2012 - Ministry of Justice call for evidence on EU Data Protection Proposals

This is Janet's response to the Ministry of Justice call for evidence on the European Commission's data protection proposals [1]. The JNT Association, trading as Janet, is the non-profit company limited by guarantee that operates the Janet network connecting education and research organisations in the UK to each other and to the Internet. We have not yet been able to determine how the change in administration of data controllers (from registration to enhanced documentation) would affect us as an SME so our response does not cover that aspect. Instead we consider the likely impact of the proposed Regulation on four areas of networked services where we and our customer organisations (universities, colleges and research organisations in the UK) have experienced problems in interpreting and applying the current Directive and Act: the status of Internet identifiers such as IP addresses; network incident response; breach notification; and cloud computing.

Internet Identifiers

Under the current Directive (95/46/EC), and the UK transposition (*Data Protection Act 1998*) in particular, the status of Internet Protocol (IP) addresses and other pseudonymous identifiers is very unclear. While a customer's Internet Access Provider (in our case, their university or college) may be able to associate an IP address or other identifier with a subscriber, other networks across which the traffic passes (including national and international backbones such as Janet) cannot. As a result it is unclear whether those networks are required to treat IP addresses as personal data and, if so, how the provisions on grounds for processing (particularly when transferring Internet traffic outside the EEA), informing data subjects and subject access requests would apply.

We had hoped that the new legislation would clarify this, however its provisions appear to be contradictory. Article 4(1) specifically mentions "online identifiers" as values that can be associated with a data subject and therefore constitute personal data, however recital 24 says that "online identifiers as such need not necessarily be considered as personal data in all circumstances". The circumstances in which these identifiers are, or are not, personal data need to be clear and practical, otherwise those Internet services that wish to comply with the law will be unable to do so, while those who wish to ignore the law as being unclear or impractical will have evidence to support their position.

If such identifiers are to be treated as personal data the Regulation does, at least, appear to resolve the current paradox that a backbone network cannot identify an individual user but is nonetheless required somehow to provide them with information and handle subject access requests from them. Articles 14(5)(b) and 15(4) provide welcome recognition that treating pseudonymous identifiers as personal data will create data controllers for whom the information and subject access duties are impossible (since these identifiers may provide neither the ability to communicate with the data subject, nor the ability to securely identify them when they present a subject access request). Article 10 of the proposal further ensures

that such data controllers will not be required to seek out additional, privacy-invasive, personal data merely to satisfy those duties.

However if backbone networks are to be considered Data Controllers for the traffic they carry, it is not clear which, if any, of the provisions in Articles 41-45 would cover the transmission of such traffic outside the European Economic Area (EEA), even though this happens billions of times a day in the normal operation of the Internet. The data subject cannot be presumed to have given informed consent, since they may not have known the geographic location of a particular website or e-mail address before they sent information to it. Indeed with some of the technologies used to achieve Internet resilience, the geographic destination and routing of a request may only be decided at the moment the request is made and cannot be predicted in advance. The number of non-EEA websites and network providers makes it completely impractical either for a backbone network to have contracts with all of them or to seek individual approval from the regulator for each traffic flow. As with the legal status of IP addresses above, if it is not clear how to comply with the law in practice, the law risks being ignored.

Network Incident Response

As the operator of one of the longest established network incident response teams in Europe, we strongly welcome the recognition in Recital 39 of the important role incident response plays in protecting privacy online, thus promoting trust in the online environment. The proposed legislation seems likely to reassure incident response teams that there is a secure legal basis for their work [2] particularly as it will allow the “legitimate interests” justification (Art 6(f)) to be used, where necessary and proportionate, to notify trusted teams outside the EEA (Art 44(1)(h)) of problems on their networks and systems. This is already an essential part of protecting European networks, computers and users, as many incidents have global, not just European, scope.

While the Regulation appears to help the work of incident response teams in network operators other companies, there may be a risk of it creating a barrier to sharing of information with incident response teams operated by Governments. If those teams are classed as “public authorities” then the Regulation will prevent them using the “legitimate interests” justification, with its associated tests of necessity and proportionality. Instead these teams may be required to have powers defined by law: the use of a different legal basis and, perhaps, different safeguards could require network and company teams to take a different approach when sharing information with Government teams, thus making information sharing harder and less likely to occur. This problem could be increased for sharing with law enforcement and judicial authorities if they are covered by completely different legislation under the proposed Directive. An approach such as the UK National High-Tech Crime Unit’s original Confidentiality Agreement might be needed to support the essential information exchange between incident response teams and law enforcement.

Privacy Breach Notification

We support the Regulation’s aim of ensuring that individuals who are the victims of a privacy breach have the information they need to protect themselves from the consequences. However we consider that the timescale proposed in Article 31 of the Regulation is unrealistic and could both decrease trust in online services and increase the impact of privacy breaches.

Apart from the very simplest breaches – for example the loss of a memory stick whose

contents are known – it is unlikely that an organisation suffering a security breach of its networked computers will be able to determine the cause and likely consequences within 24 hours. Such an organisation may need to use digital forensic tools to determine how the compromise took place and which data may have been accessed, combined with analysis of network and other logs to determine which information has actually been read by the intruder. A report to the regulator before this has been done is unlikely to contain significant useful information. Reports sent to affected individuals will involve even more work, to understand and test mitigation measures and to present the information in a form that is accessible to the affected individuals, rather than being designed for technical specialists. If the imposed time limit forces organisations to report too soon there is a significant risk that those reports will be unclear or inaccurate and cause alarm rather than providing help. We note, by contrast, that the amended Privacy and eCommerce Directive (2002/58/EC amended by 2009/136/EC) required privacy breaches to be reported "without undue delay" and that the UK Information Commissioner has advised that minor breaches should be reported as monthly summaries [3]. This approach seems more likely to protect individuals and build their confidence in on-line services.

The tight timescale and large penalties for not observing it could also make organisations change their priorities when dealing with a privacy breach. At present the usual first step in responding to an incident is to contain it, to stop it getting worse. Once the incident is contained it can then be analysed and reported. If, by placing high priority on reporting, the Regulation causes organisations to divert resources from containing the incident to reporting on it, it is likely that the impact of incidents will increase because of the resulting delay in taking action to contain them.
Since the breach notification provisions of the Privacy and eCommerce Directive are already in force we hope that their effects will be analysed and their findings used to inform the final form and implementation of the wider breach notification provisions in the Regulation. If this is not done, and a significantly different regime is imposed, we believe there is a risk that this will have the opposite effect to what is intended.

Cloud Computing
The proposal and the associated factsheet [4] include welcome provisions to support the use of cloud computing technology by consumers and within European businesses. We hope that the opportunity to design a single compliant service for 800 million European consumers will prove attractive to cloud service providers.

Unfortunately the proposal does not seem to help the many European organisations that wish to run their services on external cloud providers. Current legislation on this is unclear: UK guidance [5] suggests that US cloud providers can be covered by the Safe Harbor agreement, but onward transfers by those providers to servers in third countries may be a problem. Other EEA countries have threatened to prohibit use of US cloud providers entirely, also quoting the Directive. Since the Council of Ministers recognised "the need for legislation to reflect the economic importance to the European Union of international data transfers [6]" we hoped the new proposal would address this. However the draft Regulation does not appear to offer any new support for outsourcing to the cloud; indeed if, as has been suggested, the current Safe Harbor arrangements for US cloud providers are to be withdrawn then the Regulation will actually create a new barrier to European businesses. Since it has been estimated [7] that a single university could save several thousand pounds a year by outsourcing just its e-mail service to a cloud provider, a Regulation that made this more difficult could be very harmful to many UK and European organisations. We hope that it will be possible to both clarify and improve the current legal provisions in this area.

Links
[1] http://www.justice.gov.uk/consultations/data-protection-proposals-cfe.htm
[2] http://www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf
[3] http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_breaches.aspx
[4] http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf
[5] http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx
[6] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf
[7] http://www.janetbrokerage.ac.uk/news-blog/latest-research/cloud-email-whitepaper-financial-benefits/