2010 - Ministry of Justice call for evidence on current data protection framework

This is JANET(UK)'s response to the Ministry of Justice Call for Evidence on the Current Data Protection Legislative Framework [1]. JANET(UK) is the operator of the UK's publicly-funded National Research and Education Network, JANET, which connects universities, colleges, research organisations and regional schools networks to each other and to the Internet. We also operate national authentication and authorisation services [2] for UK education, which are designed to protect user privacy while enabling providers of on-line educational services to make accurate decisions on granting and personalising access to their services. There is growing benefit in linking these services to international peers, including other European countries and the USA.

Our response is therefore primarily concerned with the interpretation and implications of the Data Protection Act 1998 and European Data Protection Directive for on-line services, and informed by the difficulties we have had in reconciling the law with our desire to provide privacy-protecting services on a national and international basis.

Q1: What are your views on the Data Protection Act 1998 and the European Directive upon which it is based? Do you think they provide sufficient protection in the processing of personal data? Do you have evidence to support your views?
We are concerned that technical developments are stretching the Data Protection Act's simple model that everything is either personal data or not personal data to, and beyond, breaking point. We note that the Information Commissioner has himself admitted that current law poses "practical and sometimes insurmountable difficulties in complying with all aspects of the DPA in respect of non-obvious personal identifiers" (Personal Information Online Code of Practice [3] (2010), p.10), and would concur with that view.
These problems arise from the Act's (and Directive's) failure to distinguish between information that itself identifies a data subject, and information that only does so if the current holder has additional information to make the link between the information and the data subject. For example an Internet Service Provider (ISP) will often be able to identify one of its own subscribers from an Internet Protocol (IP) address and the time it was in use, but no one else will be able to make that link since the ISP is prohibited by law from disclosing the required information. Current law is very unclear as to the status of this indirectly-linked information when transferred to, or held by, anyone other than the ISP.
When asked to rule on the question of whether an IP address is personal data, therefore, courts across Europe have reached contradictory conclusions: in some cases ruling that such an address is personal data and in others that exactly the same information is not. We consider that this is harmful both because some privacy-intrusive activities have been permitted (in Ireland, examining the content of users' Internet communications to determine whether they are breaching copyright has been ruled not to involve any processing of personal data), and because other privacy-protecting services have been prohibited (for example a court in Germany has ordered ISPs to delete all logs of customer activity even

though these could be used to detect and resolve attacks on and by the users' PCs). Furthermore treating directly and indirectly-linked data alike in law means that there is no incentive for services to use indirectly-linked identifiers that provide better privacy protection We therefore believe that a new approach is required to information that is not directly linked to an individual, but could be linked if certain additional conditions are met. The decision on what measures are required to protect this indirectly-linked information must be based on the risk of those particular conditions occurring and the harm that might result. If this is not done, we believe that the disparity between the law and technology will become increasingly obvious and problematic and that, as the Information Commissioner recognises, service providers will be forced to ignore the law in order to provide the services their users need and expect.

Q2: What are your views on the definition of "personal data", as set out in the Directive and the DPA?

As in our answer to Q1, we believe that the inclusion of indirectly linked information within the same category of "personal data" as directly linked information is harmful to both privacy and compliance.

The UK Data Protection Act (unlike the European Directive) attempts to address the problem by clarifying that indirectly linked information is only personal data in the hands of a Data Controller who has, or is likely to obtain, the means to make the link. Unfortunately the law fails to deal with the necessary implication that information can change from personal to not as it is transferred from one data controller who has the linking information to another who does not. It is entirely unclear which (if any) of the Data Protection Principles or laws apply to such a transfer: for example does an ISP break the law whenever it transfers an IP address (personal data in the ISP's hands) to a web server in the USA? The law also fails to address the situation where a Data Controller discloses indirectly linked information to a third party who obtains the linking information by another route, for example direct from the Data Subject. Has the original Data Controller then retrospectively broken the law by disclosing what it, in good faith, believed to be non-personal data?

Current guidance appears to avoid these difficulties by ignoring the Act's qualification and recommending that indirectly-linked information should always be treated as if it were personal data, acknowledging that this may well make it impossible to comply with the Act!

Q3: What evidence can you provide to suggest that this definition should be broader or narrower?

As above, we consider that the definition of "personal data" should be restricted only to information that itself permits direct identification of a living individual. A new category, perhaps called "potential personal data", should be used for information that may be indirectly linked to an individual. Processing of potential personal data must be regulated, since there is a possibility that it will breach privacy, however that regulation must be based on the risk that a privacy breach may occur, rather than containing absolute requirements or prohibitions such as those on international transfer. This could well result in a wider range of data being appropriately protected, since Data Controllers, Regulators and Courts would no longer be forced to choose between the extremes of (heavily-regulated) personal data and (completely unregulated) non-personal data. In this context we note that a number of research papers [4] and unintended experiments have discovered that information thought to be anonymised, and therefore non-personal, can be linked to its origin using third party information sources. Treating such information as low-risk potential personal data would provide better privacy protection than its current non-personal status.

Q4: What are your experiences in determining whether particular information falls within this definition?

We have found it impossible to determine whether Internet Protocol (IP) addresses and privacy-protecting identifiers should be classed as personal data when held by someone other than the Data Controller who assigned them to an individual user.

According to section 1(1) of the Data Protection Act 1998 indirectly-linked information is only personal if the current data controller has, or is likely to obtain, the additional information needed to make the link. Since this information can only be obtained if the original Data Controller discloses it, in breach of the Act, it appears that the information should not be classed as personal data in the hands of any other data controller. However guidance from the Information Commissioner suggests that IP addresses should always be treated as personal data, though recognising that this may make it impossible to comply with the law, for example on Subject Access Requests (the holder of only an indirectly linked identifier will be unable to confirm that a requester is actually the Data Subject) and international transfers (since IP addresses are routinely exchanged between Europe and the rest of the world).

Regulators also seem to have different views on whether the definition of personal data requires that on-line activity be linked to a real-world person, or whether merely recognising a returning visitor is sufficient. In the latter case, even a privacy-protecting identifier, which uses both technical and legal measures to prevent linkage to a living individual, appears to be classified as personal data and subject to the full weight of regulation, giving providers very little incentive to adopt them.

We note that court opinions are equally divergent – in Germany courts have ruled both that IP addresses in web server logs are personal data and that they are not, while the Irish courts (using a definition almost identical to that in UK law) have ruled that collecting IP addresses associated with copyright breaches was not processing personal data, even though the intention was for the ISP to disconnect individuals who repeatedly offend.

Q5: What evidence can you provide about whether biometric personal data should be included within the definition of "sensitive personal data"?

Q6: If as a data controller you process biometric data, do you process it in line with Schedule 3 of the DPA which imposes an additional set of conditions?

Q7: Are there any other types of personal data that should be included? If so, please provide reasons why they should be classed as "sensitive personal data"?

We have no information relevant to these questions.

Q8: Do you have any evidence to suggest that the definitions of "data controller" and "data processor" as set out in the DPA and the Directive have led to confusion or misunderstandings over responsibilities?

Q9: Do you have any evidence to suggest that the separation of roles has assisted in establishing responsibilities amongst parties handling personal data?

Q10: Is there evidence to suggest that an alternative approach to these roles and responsibilities would be beneficial?

Q11: Do you have evidence that demonstrates that these definitions are helpful?

We are aware of a number of contract negotiations where the discipline of determining Data Controller and Data Processor status has been helpful in clarifying and documenting the responsibilities of the parties. We have not experienced any problems with the current definitions and regard them as beneficial.

Q12: Can you provide evidence to suggest that organisations are or are not complying with their subject access request obligations?

Q13: Do businesses have any evidence to suggest that this obligation is too burdensome?

Q14: Approximately how much does it cost your organisation to comply with these requests?

Q15: Have you experienced a particularly high number of vexatious or repetitive

requests? If so, how have you dealt with this?
Q16: What evidence is there that technology has assisted in complying with subject access requests within the time limit?
Q17: Has this reduced the number of employees required and/or time taken to deal with this area of work?
Q18: Is there evidence to suggest that the practice of charging fees for subject access requests should be abolished?
Q19: Do you have evidence to suggest that the £10 fee should be raised or lowered? If so, at what level should this be set?
Q20: Do you have evidence to support the case for a "sliding scale" approach to subject access request fees?
Q21: Is there evidence to suggest that the rights set out in Part Two of the DPA are used extensively, or under-used?
Q22: Is there evidence to suggest that these rights need to be strengthened?
We have no information relevant to these questions.
Q23: Is there any evidence to support a requirement to notify all or some data breaches to data subjects?
We are concerned that a number of different objectives have been suggested for data breach laws, and that these objectives are incompatible [5]. It should be a matter of good customer relations for an organisation to help individuals who may have been harmed by its actions. However if (as in the original California data breach law) the intent or effect of the law is to "name and shame" those who admit to breaches then organisations will be very reluctant to do so. This could have the perverse effect of encouraging customers to move away from organisations who do attempt to protect privacy to those who do not.
Q24: What would the additional costs involved be?
Q25: Is there any evidence to suggest that data controllers are routinely notifying data subjects where there has been a breach of security?
We have no information relevant to these questions.
Q26: Do you have evidence to suggest that other forms of processing should also be exempt from notification to the ICO?
Q27: Do these current exemptions to notification strike the right balance between reducing burdens and transparent processing?
We have no information relevant to these questions.
Q28: What evidence do you have to suggest the Information Commissioner's powers are adequate to enable him to carry out his duties?
Q29: What, if any, further powers do you think the Information Commissioner should have to improve compliance?
Q30: Have you had any experience to suggest that the Information Commissioner could have used additional powers to deal with a particular case?
We have no information relevant to these questions.
Q31: Do you have evidence to suggest the current principles–based approach is the right one?
We believe the principles-based approach is correct, though as discussed above the current principles may need to be modified to take a fully risk-based approach to indirectly-linked information.
Q32: Do you have evidence to suggest that the consent condition is not adequate?
Like both the Information Commissioner [6] and the Article 29 Working Party [7], we are concerned that "consent" is used too often as a basis for processing. We consider that it should be reserved only for situations where the data subject is genuinely able to give, and arbitrarily withdraw, free and informed consent. In many relationships with the state, and most

with employers, this is not the case.
We consider that the other Schedule 2 conditions, based on necessity for various purposes, provide a much better basis for processing in the majority of cases. These protect both privacy, since the data subject should be able to rely on only necessary processing taking place, and operations, since providers have greater assurance that the personal data they need will continue to be available and that consent will not be arbitrarily withdrawn.

Q33: Should the definition of consent be limited to that in the EU Data Protection Directive i.e. freely given, specific and informed?

Yes.

Q34: How do you, as a data controller, approach consent?

As a data controller, we treat consent as a last resort (in accordance with the Information Commissioner's advice), and process personal data on the alternative basis of necessity wherever possible. For example where JANET is providing service to universities and colleges, it is necessary that we have administrative, technical and security contacts at those organisations. Having those contacts withdraw would cause serious difficulties for us and their organisation, so our processing of them is clearly not based on their consent, but on necessity to fulfil our agreement to supply services.
We aim to use consent as a condition for processing only where it can genuinely be withdrawn without difficulties, for example for subscribing to newsletters or e-mail updates.

Q35: Do you have evidence to suggest that data subjects do or do not read fair processing notices?

We have no information relevant to this question.

Q36: Do you have evidence to suggest that the exemptions are fair and working adequately?

Q37: Do you have evidence to suggest that the exemptions are not sufficient and need to be amended or improved?

We have no information relevant to these questions.

Q38: What is your experience of using model contract clauses with third countries?

We have no information relevant to this question.

Q39: Do you have evidence to suggest that the current arrangements for transferring data internationally are effective or ineffective?

We consider that if an Internet Protocol (IP) address is classed as personal data, then it will be impossible to comply with any international transfer requirement that involves a prior arrangement. Our international network links carry billions of packets a day to servers all over the planet: we cannot contract with all of those servers or exclude those (the vast majority) whose countries have not been recognised as providing equivalent protection. Indeed technologies to improve Internet performance and reliability, such as anycast addresses and cloud services, now mean that the decision on which server, in which country, will handle a particular user request will not be made until the moment the user sends the request, so prior arrangements are, by definition, impossible.

Links
[1] http://www.justice.gov.uk/consultations/call-for-evidence-060710.htm
[2] http://www.ukfederation.org.uk/
[3] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_on
[4] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

[5] http://www.ja.net/development/legal-and-regulatory/related-regulatory-documents/Data%20breaches%20draft%20v0.05.pdf
[6] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_lega
[7] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf