In the Age of Data Breach and Cyber Threat

A call for expanding corporate criminal liability

Working Paper

15 May 2017

Author: Hélène Le Nobel
Editing: Anita Clifford

This Working Paper shall be supplemented by a further Briefing Paper on the issue of data protection to be published by The White Collar Crime Centre

In the Age of Data Breach and Cyber Threat: A call for expanding corporate criminal liability

Working Paper

1. Introduction

The extent of the data breach problem

On 12 May 2017 at least 100 countries were hit with a coordinated cyber attack, affecting data held by major public organisations and hospitals, and global telecommunications companies. At the time of this paper being published, nothing is certain about the effect of the attack except for its large scale. Though early reports suggest it is one of the most threatening cyber attacks to date, both the recent French and US elections were the victims of email hacking. Leaving aside the treasure trove of potential illegality that it uncovered, that most famous of leaks, the Panama Papers, may also be conceptualised as a mass data breach. 11.5 million electronic documents were released into the public domain, containing personal data on the finances of individuals, including numerous public officials.[1] Some of the data dated back to the seventies. On an individual level, the private medical certificates belonging to world famous athletes Bradley Wiggins and Serena Williams were published after an attack on the databases of the World Anti-Doping Agency.[2]

Global events put into sharp focus the extent of the data breach problem. And on a national level, the hacking of TalkTalk has been sobering. In October 2015, personal information of more than 156,000 telecommunications customers was accessed. In 10% of cases bank account details and sort codes were involved. Subsequent investigations found that TalkTalk had failed to take even the most basic steps to protect the personal data of its customers. As a result, the company was fined £400,000 by the Information Commissioner's Office (ICO) which released an accompanying statement that did not mince words:

[1] International Consortium of Investigative Journalists, "Key findings: The Panama Papers by the numbers", *www.panamapapers.icij.org/blog/20160403-key-findings.html*, 3 April 2016

[2] Kenneth Olmstead & Aaron Smith, "Americans and Cybersecurity", Pew Research Centre, *www.pewinternet.org/2017/01/26/americans-and-cybersecurity*, 26 January 2017

"Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers."[3]

The ICO's comments are a reminder to companies that data protection should be taken seriously. And there is a case for this not just because of the potentially grave consequences of a mass data breach, but in the light of increased public concern about the safety of data and the need for any successful business to hold public trust.

Research shows that data protection is a growing concern among people in the UK. In 2015 over 7,000 persons across seven European countries were surveyed about their data privacy perceptions. 89% of UK respondents said that data security is an important factor when choosing a company to shop with or use, beating factors such as quality of the product (88%) and customer service (85%). Moreover, half of UK respondents expressed fear that their personal information was not safe in the hands of both public and private organisations.[4] Although research of this kind is on a relatively small scale and may appear abstract, the TalkTalk case practically demonstrates what can happens if consumers lose confidence in a company's ability to protect data. Immediately after the attack TalkTalk's profits more than halved and the company lost about 95,000 of its customers. A year later TalkTalk did manage to recover significantly, however this is reportedly down to an increase in security expenses and investment in retrieving customer trust.[5]

The growing need for companies to be more proactive when it comes to data breach prevention is also reflected by new EU Regulation. From May 2018, the General Data Protection Regulation (GDPR) will apply to all EU Member States. Two of its main aims are to protect data privacy of EU citizens and reshape the way organisations approach the issue. Not a new compliance framework, the GDPR does not force corporations to implement specific controls to prevent data breaches. Instead it provides an outline of requirements and stresses the need for companies to be able to demonstrate they have done

---

[3] Information Commissioner's Officer, "TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack", *www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack*, 5 October 2016

[4] Symantec, "State of Privacy Report 2015", *www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf*

[5] John Stillwell, "TalkTalk posts surge in half-year profits as efforts after cyber attack pay off", *Business Reporter*, 15 November 2016

everything within their power to secure personal data.[6] Failing to comply with the GDPR could result in a maximum penalty of 20 million euros or 4% of the company's worldwide turnover. With the UK out of the EU in two years' time, the long-term effect of the GDPR is uncertain. The ICO has called for the UK to adopt this new EU data protection legislation, despite the inevitability of Brexit.[7] Initially the UK will be bound by the GDPR automatically, but after the date on which Brexit takes effect it will depend on the negotiated relationship with the EU whether the GDPR will remain to apply. Either way, if it is to maintain business with the EU, the UK will have to give serious thought to ensuring its data protection legislation accords with the GDPR.

Why this matters

In the context of large-scale data breach, it can be easy to overlook the individual victim. However, the unlawful disclosure of personal information is not victimless crime. In most cases, an occasion of data breach involves an attack on an individual's privacy. The unlawful disclosure of data, for example, might lead to a person being harassed with unsolicited calls (i.e. intended to promote a service or product) or having their private health records potentially comprised such, as the May 2017 attack shows, it grinds the provision of health services to a halt. In more extreme situations, leakage could result in individuals becoming victims of crimes such as identity theft and credit card fraud.

And, of course, companies face harm. Revelations about unlawful data disclosure could result in high legal costs (through fines or lawsuits), reputational damage, restoration expenses and the loss of revenue for business because clients walk away. As an indicator, research among customers of banks and insurance companies from eight different countries recently showed that many trust these financial institutions with their data, but 74% would immediately switch their provider in case of a data breach.[8] It is therefore in the economic and commercial interest of businesses to take data protection seriously and to have strong security measures in place.

---

[6] Steve Mansfield-Devine, "Data protection: prepare now or risk disaster", *Computer Fraud & Security*, December 2016, p. 5

[7] Information Commissioner's Officer, "Transparency, trust and progressive data protection", *www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/transparency-trust-and-progressive-data-protection*, 29 September 2016

[8] Capgemini, "Just one in five banks and insurers confident they could detect a cybersecurity breach", *www.capgemini.com/news/just-one-in-five-banks-and-insurers-confident-they-could-detect-a-cybersecurity-breach*, 2 February 2017

Data leakage is not a new phenomenon. We tend to identify personal data with the digital environment of computers and cyber security, but in fact it comprises all kinds of recorded information. For example, a lawsuit file brought into court could contain personal data, as does an old-fashioned card index box at a clinic. However, the introduction of computers and especially the availability of connecting networks, have added a new dimension to data protection. It is nowadays even more important to safeguard personal information, because it could potentially be accessed from all corners of the world by sophisticated hackers, something recently recognised by the British Business Federation Authority:

> *"The TalkTalk incident is one of many that have happened and continue to happen. To consider it in isolation of others would be misleading. The overall context is complex and changing fast... The problem space is international."*[9]

Companies have an enormous responsibility in this respect, both towards their customers and themselves. A study conducted by Intel Security revealed that data loss among commercial organisations in 43% of the cases is caused by internal actors, and only half of it occurs accidentally. This alarmingly means that the other half is leaked intentionally.[10] Further, in the corporate world storing data is everything. Without keeping track of information about e.g. finances, projects, employees and customers it is impossible for a company to do effective business. Corporations increasingly rely on such data to measure business activities and engage in business intelligence benchmarking, which is needed to understand customer needs, enhance services, reduce costs, improve processes and boost profits. Moreover, the volume and complexity of personal information that is collected and stored by organisations increases the value of it exponentially.[11] In essence, data is the basis for all reporting (to, for example, regulators, financial professionals and shareholders) and therefore data storage belongs to the core tasks of every company.

However, it is an open question as to whether current legislation in the UK imposes sufficient pressure upon corporations to take action. In 2016 the UK government published a report following a cyber security breach survey of over 1,000 UK businesses. About 69% mentioned that cyber security is high

---

[9] House of Commons – Culture, Media and Sport Committee, "Cyber Security: Protection of Personal Data Online", *First Report of Session 2016-17 (HC 148)*, 20 June 2016, p.3

[10] Intel Security, "Grand Theft Data – Data exfiltration study: Actors, tactics, and detection", *www.mcafee.com/br/resources/reports/rp-data-exfiltration.pdf*, 2015, p. 3

[11] Intel Security, "Grand Theft Data – Data exfiltration study: Actors, tactics, and detection", *www.mcafee.com/br/resources/reports/rp-data-exfiltration.pdf*, 2015, p. 11

on their senior members' priority lists, but further research revealed that just 51% had taken the recommended steps to identify the digital risks they face, only 29% have formal written cyber security policies in place and a mere 10% have official incident management plans.[12] The numbers are surprising when it is considered that 24% had detected at least one cyber security breach or attack during the past year. The bigger the firm, the higher the chance they got targeted, with a percentage of 65% breaches among the largest firms.[13] The report further revealed that companies seemed to underestimate the cyber security risks they face. Those in the financial sector considered that they were more likely to be exposed than others, owing to the perceived higher value of personal financial data. Those outside of the financial sector agreed with this assessment. However, as the report states:

> *"Non-financial customer data are still valuable in an interconnected world where people often reuse the same passwords across sites and services."*[14]

The results of the survey, the aforementioned scandals and the introduction of the GDPR suggest that there is a case for companies in the UK being pushed to implement robust data protection measures. According to the UK government report, for cyber security to be taken seriously across all levels of a corporation, it is important for its board members to be engaged with the topic. This reflects the ICO's statement that cyber security is a boardroom issue. Nevertheless, overall the responsibility of the 'directing mind' has proven to be relatively uncommon.[15] This paper will thus now explore whether current legislation provides enough encouragement for companies to comply with data protection measures. Should there be an expansion of corporate criminal liability with regard to data breaches in the UK? In order to address the issue, first the current data protection legislation will be outlined. This will be followed by an examination of the efficiency of the legislation to ensure corporate compliance with data protection rules. The paper will finish with an analysis of the possibility to introduce a new 'failure to prevent' offence to enhance corporate liability.

---

[12] Dr Rebecca Klahr, Professor Mark Button et al., "Cyber Security Breaches Survey 2016 – Main Report", *www.gov.uk/government/publications/cyber-security-breaches-survey-2016*, May 2016, p. 1

[13] Dr Rebecca Klahr, Professor Mark Button et al., "Cyber Security Breaches Survey 2016 – Main Report", *www.gov.uk/government/publications/cyber-security-breaches-survey-2016*, May 2016, p. 4

[14] Dr Rebecca Klahr, Professor Mark Button et al., "Cyber Security Breaches Survey 2016 – Main Report", *www.gov.uk/government/publications/cyber-security-breaches-survey-2016*, May 2016, p. 9-10

[15] Dr Rebecca Klahr, Professor Mark Button et al., "Cyber Security Breaches Survey 2016 – Main Report", *www.gov.uk/government/publications/cyber-security-breaches-survey-2016*, May 2016, p. 26-27

2. Current corporate liability position with regard to data breaches in the UK

Sections 55 and 61 of the Data Protection Act 1998

The Data Protection Act 1998 (DPA) was passed to control the use of personal information by the government, organisations and businesses. Section 1 of the DPA defines personal data as any recorded information about a living individual, who can be identified by that data. In this respect it does not matter whether the personal data is held electronically, on paper or within audio, visual or digital records.[16] The DPA regulates the processing of such information, which is a very broad term and includes obtaining, recording and holding data. More sensitive information, like data about health, ethnic background and criminal records, bears a stronger legal protection than other personal data. Under section 1 DPA the person (or persons) who determines why and how personal data are processed, is called the data "controller."

The ICO enforces the provisions of the DPA. When a person or company has been found in breach of any of its obligations, the ICO may impose regulatory fines of up to £500,000 or initiate proceedings in cases where it is considered a criminal offence has been committed. The DPA contains multiple criminal offences, but it is section 55 that is particularly relevant to corporate liability. Under sections 55(1) and (3) of the DPA, a person commits a criminal offence if he knowingly or recklessly obtains or discloses personal data without the consent of the data controller, or procures such a disclosure to another person. Sections 55(4) and (5) prohibit a person from selling or offering to sell illegally obtained personal data. Apart from the ICO, proceedings for section 55 offences can also be instituted by the Director of Public Prosecutions. It is not possible to impose custodial sentences and as such there are no powers of arrest. DPA offences are only punishable by a fine.

Section 61 DPA extends criminal liability for offences that have been committed "with the consent or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity".[17] Accordingly, directors and others at a management level could be held liable for data breaches. Although this provision should be an extra incentive for board members to take data protection seriously, it does not create corporate criminal liability in itself. Section 61 merely results in the 'directing mind' being

---

[16] The Crown Prosecution Service, "Prosecution Policy and Guidance – Data Protection Act 1998", *www.cps.gov.uk/legal/d_to_g/data_protection*

[17] *Data Protection Act 1998*, section 61

guilty of the same offence as the company. To hold corporations responsible for DPA offences a different path needs to be followed.

Corporations do not have a mind in the way individuals do, and the presence of a mind is normally necessary to be prove knowledge, intent or negligence. Law in general provides for different techniques to attribute criminal liability to companies nonetheless. In the UK corporate liability could be invoked through the so-called identification theory, which means that in absence of a real mind the corporation's 'directing mind and will' needs to be identified. If successful, it can be established whether the company possessed the necessary *mens rea* to fulfil the requirements of the offence, after which it might be prosecuted. An alternative for this type of corporate liability is offered on the basis of the strict liability doctrine. Some crimes do not require a mental element to be proven. In these cases criminal liability will arise through the commission of unlawful acts by the company's employees and agents alone, no matter whether they were at fault or not. In a business environment strict liability offences are primarily directed at regulatory misconduct, such as violations of health and safety regulations. From a criminal law perspective, strict liability offences for corporations are still scarce. In recent years we have seen the introduction of merely two pieces of legislation that specifically provide for such crimes: the Corporate Manslaughter and Corporate Homicide Act 2007 ('corporate manslaughter') and the Bribery Act 2010 ('failure to prevent bribery'), which both lack a *mens rea* element. Therefore, at the moment it is only possible to establish corporate criminal liability for DPA offences through the identification doctrine.

Possibility to reform section 55 of the Data Protection Act 1998

Reform of the DPA is not a hot topic in the UK and even less so is the possibility of expanding criminal liability for corporations that are involved in a data breach. Instead, any discussion of reform has tended to focus on increasing penalties for individuals.

With the introduction of section 77 of the Criminal Justice and Immigration Act 2008 (CJIA) the British government created the possibility of expanding the range of sentencing powers available when sentencing an individual for data breach, in contravention of section 55 of the DPA. In practice this means that the Secretary of State is allowed to introduce custodial sentences with a maximum of two years. To date the section 77 CJIA powers have not been enforced, despite the fact that the ICO has repeatedly called for stronger deterrent measures than currently available:

"With so much concern about the security of data, it is more important than ever that the courts have at their disposal more effective deterrent penalties than just fines. People who break the criminal law by trading in other people's personal information need to know that they will be severely punished and could even go to prison."[18]

The ICO took this stance after the Isleworth Crown Court sentenced in the case of *R v Nagra* in early 2016. Ms Nagra, who worked as an administrative assistant of a car rental company, sold customer information to accident claims companies in order to enable them to make nuisance calls. She was found guilty of unlawfully obtaining, disclosing and selling personal data contrary to section 55 DPA. The Court imposed a fine of £1,000 (plus a small victim surcharge and prosecution costs), while Ms Nagra obtained £5,000 for selling the customer's records. At the time, the ICO noted:

"this fine highlights the limited options the courts have. Sindy Nagra got £5,000 in cash in return for stealing thousands of people's information. She lost her job when she was caught, and has no money to pay a fine, and the courts have to reflect that. But we'd like to see the courts given more options: suspended sentences, community service, and even prison in the most serious cases."[19]

It follows that there are calls for stiffer penalties for individuals who offend against the DPA. However, any discussion about expanding corporate criminal liability for data breaches still seems to be in its infancy.

The figures on DPA offences arguably support this. To date, all prosecutions initiated by the ICO under section 55 DPA have been directed towards individuals, rather than corporations. From 9 March 2015 until 14 March 2017 the ICO obtained 27 judgments in criminal cases: 11 for individuals (mostly section 55 offences) and 16 for companies. The latter comprised contraventions of section 17 (which is a notification offence, meaning that personal data must not be processed unless an entry in respect of the data controller is included in a register maintained by the ICO) and/or section 47 (the failure of a person to comply with an enforcement notice). Both are strict liability offences and therefore do not require the presence of a mens rea element, which facilitates prosecution of companies. In two of the corporate

[18] Information Commissioner's Office, "Information Commissioner repeats call for stronger sentences for data thieves", *www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/01*, 11 January 2016

[19] Information Commissioner's Office, "Information Commissioner repeats call for stronger sentences for data thieves", *www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/01*, 11 January 2016

cases the directors were prosecuted as well, one of which for the section 61 offence of having been involved in the company's wrongdoing.[20]

Sections 17 and 47 DPA comprise comparatively minor offences, which is demonstrated by the low fines imposed. In 12 of the 16 corporate cases the organisation got away with a penalty of less than £650. The other four penalties were between £1,250 and £5,000. The ICO also has the power to enforce monetary penalties of up to £500,000. Since the coming into force of this provision in 2010 until 10 March 2017 120 cases where settled with a fine, about half of them related to (semi) public organisations and the other half concerned corporations. Not all of the corporate penalties related to DPA offences. The ICO has the power to impose similar fines for breaches of the Privacy and Electronic Communications Regulations (PECR), which sits alongside the DPA. The PECR applies to organisations wishing to send marketing messages through electronic means or provide electronic communication services to the general public. Nuisance calls and sending unsolicited text messages are examples of behaviour that could be punished by the ICO. More than two-thirds of the aforementioned corporate penalties were imposed for PECR offences. This means that in merely a handful of cases the ICO imposed monetary penalties for corporate failure to comply with DPA obligations.[21]

[20] *www.ico.org.uk/action-weve-taken/enforcement*

[21] *www.ico.org.uk/media/action-weve-taken/csvs/1042752/civil-monetary-penalties.csv*

3. Efficiency of the current provisions of the Data Protection Act 1998

A choice between criminal and regulatory justice?

Data leakage is not always a result of companies not willing to safeguard people's personal data – arguably, often it is also due lack of knowledge or the underestimation of the risks the corporation actually faces. However, if corporations are rarely held responsible for data breaches, the question arises as to whether the UK's data breach legislation is fit for purpose. At its simplest, is the occurrence of data leakage a consequence of a lack of enforcement or is there a need to reform the DPA in order to enhance corporate liability?

Broadly speaking, there are two paths available to hold corporations responsible for the commitment of offences. First, there is traditional criminal prosecution, led by the Crown Prosecution Service (CPS) or other prosecuting bodies. The other option is to apply regulatory justice, which is an administrative process and does not involve a criminal court. With regard to enforcement of DPA provisions the ICO bears both powers. When a company or an individual has been found in breach of the DPA, the ICO has several options to enforce the law. The most far-reaching is the possibility of imposing fines of up to £500,000 and initiating proceedings where a criminal offence has been committed. Other measures the ICO may take are issuing undertakings (which commit an organisation to a particular course of action with the aim to improve DPA compliance) and serving both enforcement notices as well as so-called 'stop now' orders (which require an organisation to either take or the refrain from taking specified steps, also in order to ensure DPA compliance).[22]

Imposing sanctions on corporations, whether issued criminally or regulatory, has several functions. Most obvious is the potential for reputational harm when a a company's failures are publicly outed. This has a general deterrent value. Associated with this, is the message that is sent – namely, that overlooking data safety does not pay. By issuing sanctions, which bear additional costs in the form of procedural expenses, the incentive of financial gain is taken away. A last example comprises the realisation of a cultural change among board members. If a company or its management is sanctioned for data breach, this creates a stronger culture of integrity within businesses. Whilst companies cannot be jailed, stiff monetary penalties, the potential for corporate monitoring and even debarment can serve as a catalyst for change within businesses.

[22] *www.ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection*

However, is strengthening the criminal law in the area of data breach the answer? As Horder observes, criminal law by means of prosecution in courts should only be applied in cases of *"the most serious wrongdoing or for the persistent flouting of the law"*. Less serious misconduct and *"the accidental or careless creation of a threat thereof"* are often better off dealt with in a different way, such as by imposing civil fines or licence restrictions.[23] In other words, these cases might benefit from a regulatory approach. Both systems have their advantages and disadvantages. Some features of the criminal justice path are that it is often expensive to bring proceedings, takes time and requires a higher standard of proof. Notwithstanding this, it is arguable that when it comes to data breach, criminal law has a stronger deterrent effect than regulatory measures.

Parliamentary debate

The low number of regulatory sanctions for corporate data breaches and the complete absence of criminal convictions suggest that the limited risk of getting caught provide insufficient incentive for companies to do everything they are capable of to protect personal information. In recent years, this matter has attracted some parliamentary attention.

In May 2006 the ICO published a report about the unlawful trade in confidential personal information. Investigations conducted by both the ICO and the police revealed *"a pervasive and widespread industry devoted to the illegal buying and selling of such information"*.[24] Unlawful trade in personal data proved to be enormously lucrative, due to a flourishing market with active players from all levels of society (the press, insurance companies, solicitors, and financial organisations).[25] On a number of occasions the detection of section 55 breaches led to successful prosecutions of individuals, but the overall trend in these cases was the *"generally low level of penalties imposed"*.[26] The ICO explained that *"low penalties devalue the data protection offence in the public mind and mask the true seriousness of the crime, even within the judicial system. They likewise do little to deter those who seek to buy or supply confidential information that should rightly remain private. The remedy (…) is to*

[23] Jeremy Horder, "Deterring bribery: law, regulation and the export trade", *Modern Bribery Law – Comparative Perspectives*, Cambridge University Press, May 2013, p. 198

[24] Information Commissioner's Office, "What price privacy? The unlawful trade in confidential personal information", The Stationary Office, May 2006, p. 3

[25] Information Commissioner's Office, "What price privacy? The unlawful trade in confidential personal information", The Stationary Office, May 2006, p. 28

[26] Information Commissioner's Office, "What price privacy? The unlawful trade in confidential personal information", The Stationary Office, May 2006, p. 12

introduce a custodial sentence (…). The aim is not to send more people to prison, but to discourage all who might be tempted to engage in this unlawful trade, whether as buyers or suppliers."[27]

The report's call for additional penalties resulted in a series of parliamentary debates on the possibility of reforming section 55 of the DPA. In July 2006 the Department for Constitutional Affairs issued a public consultation paper asking for views on the possible introduction of custodial penalties for invidiuals. Among the respondents were government departments, legal practitioners, independent regulators and companies, with the majority agreeing that *"custodial penalties would be an effective deterrent, because it would demonstrate the legal importance of data protection compliance and the seriousness of the offence"*. Emphasis, however, was also placed on the need for enforcement.[28] During the course of debate, various Members of Parliament stressed the importance of being proactive in safeguarding personal data[29], alongside a general concern that the possible introduction of custodial penalties for breach of the DPA might have a *"chilling effect on the legitimate activity of investigative journalism"*, potentially contrary to Article 10 of the European Convention on Human Rights.[30]

Ultimately, concerns expressed about the impact on investigative journalism led to calls to completely remove the custodial sentences provision from the Criminal Justice and Immigration Bill, unless *"a satisfactory solution balancing the need to strengthen the protection of individuals' rights and respect for their privacy on the one hand, and freedom of expression of the press on the other"* could be found. A compromise was eventually reached by way of section 77, with the result being that the introduction of custodial penalties would be a matter for the Secretary of State and not enforced immediately.[31]

Almost a decade after the passage of section 77, the provision enabling a court to impose a custodial sentence for DPA breach has still not come into force. This has occasionally attracted criticism. In 2012 Lord Justice Leveson published a report entitled 'Inquiry into the Culture, Practices and Ethics of the Press'. As the title suggests, the focus of the report was on the regulation of journalism, but Lord Justice Leveson also considered the issue of data protection. Considering the effectiveness of the DPA, Lord

---

[27] Information Commissioner's Office, "What price privacy? The unlawful trade in confidential personal information", The Stationary Office, May 2006, p. 3

[28] Department for Constitutional Affairs, "Increasing penalties for deliberate and wilful misuse of personal data", *Response to Consultation – CP(R) 9/06*, 7 February 2007, p. 8

[29] House of Lords, *Hansard – Volume 690 (Columns 1516-1528)*, 26 March 2007

[30] Public Bill Committee, *Hansard – Criminal Justice and Immigration Bill (Columns 579-589)*, 27 November 2007

[31] House of Lords, *Hansard – Volume 700 (Columns 1531-1540)*, 23 April 2008

Justice Leveson concluded that the legal framework *"puts unnecessary and inappropriate barriers in the way of regulatory law enforcement and the protection of victims' rights"* and recommended, amongst others, to give effect to section 77 CJIA as soon as possible.[32] Despite repeated calls for action, to date the matter is still under consideration.[33]

The missing element

An analysis of recent parliamentary debates about data protection reveals that the sole reference to corporate responsibility was in the context of agreement that there ought to be no difference between the public and the private sector when regulatory fines are issued. In debate in April 2008, it was thought that restricting DPA sanctions to public institutions was too narrow, as data loss occurs within the public sector and companies alike: *"Citizens do not mind who lost the data; it is irrelevant to them. What is important is that it is their data that have been sold, lost or left on rubbish heaps and it is they who are affected by it."*[34] Notwithstanding this, the matter of corporate liability for data breach has not been the subject of any extended attention.

Arguably, one reason for this is the emphasis of individual liability owing to the difficulty with prosecuting companies in the UK. In the context of the DPA – and indeed corporate liability generally in the UK – there is a need to satisfy the 'identification theory', namely the need to identify a sufficiently senior person in the company who has committed all the elements of the offence. One element of the offence under section 55 of the DPA is that the unlawful disclosure must have been committed knowingly or recklessly. Within large companies the 'directing mind' (the directors and/or senior managers) is often not directly involved with all of the minutiae of running a business. The position is only made more complicated in larger companies where it is not uncommon for responsibilities to be subdivided among teams on a senior level, making it difficult to determine the individuals aware of misconduct among its employees. Furthermore, it can be challenging to establish whether a certain indiviudal possesses the full authority to act in the name of the Board and thus, the company. For these

[32] The Right Honourable Lord Justice Leveson, "An inquiry into the culture, practices and ethics of the press", The Stationery Office, November 2012, p. 23-24

[33] House of Commons, *Hansard – Volume 556 (Columns 241W-242W)*, 8 January 2013; House of Commons, *Hansard – Volume 564 (Columns 93W-94W)*, 10 June 2013; House of Commons, *Hansard – Volume 583 (Column 671W-672W)*, 2 July 2014

[34] House of Lords, *Hansard – Volume 700 (Columns 1536-1540)*, 23 April 2008

reasons, in a data breach case it can be difficult to establish that the 'directing mind' possessed the necessary *mens rea* to fulfil the requirements of the section 55 offence.[35]

[35] Stephen Gentle & Elly Proudlock, "The problems of creating criminal corporate liability in the investigation of fraud: establishing criminal responsibility at board level", *Serious Economic Crime – A boardroom guide to prevention and compliance*, White Page, 2011, p. 233-238

4. Introducing data protection into the 'failure to prevent' framework

Recent developments

The above begs the question: should the corporate liability framework in the DPA be reformed? In recent years, the UK has slowly moved away from the 'identification theory' of corporate criminal liability and towards a risk-based model. The template for this is the Bribery Act 2010 which, in section 7, provides that a commercial organisation will be guilty of a criminal offence if it "fails to prevent" bribery by persons associated with it. An associated person is someone performing services for or on behalf of the company and could e.g. be an employee, agent of subsidiary.[36] He or she can be prosecuted individually for other BA offences, but this is not essential. Accordingly, corporations can be held liable without an individual conviction. A complete defence is available to the company under section 7 where it can prove that it had or has adequate procedures in place, which are designed to prevent bribery. Alongside the Bribery Act 2010 is guidance published by the Ministry of Justice as to what 'adequate procedures' means. Six principles are referred to: proportionate procedures, top-level commitment, risk assessment, due diligence, communication and monitoring/review.[37]

In essence, section 7 imposes corporate responsibility on the basis of the strict liability doctrine. No mental element is required, and therefore the need to identify a corporation's 'directing mind' falls away. The commission of unlawful acts by its employees and agents alone will give rise to the company's criminal liability. Since the introduction of the new bribery model the government has considered several proposals for an expansion of the 'failure to prevent' regime with regard to other economic crimes. Passage of the Criminal Finances Act 2017 in April 2017 introduced a further failure to prevent offence, namely corporate failure to prevent the facilitation of tax evasion. The UK government also has just concluded a call for evidence on whether a new failure to prevent economic crime corporate offence should be created.

Given the direction of travel, could a 'failure to prevent' corporate liability model potentially work for data protection? At first glance, the occurrence of data breach seems altogether different from the economic crimes of corruption, bribery, tax evasion, money laundering and fraud. Schedule 17 (part 2) of the Crime and Courts Act 2013 contains a list of offences that could be included in the definition of 'economic crime'. Data breach is not on the list. However, it is possible to conceptualise data breach as

---

[36] *Bribery Act 2010*, section 8

[37] Ministry of Justice, "Bribery Act 2010 – Guidance", *www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf*, March 2011

an economic crime. A lucrative market exists for unlawfully obtained personal data, and the sale of personal information can be extremely profitable. One example is a case in which employees were making £70,000 a year on top of their regular income by selling customer's data to other companies.[38] Further, a data breach can fundamentally disrupt business and, depending on scale, the economy. To categorise data breach separately to economic crime misunderstands its consequences.

The benefits of introducing a 'failure to prevent' offence into the DPA

Ultimately, introducing a new corporate offence of failure to prevent data breach into the DPA would make it easier to successfully prosecute companies for data breaches. Similar to the bribery model, a complete defence ought to be available to companies able to demonstrate that they had adequate procedures and processes in place to safeguard against data breach.

Certainly, not all unlawful disclosure can be prevented. Some hackers may possess such highly developed computer skills, that they may be able to crack even the most sophisticated cyber security systems and it would be unjust to hold a company responsible for breaches they simply could not have foreseen. However, there is a strong case for all companies to consider the safety of the data systems proportionate to their size, the nature of their business and the type of personal information that they hold. In an age of cyber threats, it is not unreasonable to expect companies to take steps to safeguard against data breaches, and depending on their size and scale of their activities, ensure that their systems are up to date and their staff are properly trained in relation to the storage and processing of personal information.

There are more benefits though. As Alldridge notes in relation to the bribery model, a strict criminal liability provision would result in a shift from a reactive law enforcement model to a more proactive one. The first is based on the idea that the police, public prosecutors and criminal courts are responsible to act upon criminal incidents and therewith create a deterrent effect. The proactive model on the other hand is focused on the prevention of crimes. Introducing a 'failure to prevent' offence into the DPA would encourage companies to take up a more active role in enforcement of the law.[39] Obviously such third party involvement will be partly due to economic interests on the side of corporations, as they might avoid data breach penalties by taking a reasonable amount of measures to prevent the unlawful disclosure of information. However, this kind of proactive law enforcement might also help to realise

[38] Public Bill Committee, *Hansard – Protection of Freedoms Bill (Columns 95-100)*, 24 March 2011

[39] Peter Alldridge, "The U.K. Bribery Act: "The Caffeinated Younger Sibling of the FCPA"", *Ohio State Law Journal*, Volume 73:5, 2012, p. 1182

the much needed cultural change among the top levels of commercial organisations. It will increase awareness that the unlawful disclosure of personal information should be a top priority among corporations, especially in today's digital world.

All this is not to say that all companies who fail to prevent data breach should be readily prosecuted. As with the bribery model, there should be the possibility of deferred prosecution agreements. A deferred prosecution agreement can be settled between a prosecutor and a company under the supervision of a court. As noted by the Serious Fraud Office: "*They enable a corporate body to make full reparation for criminal behaviour without the collateral damage of a conviction (for example sanctions or reputational damage that could put the company out of business and destroy the jobs and investments of innocent people).*"[40]

Finally, the introduction of a new corporate offence of failing to prevent data breach is arguably not such a great leap. The concept of adequate procedures and safeguards when it comes to data protection is not a new one. Presently, the ICO is required to consider the adequacy of a company's security measures when faced with data breach matter that potentially will atract a fine. The ICO guidelines on fines states that, to justify a monetary penalty, the *"contravention must either have been deliberate or the data controller (…) must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it".*[41] Accordingly, the link between data protection and adequate procedures is already there.

Potential concerns

All this is not to say that the introduction of a new corporate offence in to the DPA is an obvious next step. Since the passage of the Bribery Act 2010, some have noted that the 'failure to prevent bribery' offence has not be proved as effective as hoped. They refer to prosecutors having been reluctant to invoke it, suggesting that a commitment to enforcing section 7 is lacking.[42] Still, the lack of bribery convictions should not necessarily bes een as a sign that the 'failure to prevent' model is not working. According to a recent OECD report *"private sector representatives at the on-site visit generally agreed that section 7*

[40] *www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements*

[41] Information Commissioner's Office, "Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998", The Stationery Office, 2015, p. 5

[42] Barry Rider, "Editorial", *Journal of Financial Crime*, Volume 24(1), 2017, p. 3

provides a very effective incentive for legal persons to adopt adequate corporate compliance measures and internal controls".[43] This is an encouraging remark, suggesting that the creation of a new corporate offence in the DPA modelled on that in the Bribery Act 2010 could incentivise corporations to take a more proactive stance towards personal data protection.

A different kind of concern, however, has been expressed in the US. In October 2016 the US Federal Communications Commission adopted the 2016 Privacy Order, aiming to protect the privacy of customers of broadband and other telecommunications services. One of the provisions of the Order contained an obligation for broadband internet access providers and other telecommunications carriers to *"take reasonable measures to protect customer [proprietary information] from unauthorised use, disclosure or access"*. The US Order has been stayed, owing to concerns that implementing reasonable measures and training employees will substantially drive up business costs, in turn creating an immense burdens on companies and the economy in general. In short, the fear in the US is that it will undermine economic growth.[44] In the UK similar opposition is likely. Recently, Rider highlighted the opposition to new corporate offences from businesses in the City of London:

> *"There are those who feel that, given the uncertainties that have been thrown up by Brexit, to impose on businesses a new and potentially serious threat of prosecution for failure to police the misconduct of those associated with them would be a bridge too far!"*[45]

It follows that the cost of improving and implementing new data protection processes cannot be ignored. However, it is arguable that existing legislation already requires companies to have sufficient safety measures in place. As outlined, if unlawful disclosure of personal data occurs, the ICO already has the power to issue a regulatory fine and one of the considerations is whether the measures in place were adequate. Accordingly, it is questionable whether the burden on companies would substantially increase if a new corporate offence were introduced or whether this is simply a common refrain. Associated with this, any uncertainty about what would consitute 'adequate procedures' in the context of data protection can be readily addressed by the issuance of government guidance.

---

[43] OECD, "Implementing the OECD Anti-bribery Convention", Phase 4 report: United Kingdom, *www.oecd.org/corruption/anti-bribery/UK-Phase-4-Report-ENG.pdf*, March 2017, p. 75

[44] Eric Lipton & Binyamin Appelbaum, "Leashes Come Off Wall Street, Gun Sellers, Polluters and More", *The New York Times*, 5 March 2017; Federal Communications Commission, "Order granting stay petition in part", *FCC 17-19*, 1 March 2017

[45] Barry Rider, "Editorial", *Journal of Financial Crime*, Volume 24(1), 2017, p. 3

Perpetrator or victim?

There is one final concern to address. As the very recent coordinated cyber attack on public and private organisations shows, companies are victims of data breach. Unlawful disclosure of data causes a company significant harm. While bribery and other economic crimes, if undetected, often benefit a company, data leakage is very likely to have the opposite effect. Rival businesses might walk off with important knowledge, companies could face reputational damage, data breaches could result in financial losses and compromised customers. Is it right then to expose a company to criminal liability for failing to prevent a data breach when the company itself is also fundamentally harmed?

This paper argues that the answer to this question is 'yes'. Recent research conducted among banking executives showed that only one in five are fully confident they could detect data breaches, let alone build up protections against it:

> "*While financial institutions, particularly banks, are spending a staggering amount of money securing their systems, the number and frequency of data breaches is still rising. The evolving nature of the threat and lack of clarity among leaders perhaps explains why, despite high levels of investment, 71% of organizations do not have a balanced security strategy nor strong data privacy practices.*"[46]

The above is only a small snapshot of the issue in a particular sector. However, this paper argues that there is a need for companies across the specturm to take data protection more seriously and that to do so, there is a need for stronger corporate criminal sanctions. In a digital age, companies hold an enormous volume of personal data and, indeed, require the data in order to effectively function. Ultimately, any concern that in a data breach case exposing a company to criminal liability would have the effect of merely punishing the innocent victim is misguided. A company that had adequate and up-to-date procedures and systems in place to ensure data safety would have a complete defence. The only companies that could be successfully prosecuted for failing to prevent a data breach are those that failed to take adequate safety measures.

[46] Capgemini, "Just one in five banks and insurers confident they could detect a cybersecurity breach", *www.capgemini.com/news/just-one-in-five-banks-and-insurers-confident-they-could-detect-a-cybersecurity-breach*, 2 February 2017

5. Conclusion

The purpose of this paper is to generate debate on whether corporate criminal liability should be expanded in the context of data breaches. Ultimately, it calls for consideration of a new corporate criminal offence of failing to prevent a data breach. Such an offence could be introduced into the DPA or otherwise in a standalone Act. Like the bribery model, deferred prosecution agreements could be available which would require companies to remedy their processes. Ultimately, an approach of this kind would recognise the immense harm that can be caused by data breach. It would also incentivise companies to proactively protect the data they hold, rather than react to the damage once it is done.