pdp JOURNALS

ISSN 2049-5307

Privacy & Data Protection

Volume 15, Issue 6 June 2015

Headlines

- US government human resources office hacked, p17
- Mandatory data breach notification introduced in the Netherlands, p.18
- Google and Max Mosley settle sex session images dispute, p.19
- Germany to get new data retention law, p.20

Contents

Graham — "we are going to need to do things differently"

The Head of the United Kingdom Information Commissioner's Office, Christopher Graham, has called for a more practical approach to data protection regulation, and has made several suggestions as to how that goal might be achieved.

Speaking at a Conference of European Data Protection Authorities, which this year was hosted by the UK regulator, Mr Graham said that DPAs needed to be pragmatic in order to be effective in meeting current challenges. "We are going to have to learn to do some things differently," he said.

Mr Graham said the best place to begin was by understanding what is expected by the people whose fundamental rights the data protection authorities are supposed to be defending.

He drew on findings from newly published research from his Office into what control and security UK internet users and their counterparts in Europe expect.

The report suggests several quite far reaching changes to the role of data protection regulators, and reveals the ICO's thinking on various issues.

In the report, the ICO asks whether DPAs should take a more proactive role scrutinising privacy notices for unfair terms so that 'the public doesn't have to'. It suggests mechanisms such as privacy seals.

The report also questions the extent to which regulators are equipped to assess the public interest in data sharing agreements. It says: "there is a question as to how far DPAs should go with this type of assessment, and [whether] we have skills and knowledge to properly make these assessments."

(Continued on page 17)

New US-EU data transfer agreement imminent

EU and US officials are close to reaching a new agreement for the transfer of personal data by organisations from the EU to the US, one US official has said.

Catherine Novelli, US Under Secretary of State for economic growth, energy and the environment, said the US government is "very optimistic that we are going to be able to come to an agreement soon on Safe Harbor" and that agreement would not take months to be reached.

"It's very important that we find ways to preserve data flows," Novelli said. "Because so much of this is business-to-business, and because of the cross-investment, we don't want to be shooting ourselves in the foot by hampering this economic activity."

The new agreement would replace the Safe Harbor framework, which is currently still in operation despite extensive criticism and doubts as to its effectiveness.

Commenting on the developments, European Data Protection Supervisor, Giovanni Buttarelli, said: "More than in

(Continued on page 17)

Expert comment

Bridget Treacy is a Partner at global law firm, Hunton & Williams — the views expressed are her own

In recent days, there have been reports that the body responsible for administering aspects of the UK NHS' care.data database, the Health and Social Care Information Centre, has been unable to manage the significant number of opt-out requests it has received. The wishes of NHS patients who did not want their data shared appear to have been overlooked, creating chaos that must now be resolved.

Independently of the NHS care.data issues, the European Data Protection Supervisor ('EDPS') recently published Opinion 1/2015 highlighting the challenges of mobile health data. Mobile healthcare promises to revolutionise health services, but to be effective, consumers must be confident that the personal data they provide are appropriately safeguarded and used in accordance with their wishes.

At present, sensitive personal data (which includes health data) are subject to additional safeguards under European data protection laws. However, in the lifestyle context it is not always clear whether particular data are health data, or even personal data at all. The growth of the so called 'wellness' market, and the processing of vast data sets to derive health related information about individuals, can be particularly challenging.

The EDPS Opinion should be seen as part of a broader European focus on eHealth. In 2014, the European Commission launched a public consultation on mobile health, and during its eHealth Week in May 2015, the Commission presented plans to develop an industry-led Code of Conduct for mobile health apps. The Commission is also identifying policy issues in the mobile health arena that will need to be addressed.

In offering its views on mobile health, the EDPS Opinion promotes transparency, better consumer choice (including a choice to limit any processing to the local device) and organisational accountability, backed by the stronger privacy framework of the Proposed General EU Data Protection Regulation. It also highlights a number of specific challenges that will need to be addressed.

One challenge is determining the nature of the data — i.e. whether the relevant data are personal data or sensitive personal data. The current EU Data Protection Directive (95/46/EC) does not define 'health data', although the term is defined within some Member States. If defined too narrowly, consumers' expectations may not be met, and their trust jeopardised. If defined too broadly, organisations may be too constrained in their use of data. A further challenge is allocating responsibility. Given the multiplicity of actors in the health data ecosystem, and the variety of roles they play, it is not straightforward to ensure that there are appropriate constraints on the use and re-use of data.

The impact of Big Data must also be considered. Big data allows connections to be made between apparently unconnected data sets, and in the mobile health context will enable links to be made between lifestyle choices and disease. It may also enable service providers to discriminate between customers and to engage in differential pricing based on ability to pay or need.

Another challenge is the potential for profiling and market distortion in this area. For some time there has been a concern that widespread collection of health data outside a medical context could result in profiling and discrimination, for example in an employment or insurance context. It is also of course essential to ensure the security of data in the mobile health context. Failure to do so will deter users and undermine confidence in mobile health apps.

Finally, as many apps and devices are distributed globally and the data they collect processed abroad, EU data transfer restrictions will needs also to be considered, and an appropriate transfer mechanism (such as model clauses) implemented.

Mobile health data processing is still in its infancy, and the challenges inherent in processing health and wellness data will become ever more complex as Big Data, interconnected devices and the Internet of Things evolve. Addressing these challenges will not be easy. Perhaps the most rudimentary consideration, however, is to ensure that individuals' wishes concerning their personal data are respected. The care.data project should be seen as a cautionary tale for us all, illustrating how easily consumer trust can be undermined when consumers' wishes are not taken into account.

Bridget Treacy
Partner at Hunton & Williams
btreacy@hunton.com

ICO's approach to cyber security — identifying trends and mitigating risk

Samantha Sayers and Sabba Mahmood, Fieldfisher, provide guidance on what to do to ensure adequate cyber security, drawing on recent fines from the UK regulator

The threat of a cyber-attack is now more immediate than ever. In 2014, we saw an increasing number of high profile attacks on a variety of organisations ranging from government departments to blue-chip companies. These attacks came with devastating consequences such as major service interruption, loss of confidential information as well as significant reputational and brand damage.

Last year also saw increased regulatory action being taken by data protection authorities for cyber security breaches, including by the UK's Information Commissioners Office ('ICO'). This served to reinforce that cyber security is of increasing importance not just to the general public, but also to the regulators.

This article provides a brief overview of the law in the UK on cyber security, and highlights key trends in recent enforcement action taken by the ICO for cyber security failings. We also offer guidance on what organisations can do to ensure they are appropriately prepared to deal with cyber-security risks.

What is cyber security?

In the UK, being 'cyber secure' essentially means ensuring compliance with the data security requirements in the Data Protection Act 1998. This means implementing technical and organisational measures to protect personal data, and mitigate any risks of their loss or damage, which can arise through threats to information systems.

Cyber-attacks can take many forms including the use of botnets, DOS and DDOS, spamming, pharming, phishing, spoofing, viruses, worms and Trojan horses. Attacks are becoming more and more frequent, and increasingly sophisticated. Aside from the clear reputational damage that could be suffered as a result of a successful cyber-attack, the regulatory ramifications and litigation risks are significant.

ICO's enforcement action for cyber security failures

The ICO has imposed fines on numerous organisations for a variety of data protection failures — including cyber security failures. Highlighted below are the key cases, and some of the common security flaws that organisations should watch out for if they want to avoid fines from the ICO.

Staysure

In February 2015, Staysure.co.uk ('Staysure') was fined £175,000 as a result of a cyber-attack the organisation suffered in late 2013.

Staysure, a specialist online travel insurer's website, had its website breached after hackers managed to exploit vulnerability in Staysure's server. This effectively created a backdoor to the website, allowing the hackers to view and modify the website source code and customer database.

At the time of the attack, Staysure's database contained approximately 3 million customer records which included a variety of details, ranging from name, date of birth and email addresses, to payment card data including CVV numbers. Although all of the data were at risk, the payment card data were primarily targeted by the attackers.

What is also important to note here is that by storing the CVV numbers of its customers, Staysure was also in breach of the Payment Card Industry Data Security Standard. It transpired during the ICO's investigation that Staysure had applied encryption to the payment card numbers within its customer database, but not the CVV numbers. So when the hackers gained access to Staysure's system, they were able to identify the keys used in encrypting the data and used this to decrypt the payment card numbers accessing more than 5,000 customer records.

There were three main reasons why the ICO imposed a relatively large fine on Staysure:

- Staysure had failed to put adequate policies in place and were in breach of the payment card standard by storing the CVV numbers;

(Continued on page 4)

(Continued from page 3)

- there was evidence of fraud having taken place, which was likely to cause substantial distress; and
- Staysure (due to its size and resources) ought to have been aware of the risks associated with payment card data and should have taken steps to prevent the contravention.

When fining Staysure, the ICO noted that the company had voluntarily reported the incident, cooperated fully with the ICO and taken remedial action to remove all payment card data from its systems to avoid future breaches.

Worldview

The ICO took a slightly different approach towards Worldview Limited ('Worldview'), which was fined only £7,500 in October 2014 for its failures.

Worldview provides a booking service for serviced apartments and hotels, and compared to Staysure is a smaller company. There was vulnerability in the code on one of the webpages on its website, which allowed the attacker to extract passwords from the website's blog database. The attacker then used the access information they had obtained to log into the blog tool and alter files. This allowed them to access the server as well as browse the file system and download and upload files.

In this case, although there was no evidence of fraud having taken place, the attacker still had unauthorised access to the system for 10 days, and for this reason the ICO issued a fine. In issuing the fine, the ICO found that Worldview had failed to:

- provide relevant security training to its staff; and
- sufficiently test the webpage for any security vulnerabilities.

The ICO took the view in this case that as the incident affected a relatively small number of individuals, a smaller fine was more appropriate.

The ICO also noted, as it had in the Staysure case, that Worldview had voluntarily reported the breach to the ICO, had fully cooperated with the investigation and taken substantial remedial action following the incident.

"the ICO will not always impose a lower fine where the breach affects a relatively small number of people, and it will take into account the nature of the data. The ICO will take a stricter approach where the data involved are of a particularly sensitive nature, as they were in the BPAS case."

Think W3 Limited and British Pregnancy Advice Service

Two other notable cases in 2014 concerned Think W3 Limited ('Think W3') and the British Pregnancy Advice Service ('BPAS').

In the Think W3 case, the ICO imposed a fine of £150,000 on the online travel services provider when its subsidiary's website login page was found to be insecure. The webpage was found to contain a coding error and had not been tested properly. So when the website was targeted in 2012, due to this vulnerability the attacker was able to bypass the login authentication process and accessed and modified files within Think W3's network, including their customer database and files used to process payment cards. The attacker managed to extract nearly 1.2 million credit and debit card records.

During its investigation, the ICO discovered many other failures that had led to the breach including the fact that Think W3 had failed to:

- properly test/review the security of the coding of its website;
- implement a suitable intrusion detection system;
- update anti-virus software; and
- implement a suitable security policy addressing technical security issues.

In comparison, the BPAS received an even larger fine of £200,000 in 2014 after an attacker used an automated tool to identify website vulnerabilities and gained unauthorised access to the BPAS' website content management system.

The BPAS was only alerted to the incident when staff noticed that the website had been defaced.

In this case, the attack was reported to the police due to the sensitive nature of the information that was accessed and the risks associated with the attack.

This case highlighted that the ICO will not always impose a lower fine where the breach affects a relatively small number of people, and it will take into account the nature of the data. The ICO will take a stricter approach where the data involved are of a particularly sensitive nature, as they were in the BPAS case.

Sony

No article on the ICO's enforcement actions would be complete without mentioning the £250,000 fine imposed on Sony in 2013 for its security breach.

The case was highly-publicised and brought cyber security issues to the forefront of consumers' minds.

The hack of Sony's PlayStation Network Platform was taken particularly seriously by the ICO due to its nature and the volume of data involved, as the hacker had compromised the personal data of millions of Sony customers around the world, not just in the UK.

At the time, David Smith (the ICO Deputy Commissioner) commented: "There's no disguising that this is a business that should have known better. It is a company that trades on its technical expertise, and there's no doubt in my mind that they had access to both the technical knowledge and the resources to keep this information safe".

This comment clearly illustrates that the ICO has higher expectations of large organisations such as Sony, which have the necessary resources to prevent breaches.

Key trends and risk mitigation

It is clear from the cases that the ICO has certain expectations of data controllers that suffer cyber security breaches. The ICO's expectations will vary depending on:

- the nature of the data involved (e.g. whether the incident concerned sensitive personal data);
- the volume of the data involved;
- the number of individuals affected by the incident; and
- the data controller's size and technical expertise.

Across its enforcement actions, it is clear that the ICO expects organisations to implement technical and organisational measures to mitigate the risks to their data and information systems. In order to prevent a breach happening, the ICO recommends that organisations:

- review and regularly update their IT infrastructure to ensure they have the latest security patches, and websites are tested for any vulnerabilities;
- implement appropriate security measures to protect the personal data from vulnerabilities such as encryption;
- have a good understanding of the data flows both within the organisation and between them and external third parties;
- put in place comprehensive data protection and data security compliance frameworks, which include an information security policy;
- provide relevant data protection and data security training for all personnel (including website/code developers);
- ensure that any contracts with third parties processing data on behalf of the organisation have robust provisions on data protection and data security; and
- are prepared for when things go wrong and that they have a robust incident response plan in place to mitigate risk.

Once a cyber-attack occurs, the key recommendation from the ICO is to ensure that the relevant website/system/server is locked down in order to prevent further disclosure, loss and/or destruction of data.

Conclusions

The ICO is increasingly taking action for cyber security breaches and will expect organisations with sufficient resources to take appropriate remedial action — both to prevent a breach occurring, and to take measures to contain a breach after it has occurred.

If an organisation does fall victim to a cyber security attack and is subsequently investigated by the ICO, data controllers should cooperate fully with investigations.

As has been demonstrated in the cases discussed in this article, cooperation with the ICO will inevitably count in an organisation's favour, and may perhaps deter the ICO from imposing a larger fine.

Samantha Sayers and Sabba Mahmood
Fieldfisher
samantha.sayers@fieldfisher.com
sabba.mahmood@fieldfisher.com

Data sharing agreements — avoiding common pitfalls

Heledd Lloyd-Jones, Partner at Blake Morgan LLP, considers common pitfalls that can arise when using data sharing agreements to govern the transfer of personal data and suggests how these pitfalls may be avoided

Data sharing continues to be a high risk activity for many organisations. In 2013-2014, errors in data sharing and disclosure accounted for 17% of complaints to the UK Information Commissioner's Office ('ICO') and approximately 45% of ICO enforcement action.

Risks for data controllers of inappropriate or insecure data sharing and disclosure include monetary penalty notices and ICO enforcement action, civil claims and reputational damage. These risks are likely to increase in future as a result of increased sanctions for data breaches under the proposed EU General Data Protection Regulation, and as a result of strengthened rights for data subjects seeking to recover compensation for distress following the judgment of the Court of Appeal in *Vidal-Hall v, Google Inc [2015] EWCA Civ 311.*

Data sharing agreements are often used to minimise risks associated with data sharing. Use of data sharing agreements in appropriate circumstances is recommended in the ICO's statutory Data Sharing Code of Practice (copy available at: www.pdpjournals.com/docs/88438) and when investigating complaints the ICO will take the use of data sharing agreements into account.

However, data sharing agreements will not be suitable in all cases, and the use of template agreements on a 'one size fits all' basis can introduce unwelcome confusion. Data sharing agreements that impose unnecessary restrictions on data recipients may even operate to the detriment of disclosers.

So when is it appropriate to use data sharing agreements? What should they contain? What are the benefits and what, if any, are the potential drawbacks?

When should data sharing agreements be used?

Despite their playing a valuable role in supporting DPA compliance where personal data are disclosed to, or shared with, third parties, the use of data sharing agreements is not mandatory under the UK Data Protection Act 1998 ('the DPA').

Firstly, it is important to distinguish data sharing agreements which may be used to support outright disclosure to third parties or collaborative data handling projects, and data processing agreements which must be used when data processors are engaged by data controllers to process personal data on their behalf (as required by Schedule 1, Part II, para 12 DPA).

Secondly, it is worth noting that data sharing agreements are unlikely to be useful in cases involving one off or ad hoc disclosures of personal data, unless those data are particularly sensitive or voluminous. It is important in all cases that a data controller retains a record of its decision-making insofar as the decision to disclose is concerned, and ensures appropriate and proportionate security measures (e.g. tracked delivery, password protected email, prearranged use of a secure fax facility or the use of a secure IT platform) are used to govern transfers. In cases involving the ad hoc disclosure of personal data that is of limited sensitivity, the use of a formal data sharing agreement is unlikely to be helpful, and may simply serve to introduce delay and an unwelcome bureaucratic burden. In such cases, an internal data sharing checklist for audit purposes is likely to be more suitable.

Where data sharing agreements can perform a valuable function is where organisations are involved in the systematic or frequent disclosure or exchange of information, or where they are involved in collaborative projects that will involve the pooling and further use of personal data for joint purposes.

What should data sharing agreements contain?

In order to decide what provisions should feature in a data sharing agreement, it is essential to be clear about the purpose, or purposes, that the agreement is intended to achieve.

Broadly speaking, data sharing agreements can support data sharing activities in three different ways.

Firstly, data sharing agreements afford an opportunity for the discloser and the recipient to set out the basis on which they consider themselves entitled to share personal data — that is, the basis upon which the transfer is considered to

meet the requirements of the First and Second Data Protection Principles (fairness and lawfulness, and lawful purposes).

Secondly, agreements can be used to record the technical and organisational steps that the parties agree to follow to ensure the secure transfer of personal data from one to the other to minimise the risk of loss, degradation or interception in transit and secure safe delivery. In this way, agreements can play an important role in supporting compliance with the Seventh Data Protection Principle (data security).

Thirdly, agreements can be used to detail arrangements that will be applied jointly by two or more parties to data that are shared or pooled for a continuing joint purpose. The use of an appropriate data sharing agreement in this context will assist both parties to comply with the full range of their obligations as data controllers insofar as jointly held data are concerned, and may assist them to allocate responsibility (and possibly liability) between themselves for specific data handling activities.

Compliance with the First and Second Principles

In order to comply with the First and Second Principles when sharing personal data, it is usually necessary for the parties to be satisfied that the proposed disclosure is fair and lawful and is made for a purpose that is compatible with the purpose for which the data were originally obtained. It is also usually necessary for the parties to be satisfied that at least one condition from Schedule 2 of the DPA applies, and in the case of sensitive personal data, that at least one condition from Schedule 3 of the DPA also applies.

In many cases, this decision-making process will involve a fairly straightforward analysis, based on the information supplied to data subjects at the time their data were first obtained, along with assurances from the proposed recipient regarding its intended use of the data that are to be transferred.

"In the case of systematic data sharing between two or more organisations, as well as in the case of one off disclosures of voluminous or highly sensitive personal data, data sharing agreements can operate as important organisational measures to manage and reduce the risk of loss, degradation or interception of data in transit."

In cases where data are to be transferred outright and data subjects have been made aware of, or have consented to, the proposed transfer, and the recipient is itself subject to the DPA, it may be unnecessary and in some cases will be inappropriate to seek to impose restrictions on the data recipient insofar as the future handling of transferred data are concerned.

For example, in cases involving the transfer of personal data to statutory agencies who will be using transferred data for the purpose of their statutory functions, attempts to impose restrictions on their subsequent use of the transferred data may well introduce an unwelcome element of confusion, and suggest a continuing acceptance of responsibility on the part of the discloser for data following transfer, contrary to the intentions of the parties.

In order to avoid the appearance of on-going responsibility for personal data that have been transferred outright to a third party, data controllers that are considering making an outright disclosure should exercise caution when seeking to impose restrictions on the future use of such data by data recipients.

The imposition on the recipient of obligations in relation to, for example, the handling of subject access requests, or data security breach reporting, or the use of data processors, is unlikely to be consistent with the notion of an outright data transfer, and may suggest a continuing responsibility on the part of the discloser for the personal data following transfer to the recipient.

It does not necessarily follow that conditions attached to outright data transfers will not be appropriate in such cases. In certain instances, a disclosing data controller may conclude that it can only be satisfied that disclosure will comply with the First and Second Principles if certain assurances are given in relation to the future handling of transferred data.

For example, a disclosing data controller may take the view that disclosure will be fair only if the recipient provides an assurance regarding the purposes for which it intends to use the data that are to be disclosed, or if the recipient agrees to retain the data only for a prescribed period of time or agrees to apply specified security standards to the data once those data have been received. Similarly, a disclosing data controller might conclude that disclosure will be unfair unless data subjects are expressly informed about the transfer, and might therefore seek to impose an obligation on the recipient controller to notify all affected data subjects.

To the extent that assurances of this kind are required by a disclosing data controller in order to decide whether personal data may be shared fairly and lawfully, the inclusion of provisions in a data sharing agreement requiring the recipient to give assurances regarding its proposed use of data following transfer will clearly be appropriate. Reasons for including such assurances should, however, be clearly stated, and disclosing data controllers should avoid imposing unnecessary obligations on recipients in relation to future data handling, especially where this may be sugges-

(Continued on page 8)

(Continued from page 7)

tive of a continuing responsibility for data protection compliance following transfer.

Applying the Seventh Principle to data in transit

In the case of systematic data sharing between two or more organisations, as well as in the case of one off disclosures of voluminous or highly sensitive personal data, data sharing agreements can operate as important organisational measures to manage and reduce the risk of loss, degradation or interception of data in transit. Data sharing agreements can therefore support, and demonstrate compliance with, the Seventh Data Protection Principle which requires that '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.'

In the case of outright data transfers, it is very much in the interests of the disclosing data controller to ensure that arrangements governing the security of data in transit are robust and to impose obligations on the recipient of the data that ensure that the activities of the data recipient do not jeopardise the reliability of these arrangements. The receiving party will also have an obvious interest in working with the discloser in the interests of ensuring the integrity of data in transit and safe receipt.

Appropriate provisions for inclusion in most data sharing agreements will therefore typically include provisions designating agreed means of communication, arrangements for the management of passwords for the purposes of encrypted email, mobile devices and data sharing platforms, and arrangements for auditing compliance and keeping the effectiveness of relevant security mechanism under review.

Supporting compliance in the case of joint projects

Where personal data are shared or pooled for the purpose of collaborative projects in which two or more parties will have continuing responsibilities under the DPA for shared data, data sharing agreements can take on an entirely different significance. Agreements in such cases set out not only the basis upon which data sharing is considered fair and lawful and the mechanisms necessary to ensure secure transfer, but detail arrangements that will apply to the future joint handling of the data to be shared. In these circumstances, data sharing agreements can play a vital role in identifying and addressing particular privacy and compliance risks arising from the data sharing project, and in allocating responsibility for different aspects of data handling between the parties.

It is in the context of such joint projects where the parties may have joint and several liability for data protection compliance in respect of shared data, that it will often be advisable to agree mechanisms for managing a wide range of compliance issues, including the handling of subject access requests and complaints, the management of data security breaches, the retention and disposal of shared data, the periodic review of shared data to ensure accuracy and relevance, the selection and management of processors and arrangements for international transfers.

Where data are shared or pooled for the purpose of collaborative projects and one party assumes the day-to-day responsibility for certain aspects of data handling, for example data collection or data security, it will usually be advisable for this assumption of responsibility to be expressly reflected in the data sharing agreement.

The ICO has indicated that where joint data controllers have allocated responsibility for specific aspects of data handling between themselves, such agreement will be taken into account in the event that an ICO investigation of a complaint or alleged breach proves necessary. Given that joint data controllers may have joint and several liability for losses arising from DPA breaches, it may also be advisable to include indemnity provisions where relevant, so that each party has some protection from claims or penalties resulting from failure on the part of the other party or parties to follow agreed processes.

Conclusion

Data sharing agreements clearly have an important role to play in supporting data protection compliance and minimising risk for both data subjects and data controllers. But they should always be approached with care and with a clear understanding of the purposes they are intended to fulfil.

As the ICO Data Sharing Code of Practice makes clear, 'drafting and adhering to an agreement does not in itself provide any form of legal indemnity from action under the DPA.' They are not always necessary and the use of a poorly thought out agreement will not operate to perfect otherwise defective data sharing arrangements. Where they are used, care should be taken to ensure agreements are clearly drafted and reasons for the imposition of any continuing obligations are readily justified.

Heledd Lloyd-Jones
Blake Morgan LLP
heledd.lloyd-jones@blakemorgan.co.uk

Cross device profiling — ensuring compliance

Bridget Treacy, Partner, and James Henderson, Associate, consider the compliance issues that arise from the use of techniques and algorithms enabling cross device profiling, and explain how organisations can ensure that they are sufficiently transparent with their use

Cross device profiling, the range of techniques that allows individual users to be identified across different devices and platforms, is now commonplace. In the past, organisations have relied on cookies and similar technologies to identify users. As the mobile ecosystem has become more sophisticated, and service offerings have been deployed on new platforms, organisations have turned to newer technologies to enable them to identify individual users across those platforms. It is now common for users to access a single service through multiple platforms, for example, a smartphone, tablet, laptop, and even smart televisions. Through cross device profiling, organisations can identify and target individual users more accurately than ever before, and provide increasingly personalised services.

However, the techniques and algorithms utilised to enable cross device profiling are often less than transparent, raising complaints from individuals that such practices are 'creepy' or intrusive. Such techniques have only recently begun to receive specific regulatory attention, but as awareness of individuals' privacy rights continues to grow, and those rights are further enhanced by the proposed General Data Protection Regulation, companies deploying these techniques will need to consider whether their practices are sufficiently transparent.

Accuracy of deterministic or probabilistic techniques

Organisations typically employ a range of techniques to achieve cross device 'identifiability'. These techniques may be deterministic (i.e. where the organisation uses a unique identifier to identify the user when he or she uses different devices) or probabilistic (i.e. where the organisation, typically through a combination of techniques, infers the identity of the user in question, through a range of factors and characteristics associated with his or her device or usage, such as IP address range, past browsing history, etc.).

Many profiling techniques will employ both deterministic and probabilistic methods. Commentators estimate that most probabilistic techniques have a level of accuracy of between 60-80%. This means in 20 — 40% of cases, organisations associate a range of inferred characteristics and behaviours with the incorrect user. Over time, these accuracy levels will undoubtedly improve, but the risks of error that currently exist make it imperative that organisations think carefully about data protection compliance now.

Data Protection Directive

The Data Protection Directive (95/46/EC) regulates the processing of 'personal data' by 'data controllers' that are established in the EU or employ equipment based in the EU for the purpose of processing personal data. If each of these three elements applies, then an organisation performing cross-device profiling will be subject to the compliance obligations set out in the Directive.

Are personal data being processed?

The definition of 'personal data' in the Directive captures any information that relates to an individual and which identifies an individual, or from which an individual may be identified. This definition is extremely broad and captures expressions of opinion about an individual, as well as factual statements, provided the information identifies the individual or the individual can be identified from the data.

Deterministic profiling measures typically utilise a unique identifier that is tied to a particular identified individual. Such an identifier clearly allows the particular user in question to be identified and singled out (indeed, this is the intention of profiling). Accordingly, that unique identifier, as well as any other data linked to that identifier (e.g., devices, IP address, browsing habits and history) will constitute personal data.

Probabilistic profiling techniques typically analyse vast sets of data

(Continued on page 10)

(Continued from page 9)

to identify particular users from that data. Once tied to a particular known (or suspected) individual, that data will constitute personal data. It should be noted that the data in question will also constitute personal data even if they are associated with the incorrect individual, provided an individual can be identified from those data.

Is processing conducted by a controller?

The second requirement is that the organisation conducting the profiling is a 'data controller' within the meaning of the Directive.

A data controller is a person who 'determines the purposes and the means of the processing of personal data'. Organisations that perform cross device profiling typically are data controllers, but organisations may perform cross device profiling on behalf of another website or service operator — in which case the website or service operator will be the data controller. Care is required to determine which entity is the data controller, and has the applicable legal compliance obligations under the Directive.

EU establishment

Assuming that an organisation processes personal data in the capacity of a data controller, the organisation will be subject to the Directive if it is established within the EU, or if it utilises equipment within the EU for the purpose of processing personal data. Organisations that are located within an EU Member State (either by a legal entity established in that jurisdiction, or some other physical presence) will be subject to the Directive as implemented in that Member State. It should be noted that the 'use of equipment' test is interpreted widely, and the mere placing of cookies on a user's equipment is likely to bring a non-EU data controller within scope of the Directive, even if they have no physical presence in the EU.

"In many cases, the nature of the profiling and the techniques deployed may not be transparent or understandable to data subjects, raising the risk that any consent is invalid. For consent to be valid, users must be given a genuinely free choice as to whether they are tracked, or not."

Legal basis for processing

Data controllers must satisfy one of the processing conditions set out in the Directive. In the context of cross-device profiling, the relevant conditions are consent, and the legitimate interests of the data controller. The contractual necessity ground will not usually be applicable, unless cross-device tracking is strictly necessary for provision of the service. This is a strict test, and will not apply to cross-device tracking carried out for purposes that are not strictly necessary, for example for the purpose of providing personalised services.

In many cases, organisations seek to rely on consent as the legal basis for cross-device profiling. The Data Protection Directive does not dictate the form by which consent is obtained, but consent must be freely given, specific and informed. This requirement has been interpreted differently across the Member States. In some jurisdictions, forms of implied consent (such as 'banner' systems deployed in the context of cookies) may be valid, and in some cases valid consent maybe obtained through web browser settings.

In the context of cross-device profiling, the key consideration is to ensure that data subjects are fully aware of what they are consenting to. Organisations should explain, in a user friendly and transparent manner, why profiling techniques are deployed. This is particularly important where the profiling techniques deployed may have a significant impact on the privacy of individuals or otherwise significantly affect them, for example, where differential pricing is used. In many cases, the nature of the profiling and the techniques deployed may not be transparent or understandable to data subjects, raising the risk that any consent is invalid. For consent to be valid, users must be given a genuinely free choice as to whether they are tracked, or not.

Alternatively, controllers may rely on their legitimate interests as a basis for cross device profiling, provided such legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject. The Article 29 Working Party has published an Opinion (copy available at: www.pdpjournals.com/docs/88446) on legitimate interests in which it set out a three-stage test to determine whether the legitimate interests basis is available in a particular context. In the context of online cross device tracking, the legitimate interests basis may be difficult to establish, as users may not be fully aware of the processing that takes place, and due to the broader privacy implications of being tracked across multiple devices.

Typically, data controllers rely on consent for cross device profiling, but care is needed to satisfy the requirements for consent outlined above.

Fair processing notice

Under the Directive, data controllers are required to provide notice to individuals as to how their personal data will be processed. At a minimum, this information includes the identity of the data controller (and its representative,

if established outside the EU), the purposes for which personal data will be processed, and information as to the recipients or categories of recipients to whom personal data will be disclosed.

In addition, the data controller is required to provide any further information that is necessary to guarantee fair processing of personal data. In the context of cross device profiling, the scope of such further information will require careful consideration, not least because this requirement has not been interpreted uniformly across the EU.

Perhaps the key compliance risk in this context, assuming that an adequate information notice has been prepared, is making the information available to data subjects in a fair and easily understandable manner. This can pose particular challenges where sophisticated tracking techniques are utilised. Data controllers must explain such techniques using clear language, free from technical jargon. Typically, information relating to cross device profiling would be included in the privacy notice placed on a website that utilises cross device profiling techniques.

Data subject rights

The Directive provides data subjects with certain rights in relation to the processing of personal data about them. These rights include the right of subject access, the right to be made aware of the logic involved in any automatic processing of personal data, the right to have inaccurate, irrelevant or out of date information blocked, rectified or erased, and the right to object to processing on compelling legitimate grounds. In addition, data subjects have the right not to be subject to decisions that significantly affect them that are based solely on automated processing of data.

Data controllers that are engaged in cross device profiling will need to be ready to comply with each of these requests. Of particular importance is the right to correct irrelevant, inaccurate or out of date personal data and the right to object to processing on compelling legitimate grounds.

In the case of probabilistic profiling, users should be given the right to disassociate their profile from the actions of other users, particularly where it is clear that the data controller has not accurately identified the individual in question. Various mechanisms may be deployed to enable controllers to honour these rights, but typically 'dashboard' style systems that enable a high degree of transparency over the precise categories of data that are used to build the user's profile, as well as the opportunity to access, correct and block those data at a granular level, enable better compliance.

E-Privacy Directive

The e-Privacy Directive requires that an individual's informed consent is obtained before information can be stored on, or accessed from, their terminal equipment. Often referred to as the 'cookie law', the language of the e-Privacy Directive extends beyond cookies and includes all technologies that either store information on or read information from a user's device, including web based services and applications. The specific type of cross device tracking technology to be deployed will need to be analysed carefully, but it is likely that many (or perhaps most) of these technologies will fall within the scope of the e-Privacy Directive. Further, it is unlikely that the exemption to consent, where the technology is strictly necessary in order to provide a requested service, will apply to cross device tracking. Typically, cross device tracking enables additional, value added, personalised or tailored content, but in most cases this will not be 'strictly necessary' in order to provide the core service.

Organisations will need to think carefully about how they obtain any required consent. Guidance has been provided by the Article 29 Working Party in Working Document 02/2013 (copy available at: www.pdpjournals.com/docs/88441) on obtaining consent to the use of cookies. In that guidance, the Working Party notes that consent must be given before any data processing begins. This means that cross device tracking technologies that are subject to the e-Privacy Directive should only be activated after the user has been provided with relevant information, and given the opportunity to accept or decline the use of the tracking technology. The Working Party reiterates in the guidance its view that valid consent requires that a user is given a free and active choice. Any consent must constitute an active indication of the user's wishes, although the means by which consent is given is not prescribed. This requirement has been interpreted differently across the EU, but many Member States accept that implied consent (for example, inferred from a user's failure to navigate away from the site in question, after having been provided with clear notice of the use of cookies) is sufficient. Data controllers engaged in cross device profiling will need to consider these requirements in each Member State in which they operate.

Proposed General Data Protection Regulation

The proposed EU General Data Protection Regulation is expected to result in significant changes for organisations that carry out cross device profiling. The final text of the Regulation is still being negotiated by the EU institutions. It is expected to be agreed in late 2015, and to enter into force in 2017. However, a number of key concepts and proposed changes appear to be accepted, in principle, by the respective institutions.

The territorial scope of the Regulation will almost certainly be wider than under the Directive. The 'equipment test', described above, will be replaced by a test that focuses on whether the data controller monitors the behaviour of EU residents. Organisations (possibly processors as well as controllers) that monitor EU-based users' behaviour for the purpose of identifying them across devices will fall within scope of the Regulation. Whereas under the Directive organisations may have been able to argue that the 'equipment test' did not apply, this argument will be even more difficult to sustain under the Regulation.

(Continued on page 12)

(Continued from page 11)

The second key change concerns the definition of 'personal data'. The Regulation will specifically include 'online identifiers' within the categories of personal data. Most forms of deterministic profiling that utilise a unique user identifier will be personal data under the Directive, but this will be put beyond doubt in the Regulation. This change in the definition of personal data will not specifically affect forms of probabilistic profiling, but where an individual can be identified, then the Regulation will apply, just as the Directive does at present.

Under the Regulation, profiling will for the first time be specifically regulated. The Regulation defines profiling as processing intended to 'evaluate, analyse or predict any feature of [the data subject's] behaviour, preferences or identity'. This definition is cast extremely widely, and would clearly capture cross device profiling that attempts to infer the identity of a particular user through the evaluation and analysis of their online behaviour and characteristics.

The Regulation will prohibit all forms of profiling that produce 'legal effects' or otherwise 'significantly affect' the data subjects that are profiled. Although these terms are not defined, they are likely to be interpreted widely, for example, to include personalised ads served on the basis of the identity of the user, or differential pricing offered on the basis of the particular user in question. It is as yet unclear whether less privacy intrusive profiling use cases would be captured, for instance cross device profiling carried out for the purposes of providing personalised services to a particular user on the basis of the device they are using.

Profiling that produces a legal effect or otherwise significantly affects data subjects will be prohibited subject to limited exemptions, the primary one being that the profiling is carried out with the consent of data subjects. Under the Regulation, such consent will need to be 'explicit' in order to be valid. In practice this requirement will mean that mere acquiescence on the part of data subjects (for example, failing to un-tick a pre-ticked box, or failing to navigate away from a website) is unlikely to constitute valid consent. All organisations that carry out cross device profiling will need to review their consent mechanisms to ensure they will remain valid under the Regulation, particularly those that currently rely on forms of implied consent.

The scope of the legitimate interests processing ground under the Regulation is not yet clear. If legitimate interests is no longer available, consent is likely to be the next best option to consider. It is also unclear whether profiling based solely on categories of sensitive data will be prohibited, or permitted with data subject consent.

Finally, it should be noted that the Regulation will significantly increase the applicable penalties for non-compliance, with fines of up to 5% of global revenue under discussion. It is as yet unclear how such fines will be applied, but the order of magnitude represents a significant departure from the position under the Directive.

Conclusion

Cross device profiling poses significant compliance risks under the Directive and the e-Privacy Directive. In particular, organisations will need to ensure they have a valid legal basis on which to conduct cross device profiling, and that appropriate, clear information is provided about the processing activities. Ensuring that data subject rights can be accommodated may pose particular difficulties in the cross device profiling context.

More generally, cross device profiling has received little specific regulatory attention to date (other than in the context of cookies), and there has been little or no enforcement action on these issues to date. Whether this position changes in future will remain to be seen, but profiling seems likely to be subject to increased scrutiny under the proposed Data Protection Regulation.

Bridget Treacy and James Henderson
Hunton & Williams
btreacy@hunton.com
jhenderson@hunton.com

Internet of Things — where are we now?

Rob Corbet, Partner at Arthur Cox, examines the application of privacy laws in a global IoT ecosystem

Ten years ago, when we thought about the internet, we thought in terms of personal computers and laptops. That has now evolved to encompass tablets and smartphones. In a few years' time, we will associate the internet with, well, just about everything — a so-called Internet of Things ('IoT'), where all types of household, medical or other devices are web-enabled through the use of miniaturised sensors, GPS receivers and remote communications capabilities. We will be familiar with the connected car, the remote baby monitor, the Apple watch — even the fridge that tells you when you are out of milk.

The rise of the IoT is predictable. The number of internet connected devices in our world is expected to increase from approximately 25 billion in 2015 to around 50 billion in five years' time. The associated rise in data processing is phenomenal — it is estimated that in the past two years, the world has generated 90% of the data that was generated in the entire period of mankind beforehand.

So we know we are moving to an era where wearable computing will be common, where cities will compete to be 'smarter' than each other, and where even disposable household devices will include sensors. As a result, we know that our images, voices, lifestyles, habits and health will be processed in new ways and on a scale never before imagined.

So how do you apply privacy laws in a global IoT ecosystem?

The role of regulation in IoT

While the scale of growth of the IoT and the associated privacy and data protection challenges are already known, there is no firm consensus on how to apply privacy rules in a manner that strikes the right balance between encouraging product innovation and protecting user security and privacy.

As was the case in other innovations where there was rapid mass adoption, such as search engines and social networks, there remains a philosophical divide as to the role regulation should play in the IoT, in particular between the US and Europe.

EU and US perspectives

The divide is vividly illustrated by two recent official reports — one from the US and one from the EU — which specifically reviewed IoT and associated privacy and security concerns.

In Europe, the Article 29 Working Party published an Opinion in September 2014 on Recent Developments on the IoT (Opinion 9/2014, copy available at: www.pdpjournals.com/docs/88440). A few months later in January 2015, the US Federal Trade Commission ('FTC') published its Staff Report entitled 'Internet of Things — Privacy and Security in a Connected World'.

The views expressed in each paper demonstrate the challenges that are faced by the IoT stakeholders who are already building, deploying and using products and services in an IoT environment. These stakeholders include you and me, the consumers of IoT devices, but also device manufacturers, app-developers, social platforms, telecoms companies, property owners and many others.

Common ground — transparency, consent and data minimisation

Both the FTC and Working Party papers clearly identify the data security and privacy risks for consumers who will have no choice but to live in an IoT world.

It is also common ground that core privacy principles such as transparency, consent and data minimisation should apply in an IoT ecosystem. However, there is some difference of opinion between the jurisdictions as to how to impose those principles on IoT stakeholders.

Legislation

An over-arching difference between the two trading blocs is the fact that Europe has effectively had a federal data protection law for the past 20 years, with plans to significantly

(Continued on page 14)

(Continued from page 13)

update it in the short term if agreement can be reached to finalise the draft General Data Protection Regulation.

In contrast, the FTC regards itself as disadvantaged by the lack of any US federal privacy laws. In fact, the FTC paper re-iterates its recommendation that Congress should enact broad-based (as opposed to IoT-specific) privacy legislation which should be 'flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.'

There seems to be little prospect of a federal US privacy law in the short to medium term, so the practical implications for IoT stakeholders are that they will build and deploy products for a global market which will be subject to significantly differing privacy laws and standards in the two largest markets in the western world.

So while there will be one 'Internet' for each 'Thing', from a regulatory perspective, there may in fact be two Internets of Things.

Transparency

The fact that many IoT devices are not immediately visible to the eye creates difficulties in terms of meeting the legal standards typically imposed in the context of other forms of data capture. Privacy notices and privacy policies have traditionally been the means by which data controllers have tried to meet their disclosure obligations under the Data Protection Directive (95/46/EC) and under US fair trade laws. But is this workable in an IoT environment?

For example, if I wear a connected watch or sunglasses with an inbuilt camera and sensors which are capable of videoing the images and voices of passers by, must I wear a sign to warn users that I am processing their data?

This appears to be what the Working Party has in mind when it says that 'the identification of data processing through Wearable Computing...might be solved by envisaging appropriate signposting that would be actually visible to the data subjects'. Such signposting could be met by the device manufacturer printing on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures, as well as the purposes of the data collections, emphasising that they should be as user-friendly as possible.

The FTC is less prescriptive, instead setting out a number of options which could enhance transparency. It includes offering choices at the point of sale or during sign-up, customer tutorials (including codes on devices), offering management portals or dashboards, using privacy icons, 'Out of Band' communications (where users configure their devices to receive information through emails or texts) and General Privacy Menus. The FTC report acknowledges that none of these options is perfect, in particular for those devices that do not have screens or that have tiny screens.

Consent

While both papers advocate transparency, they present differing approaches on the issue of data subject consent. The EU position is consistent with earlier Working Party guidance in that consent to the use of a connected device and to any resulting data processing must be informed, specific and freely given.

Within Europe, they say that users should not be economically penalised or have degraded access to the capabilities of their devices if they decide not to use the device or a specific service. In addition, any non-user data subject must also have capacity to exercise his/her rights of access and opposition to the use of their data.

The Working Party states that privacy-friendly defaults are expected by EU citizens so 'Privacy by Design' and 'Privacy by Default' remain core principles.

We don't have to look far to find examples of the practical difficulties of applying European consent rules online. Article 5(3) of the e-Privacy Directive (2002/58/EC) introduced the so-called 'cookies consent' rule, which led to the introduction of express click-through consents on European websites. While designed to try to obtain consent from consumers to non-obvious uses of their data, in practice it has served only to annoy many users and website designers (who has ever read a cookies policy?).

The view of the Working Party is that the same consent requirements will arise when an IoT stakeholder stores or gains access to information already stored on an IoT device (as the relevant provision applies to all 'terminal equipment', which is broadly defined). Article 5(3) requires that the user must consent unless storage or access is 'strictly necessary in order to provide a service explicitly requested by the subscriber or user'. This is a very high bar for an IoT device, which may be capable of capturing data for any number of purposes.

It is recognised that these consent standards will be difficult to apply to IoT, but the Working Party encourages the adoption of innovative notification and consent processes to ensure a user's valid consent is obtained. It gives the examples of 'privacy proxies' (e.g. routing communications through private channels with limited third party access) and machine-readable 'sticky policies' (that govern all subsequent use of a particular packet of data) as emerging solutions.

The FTC approaches the consent issue differently. It recognises the need to balance future, beneficial uses of data with privacy protection, and it notes the concerns of some who participated in its IoT workshop that a strictly applied consent requirement could act as a barrier to socially beneficial uses of information, which may not have been imagined at the time of the original data capture.

To this end, the FTC sides more with the concept of 'expected' and 'unexpected' uses. In the case of an expected use, the FTC takes

the view that a company need not offer a choice to the consumer at all. However, for uses that would be inconsistent with the context of the interaction (i.e. unexpected), companies should offer 'clear and conspicuous' choices (in contrast with the Working Party's approach, the FTC stops short of mandating pro-active consent).

The FTC concedes that these types of use-based limitations are difficult to apply where the underlying fair use principles are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct. So while the problem is clear, the solution is less so.

Data minimisation

Another common principle in the two papers is the concept of 'data minimisation', which has been a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 APEC Privacy Principles and the 2012 White House Consumer Privacy Bill of Rights. In the EU Directive, the principle is captured by the words 'adequate, relevant and not excessive' in Article 6.

The view of the Working Party is that this principle specifically implies that when personal data are not necessary to provide a specific service run on the IoT, the data subject should at least be offered the possibility to use the service anonymously. The FTC suggests multiple options for data controllers to meet the requirement of this data minimisation principle: they can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that are less sensitive; or de-identify the data they collect. If none of these options are viable, they can then seek consumers' consent for collecting additional, unexpected categories of data.

It can be challenging to reconcile the principle of data minimisation while realising the true potential of IoT. Innovators will point to the fact that in the connected health space, for example, medical knowledge and predictors of ill-health are at a very early stage, and so minimising data capture (e.g. running shoes that record exercise patterns for fitness purposes) may serve to prevent IoT users from availing of breakthrough technologies (e.g. early predictors of Parkinsons disease).

As against this, privacy advocates would point to the dangers of allowing commercial enterprises to build health databases without a very informed consent by the device user.

Conclusion

Privacy and data security are acknowledged as cornerstones of an IoT world. However, we seem to be moving towards a two-tier regulatory system. For their part, the Europeans are committed not just to applying long-standing data protection principles to the IoT, but to enhancing and enforcing them under the proposed Data Protection Regulation.

In contrast, the US seems to be struggling to find a legal baseline against which it can regulate IoT stakeholders, notwithstanding that its privacy and security concerns "permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue."

The IoT will not just require technical innovation. Legal innovation will be at a premium. New thinking and new paradigms are required if IoT stakeholders, many of whom are based in the US, are to have any hope of complying with prescriptive and evolving EU privacy laws. One internet, one thing, two worlds.

Josh Maxfield, General Counsel at Garmin, will be speaking on 'Privacy and Data Protection Challenges of Rolling Out a New Technology Globally', at the 14th Annual Data Protection Conference being held in London on 15th and 16th October 2015.

See www.pdpconferences.com for further details.

Rob Corbet
Partner at Arthur Cox
rob.corbet@arthurcox.com

News & Views

UK regulator insists on pragmatism

(continued from page 1)

The report indicates that the ICO is considering reformulating the classic right of subject access in order to meet individuals' changing expectations. "People expect real-time, for free parcel-tracking and access to their bank-accounts and online order history. Perhaps DPAs should be doing more to encourage the development of much more powerful, faster and cheaper access rights for the public. Should the public have to make multiple access requests when their data are shared between a number of organisations?," asks the report.

On the question of future funding, the report asks whether there is scope for DPAs to retain the income from fines or a proportion of them, or recover costs from certain investigations. It raises the possibility of charging for certain services, citing audits as an example.

The ICO speculates: "It may be in the future that greater emphasis is put onto cross border investigations which cumulate in joint enforcement action between DPAs, especially since compliance issues can cover many jurisdictions. But what are the practicalities of such a process and how do we ensure that it is of value to the public? Are we more likely to see class actions from members of the public who bypass DPAs altogether and if so what role, if any, do we have to play in this?"

Mr Graham proposed a Resolution to the EU DPAs about 'meeting data protection expectations in the digital future'.

The Resolution makes a call for the funding of EU DPAs to be sufficient to meet the increasing demands on them, and calls upon lawmakers in Europe to ensure that the next generation of data protection laws are drafted in a clear and easily understood way. It also reminds DPAs of the need to develop systematic and proactive approaches to tackling non-compliant behaviour, be more responsive to new technologies, be assertive in making the case for resources, and to continue to develop Europe wide co-operation initiatives to share information and knowledge about practical approaches to data protection.

A copy of the report 'Data protection rights: What the public want and what the public want from Data Protection Authorities' is available at: www.pdpjournals.com/docs/88443

New EU/US data transfer agreement

(continued from page 1)

danger, I see Safe Harbor in dead waters.

The two deadlines to find an agreement have both expired. We are aware of the difficulties, but at the same time, it's time to have an answer from the US side. On the commercial dimension and on the national security exception."

Mr Buttarelli argues that Safe Harbor should be reformed, and not abandoned for another agreement, since it has made it easier for American companies to do business in Europe. "Safe Harbor, though not entirely satisfactorily from a European data protection viewpoint, has been playing a role," Buttarelli said.

"Today, we can't imagine that the intensive set of transfers of data from Europe to the US could be covered only by consent or by contracts or clauses or by binding corporate rules. This explains why more than 4,000 companies have been making use of Safe Harbor. So if we abandon it, it will be replaced by something else. Why necessarily move to something else when you can simply make the existing safeguards more effective in practice?"

US government human resources office hacked

The personal data of nearly four million US government workers are understood to have been compromised in a massive data breach carried out by Chinese hackers.

The US Office of Personnel Management, which serves as the human resource department for the federal government, confirmed that both current and past employees have been affected — and potentially also every federal agency.

The agency issues security clearances and compiles records of all federal government employees. Information stored on databases includes employee job assignments, performance reviews and training. The Office said it would be contacting all individuals whose personal data may have been breached in the coming weeks, and offering them 18 months of free credit monitoring and identity theft insurance.

The Office became aware of the breach in April 2015 during an 'aggressive effort' to update its cyber security systems.

(Continued on page 18)

(Continued from page 17)

Mandatory data breach notification introduced in the Netherlands

The Dutch Senate has passed a Bill on notification of data leaks, making it mandatory for data controllers to notify certain breaches of personal data.

Data controllers must notify breaches immediately to the Dutch regulator, the CBP, if a breach is likely to have serious adverse consequences for the protection of personal data. It is expected that the regulator will issue guidance defining a serious breach. Individuals may need to be notified too, unless the data have been encrypted.

Data controllers based in the country will now need to maintain an internal data breach register recording all security breaches they experience that have or might have potential negative effect on data subjects, including information about the breach, mitigating measures, and the text of notifications to the data subjects affected. There is no obligation to make this register public.

Failure to notify breaches is punishable by a maximum fine of 810,000 euros or 10% of a company's annual net turnover. Importantly, the fines may not be limited only to a company's establishment in the Netherlands, but instead be calculated according to global turnover.

It is expected that the majority of the requirements will enter into force on 1st January 2016, but the exact date will be set by a Royal Decree.

The Dutch government said it elected not to wait until the adoption of the EU General Data Protection Regulation (which also contains a data breach notification duty) due to the widespread occurrence of data breach incidents.

UK police bodies still falling short on records management

The UK Information Commissioner's Office has published a report highlighting its experience of personal data handling of police forces, based on 40 audits and 30 follow-up audits.

The report shows that 54% of all ICO recommendations were complete by the time of follow up reviews. A further 30% were partially completed or in progress. However, records management was where the fewest recommendations from follow ups had been completed. The ICO observed: "we believe that there is still work to be done to mitigate information rights risks, and in particular police forces need to implement changes in some common areas of concern."

The ICO highlighted the following things as being problematic: lack of refresher training plans for records management; lack of controls or processes for the secure disposal of electronic and manual records; and no information asset register or information asset owners.

A copy of the report is available at: www.pdpjournals.com/docs/88444

UK police force fined £160,000

The ICO has issued South Wales Police with a fine of £160,000 for losing a video recording which formed part of the evidence in a sexual abuse case. Despite the DVDs containing a graphic and disturbing account, the discs were unencrypted and left in a desk drawer.

In addition to the monetary penalty, the Information Commissioner has asked the police force to sign an Undertaking to ensure the changes are made to implement policies to prevent such incidents from reoccurring.

A copy of the Monetary Penalty Notice is available at: www.pdpjournals.com/docs/88442

US law limits snooping, just as UK gears up to make its spies more powerful

The US has limited the powers of its intelligence agencies for the first time in over 30 years, just as the UK gears up to hugely increase what its own can do.

In what has been hailed as a victory for privacy campaigners and a direct result of whistle-blower Edward Snowden's leaks, the Senate has passed the USA Freedom Act, placing new restrictions and oversight on the way that the country's National Security Agency can spy on citizens.

The Freedom Act bans the storage of phone records indiscriminately. Instead of the NSA directly capturing and holding the metadata for every American citizen's cellphone conversation, telecommunication companies will hold onto the data, and the NSA may access it through the federal court system.

The mainstream media has celebrated the USA Freedom Act as a victory for civil liberty, although some privacy campaigners have complained that the provisions do not quite go far enough.

Meanwhile, in the UK, lawmakers are getting ready to pass into law the Draft Communications Data Bill, which among other things requires internet service providers to store information on their users so that intelligence agencies can access them. Following the election of the Conservative government, the Bill will potentially include even more powers. Prime Minister, David Cameron, has indicated that he will ban or reduce the encryption that is used to keep data secure.

CNIL to conduct 550 onsite inspections this year

The French Data Protection Authority has released its annual inspection programme for 2015, revealing its target of 550 inspections for the year, including 350 on-site inspections and 200 online inspections.

A quarter of the on-site inspections will focus on closed-circuit television monitoring. The CNIL will also focus on contactless payment systems, companies' processing of employee personal data for the management of psycho-social risks at the workplace, the National Register of Driving Licenses held by the French Ministry of the Interior, connected objects for wellbeing and health, public WIFI connections and data processing operations covered by Binding Corporate Rules.

The CNIL recently created a new regulatory tool — 'compliance packs' — helping various industries to comply with data rules. Packs have already been published for insurance and social housing, and are being developed for the banking sector.

Italy's DPA consults on Internet of Things

The Garante is inviting comments on the Internet of Things in order to gain insights for defining rules and safeguards.

In particular, the Garante is seeking views on how to provide information to individuals and gain their consent, types of data that are processed, the possibilities to deploy Privacy by Design, anonymisation of personal data, interoperability of services, and development of certification tools, both in Italy and at an international level.

The DPA is asking that responses are sent to iot@gpdp.it

Further enhancements to South Korea's data protection laws announced

As a response to the serious data breaches suffered by three major credit card companies last year, the South Korea government continues to tighten its data protection regime.

Following the introduction of the Standards of Personal Information Security Measures in December 2014, proposed amendments to the Utilisation and Protection of Credit Information Act were announced in March 2015. These are tentatively expected to come into effect on 12th September 2015.

The proposed amendments impose specific responsibilities on credit information custodians and managers (for example, the privacy officer in a financial institution), requiring them to report regularly to the board of directors and the Financial Services Commission on monitoring and management of credit information. Heavier administrative sanctions and civil damages will be imposed for non-compliance with the amended rules.

The government has also recently passed the Act on the Development of Cloud Computing and Protection of Users. This is also expected to come into effect in September 2015. Some provisions of this Act will apply both to Korean and global service providers.

Key requirements of the Act include a requirement on cloud service providers to notify their users of a data breach or service outage, as well as compliance with existing data protection laws.

Australian Commissioner launches privacy framework

The Office of the Australian Information Commissioner has launched a new privacy guide, 'Privacy management framework: enabling compliance and encouraging good practice', which sets out recommended best practices and practical guidance on how to establish and implement a privacy management plan for those organisations seeking to comply with the Australian Privacy Act. It includes a four-step approach to embedding a culture of privacy.

The publication follows OAIC's findings that 55% of privacy policies of the organisations and agencies that it surveyed failed to meet the requirements of Australian Privacy Principle 1, requiring that personal information is managed in an open and transparent way.

A copy of the framework is available at: www.pdpjournals.com/docs/88445

Germany to get new data retention law

German policymakers have introduced a new data retention law requiring data to be stored in Germany and the mandatory data retention of telephone use and computer IP addresses for ten weeks. Germany is one of the first EU countries to draft a new law on data retention following the European Court of Justice's decision that the EU's Data Retention Directive violated privacy rights.

The draft bill is a stark contrast to the requirements under the European Data retention Directive which required the storage of data for between six months and twenty four months.

Google and Max Mosley settle sex session images dispute

Former Formula One boss, Max Mosley, has settled his legal dispute with Google over images from his sadomasochistic sex session with five women, representatives of both sides have confirmed.

Mr Mosley launched his claim in the UK in 2014 shortly after the European Court of Justice recognised a 'right to be forgotten' (in *Google Spain v AEPD*). The ruling confirmed that Google was subject to data protection regulation, allowing Mr Mosley to establish a claim around the UK's Data Protection Act.

The settlement brings to an end one of the highest-profile privacy claims of recent years, raising new questions about the obligations on internet companies to protect celebrities' personal data.

The terms of the deal were not disclosed.

Mr Mosley's remaining claims will not now proceed to trial in the UK, Germany, France or any other country.

(Continued on page 20)

(Continued from page 19)

Daily Mirror to pay £1.2m to celebrity phone-hacking victims

The publisher of the Daily and Sunday Mirror has been ordered to pay £1.2m in compensation to eight phone-hacking victims, including the actor Sadie Frost and the former footballer Paul Gascoigne.

Frost was awarded £260,250 in what is believed to be the single biggest privacy damages pay-out since the phone-hacking scandal broke in 2010. Gascoigne is to receive £188,250 in compensation from Trinity Mirror after the former England footballer told the High Court he was driven to alcoholism and severe paranoia when journalists snooped on his voicemails from 2000 to 2010.

With the company now facing new phone-hacking damages claims from more than 100 high-profile figures, it said it was increasing the amount of money set aside to deal with the legal cases from £12m to £28m.

Health body signs Undertaking following fax errors

A health body has formally committed to improving its data handling after it mistakenly sent five faxes containing patient information to a member of the public.

In its Undertaking with the ICO, Northumbria Healthcare NHS Foundation Trust promises to introduce clear procedures so that any data breaches reported to it are acted upon promptly, and also to introduce remedial measures across the organisation. In addition, the health body has committed to adopting fax procedures to ensure adequate security standards are maintained across all wards, including making use of pre-programmed numbers.

A copy of the Undertaking is available at: www.pdpjournals.com/docs/88446

ICO reviews children's websites and apps

The ICO has participated in a review of websites and apps used by children, as part of an international project to consider privacy concerns around the type of personal information that services collect.

The ICO looked at 50 websites and apps, particularly at what information they collect from children, how that is explained, and what parental permission is sought.

Other regulators that are members of the Global Privacy Enforcement Network have also carried out a review. The results will be published in the Autumn.