sophisticated online activities unless they can fully rely upon their networks.[5] Online retailing has been growing at an average rate of over 18% per annum globally over the last three years and the size of the global online market is estimated at approximately $580 billion.[6] It is, however, fundamental for the continued growth of the online community (and therefore, intermediaries such as Google), that users feel safe and secure when they connect online. As Brad Smith, general counsel for Microsoft recently observed, "Just as people won't put their money in a bank they won't trust, people won't use an Internet they won't trust".

In this vein, as an example of related legislative endeavours, the European Parliament recently passed Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "**eID**"). The eID is aimed at encouraging cross-border digital transactions by expanding the law around electronic signatures and establishing a general legal framework for the use of trust services. The opening recital to the eID recognises that building trust in the online environment is key to economic and social development. The recital goes on to say that a lack of trust makes consumers, businesses and public authorities hesitant to carry out transactions electronically. This is one example amongst many of the ways in which the European Union is legislating in an apparent attempt to provide a predictable regulatory environment to enable secure, electronic transactions.

The path of legislative reform, however, is rarely a sufficiently swift solution to technical needs and, in the incredibly fast-moving digital context, this lack of pace is particularly marked. As the world's largest internet company (by market capitalisation), Google finds itself in a unique position to use its commercial leverage to drive better behaviours and dictate higher standards without the red tape of the legislative process. By encouraging encryption and fostering trust in the online community, Google boosts the survival prospects of players within the global marketplace and as a result, its own success. Users recognise the value of search engine optimisation (the first page of Google accounts for 91.5% of traffic)[7] and so the "carrot" of an improved rating is a significant incentive. Therefore, whilst it would be unfair to characterise Google's altruistic rhetoric as a mere "front", there is clearly much to be gained for Google from increased confidence in the internet.

APPLES AND LOLLIPOPS – LEGAL IMPEDIMENT?

Google's interest in data encryption has also attracted attention recently in the context of its mobile operating system. Within days of one another, Apple and Google both announced that the latest versions of their operating systems, iOS 8 and Android 5.0 Lollipop respectively, would offer encryption as the default setting.[8] Announcing the decision, Apple CEO Tim Cook explained that the company believes that "a greater customer experience shouldn't come at the expense of your privacy". Crucially, Apple and Google will not retain the encryption keys and therefore, even if faced with a court order, it will not be technically feasible for the companies to hand over personal data to law enforcement personnel.

The decision has caused great alarm throughout the law enforcement community, particularly in the United States. Director of the FBI, James Comey, has described the move as "marketing something expressly to allow people to place themselves beyond the law"[9]. In contrast, privacy advocates have spoken out in support of the technology firms and pointed to other routes by which law enforcement officials may gain access to the necessary information,

5 "Digital Agenda for Europe: Communication from the Commission", 26 August 2010, pg. 5.
6 "Global Perspective on Retail: Online Retailing", *Cushman and Wakefield*, July 2013, pg. 7 and 15.
7 "The Value of Google Result Positioning", *Chitika Insights*, 7 June 2013.
8 http://www.apple.com/privacy/government-information-requests/ and http://www.android.com/versions/lollipop-5-0/
9 http://www.cbsnews.com/news/fbi-director-james-comey-on-privacy-and-surveillance/

citing the use of warrants for iCloud accounts, obtaining location information from phone carriers, employing wiretaps to acquire real-time information and collecting metadata.[10]

Dissatisfied with such options, Comey has lamented the inability of the law to keep up with the speed of technological change.[11] In the US, the Communications Assistance for Law Enforcement Act is now 20 years old and focuses on traditional telephony and mobile telephone services rather than internet-based communications. In the UK, the Regulation of Investigatory Powers Act 2000 ("**RIPA**") regulates the interception of communications by public bodies. Under section 49 of RIPA, a person in possession of an encryption key can be required to disclose the protected information in certain circumstances. In the event that the operators do not hold the encryption key, however, UK law enforcement officials find themselves in the same position as their US counterparts.

This collision of technology, privacy and the rule of law marks the challenges posed by encryption in the post-Snowdon era. Edward Snowdon himself described encryption as "defence against the dark arts in the digital age", suggesting that citizens should be able to enforce their liberties through technical standards.[12] The possibility of collaboration between technology firms and law enforcement seems bleak given the lack of consensus over the viability of a "golden key". Opponents of the encryption decisions have called for companies to invent such a key to enable police with a court warrant to decrypt a smartphone whilst security experts warn that there is no way of safeguarding a golden key from abuse. In the absence of such collaboration, it is likely that the legislator will need to step in to deal with the "going dark" problem and adjudge upon the need for mandatory interception capabilities in developed technologies.

CONCLUSION

These recent spotlights on encryption demonstrate how technology can be a useful adjunct to legislative efforts but, equally, can suppress its objectives. For companies such as Google and Apple, the use of encryption technologies is a powerful marketing strategy aimed at meeting the perceived needs of their users. Regardless of whether technology is working alongside legislation or at cross-purposes, however, there is one constant – technology is forever moving faster. The tremendous challenge for the legislator is in future-proofing legislation to ensure the law remains relevant and effective in this rapidly and constantly evolving digital environment.

This briefing was written by Rob Sumroy (Partner) and Laura Houston (Associate) from Slaughter and May's Technology Group. It was first published in e-commerce law & policy, November 2014.

10 "Your iPhone is now encrypted. The FBI say it'll help kidnappers. Who do you believe?", Trevor Timm for theguardian.com, 30 September 2014.
11 http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
12 "Snowden: Surveillance is 'setting fire' to the internet.", *BBC Echo Chambers*, 10 March 2014.