PRIVACY INTERNATIONAL

RESPONSE TO THE EUROPEAN COMMISSION'S COMMUNICATION ON THE 'COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION'

JANUARY 2011

PI REGISTRATION NUMBER: 78180074927-85

265 Strand, London, WC2R 1BH, GB • T:+44(0)208.123.7933 • www.privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

For over twenty years Privacy International (PI) has vigorously defended personal privacy. We have campaigned across the world to protect people against intrusion by governments and corporations that seek to erode this fragile right. We believe that privacy forms part of the bedrock of freedoms, and our goal has always been to use every means to preserve it. Our campaigns are often controversial, but they always respect the primacy of truth and principle.

PI is the oldest surviving privacy advocacy group in the world, and was the first organisation to campaign at an international level on privacy issues. Its antecedents stretch back to 1987, at which time the organisation's founders started to build an international network in response to mounting concern across the world over the changing nature and magnitude of privacy violations.

We have organised more than 100 conferences and events, participated in hundreds of national and international meetings, participated in thousands of media interviews, organised influential campaigns, and produced widely-cited publications.

We are frequently called upon to give expert testimony to parliamentary and government committees in countries around the world. We are the secretariat to the UK Parliament's All-Party Group on Privacy. We have also advised and reported to international and inter-governmental organisations including the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, and the United Nations (e.g. ECOSOC, OHCHR, UNDP, UNESCO, UNHCR). PI now has active associates and networks in over 40 countries.

PI is registered in the UK as a non-profit private limited company (no. 4354366).

RESPONSE

Privacy International, the 20-year-old global campaigner for citizen and consumer privacy rights, has been actively engaged in the consultation process for the review of the European Union data protection legislation framework, and is happy to contribute our views on this Commission Communication. We are pleased that the Commission recognises the need to improve the coherence of the data protection legal framework in order to safeguard the fundamental right to privacy, as expressed both in the European Convention of Human Rights, and the EU Charter of Fundamental Rights. Privacy is a human right, and we believe that it must be discussed, promoted, protected, and continuously enhanced.

We have always been ardent supporters of the EU Data Protection Directive. Its principles-based approach and the principles themselves have been a success story, a beacon for Europe and the World. These principles have worked well, and therefore must be maintained. We have, on the other hand criticised strongly the lack of compliance with data protection laws by data controllers and data processors, the inconsistencies between various national legislations, as well as the limited powers and weak enforcement by data protection authorities. We remind readers of this consultation response however that we have been frequent users of this Directive, as we have filed numerous complaints across all the member countries. And we are also ambassadors of the Directive, as we promote its principles around the world.

1. General remarks

Overall, the Communication reflects well the feedback from the series of stakeholder consultations, impact assessments and studies carried out in preparation to the review; it gives a fairly comprehensive picture of the new challenges to effective privacy protection; and it reflects well issues that will need to be addressed in the planned review of the data protection framework. The key objectives outlined are the right ones, though those connected to strengthening individual rights and improving enforcement must remain the absolute priorities.

However, in our view, there are a few areas that it fails to address as fully as needed:

- Privacy enhancing technologies (PETs) and privacy by design is mentioned briefly in the context of enhancing the data controllers' responsibilities (2.2.4), but these are essential tools to ensure effective privacy protections that have been paid lip service in the past but not used. They deserve a place in their own right, including examining ways in how they can be practically adopted. In many online transactions it is not necessary to give away personal information and effective authentication technologies do exist. However they have not been widely adopted, or used, because it is rarely in the interest of service providers to adopt or promote such technologies, since their business models depend on constant data harvest-

ing, and since such information has economic value. So there is an inherent tension between the rights of the individuals in legislation, and the desire of a great number of service providers to circumvent those rights as much as possible. These kinds of tensions will need to be solved if a review of the legislation is to succeed.

- While the need for enhancing transparency is rightly acknowledged, there is no mention of the challenges posed by people's natural behaviour (behavioural economics) and the need to address this within a future review. Any measure adopted in future legislation that will have data collection as default is bound to fail, as it has until now. So considerations of behavioural economics are particularly important in the context of discussions of various default settings and user control, as well as future risk/detriment assessments. Only privacy by default, data minimisation and avoiding unnecessary identification will meet the stated goal of strengthening individuals' rights.

- There is little mention of the challenge of dealing with the issue of individuals as data controllers - i.e. user generated content, bloggers, video makers that release a constant wave of personal data which is often public by default. This is a phenomenon that did not exist at the time of the formulation of the current directive, and needs to be addressed in any future review, since an individual using a platform service cannot be treated in law in the same way as large service provider weather public or private. In this respect we agree with those that recommend settings of maximum privacy by default on the platforms that provide services to individuals (blogging sites, social networks, etc).

- While the challenges identified are indeed very real, we are concerned that they are all given equal status. In our view the effectiveness of personal information protection and effective enforcement should be the prime and overriding objectives, while lessening administrative burdens, making transfers simple, etc, should come as secondary objectives, albeit desirable.

We ask the Commission to address all these issues comprehensively during the coming process of the review of the legislation, in order to ensure a meaningful 'strengthening' of people's privacy rights. As the Communication acknowledges, the EU will need to have a consolidated general framework, which can be complemented with more specific rules and alternative measures.

We give some more specific comments in the sections below, following the main headings and contents of the Communication.

2.1 Strengthening individual's rights

2.1.1 Ensuring appropriate protection

The Commission is right to address the concept of 'personal data', the issues round its definitions, and various processing and mining technologies as some of the most essential if fundamental privacy rights are to be protected.

Regarding definition of the concept of personal data, we support a wide definition, as included in the current Directive and interpreted by the Article 29 Working Party (Opinion 4/2007). This will continue to ensure the necessary flexibility and make the legislation future proof. The issue that will need to be addressed in the review is not the definition, but its different interpretations and lack of clarity on national levels, as is the case for example with IP addresses. One way to address this is to provide authoritative guidance that has to be taken on board by member countries, and the Article 29 Working Party is well placed to provide such guidance.

We are particularly concerned that the concept of personal information appropriately reflect the increasingly common use of 'analytics' which can select individuals for attention; e.g. for customised direct marketing, presentation of webpage content etc, even though the data controller may not know, or even be able to find out, the actual identity of the target. The effect of this sort of intrusion on individuals' privacy, based on analysis of their behaviour, is just as much a matter of privacy concern as if the controller actually knows their identity.

We also support consideration in the future review of additional measures regarding mining techniques and technologies under Union law, such as location data. The current debates in the UK round the implementation of the e-privacy directive with regards to user consent for storing of cookies in users' terminal equipment illustrate well the tensions between the service providers' desire to collect as much information as possible, and the need for data protection; if implementation is going to end up passing responsibility to individuals to set their own browsers at the appropriate cookie-rejecting levels, and/or possibility to opt-out via complex multiple choices on industry websites, then meaningful protection will not be ensured and the situation will be no different from the current one.

The protection of individual's rights requires more than just considering definitions: it is also a matter of scope. Many of the poorer decisions made by regulatory authorities have been a result of the lack of consideration of individual rights. We believe that it is necessary that the powers of each Privacy Commissioner should explicitly be extended to the processing of personal data in circumstances where the processing at issue is alleged to cause a breach of Article 8 of the ECHR.

The Directive is founded upon this concept, but the concept is poorly incorporated into enforcement. Article 1 of Directive 95/46/EC begins with these words: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data". Recital 1 adds further clarification in that the Directive is a step towards "...preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms".

Recital 10 then amplifies what the "right to privacy" means. It states that "... the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms". Recital 11 then adds that "the right to privacy" in the Directive is intended to "give substance to and amplify those (provisions) contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data".

As the Directive already has links with Article 8, then it is a small step to specify in a revised Directive that each Privacy Commissioner should be explicitly able to enforce the Data Protection law in circumstances when Article 8 compliance is in question with respect to the processing of personal data. For example, it should have been possible for Commissioners to assess whether or not some processing is lawful (i.e. proportionate) in terms of Article 8 in cases such as international data sharing or with the retention of personal data.

The effect of this change would explicitly link the Human Rights and Data Protection regimes. It would reassure the public that Europe and law enforcement and national security agencies would be open to a constructive debate about data protection issues, whose outcome would then reassure the public that these agencies have not strayed beyond their allotted functions.

2.1.2 Increasing transparency for data subjects

We would support a general requirement for transparent processing, though after years of relatively fruitless discussions regarding simple or layered privacy notices and use of plain language, we are a little cynical on whether such a requirement can succeed in practice unless presentation and contents standards are also set by the data protection authorities. So we agree in principle with the idea of model 'privacy information notices' providing their design, placement and contents is brainstormed with stakeholders who understand behavioural economics, and user tested prior to release.

We are also wary of good transparency without meaningful choice, as happens now in many instances, where providers tell you comprehensively how they use your information, whom they

share it with and how long they are going to keep it for, but you do not in fact have a choice, unless you reject the whole service, which means no choice at all in some cases. So while we strongly support transparency and easy, accessible privacy policies, we also urge the Commission to only consider this as part of a whole package of pro-privacy measures, as all too often transparency in itself is an easy 'win' and only measure. In general we also think that comprehensive privacy notices should be part of the consumer contract, for e.g. in contracts for energy or cloud computing services, and as such be subject to and comply with unfair contract terms legislation.

Regarding the statement on children in the context of transparency, we do not consider that good information alone is going to help much with the specific issues around the protection of children and minors. This is in fact the only place in the Communication where children are mentioned at all, while we believe that more consideration should be given to privacy-related children's issues.

Finally, and regarding transparency, Privacy International fully supports extending mandatory personal data breach notification from the telecommunication sector to all relevant industries and sectors (including public). We have in fact been campaigning for such a measure to be introduced during the discussions on the revision of the e-Privacy Directive, and believe that extending the rule horizontally will ensure consistency between regulations, and will serve as a deterrent and incentive to companies to strengthen their security processes.

2.1.3 Enhancing control over ones own data

Privacy International would welcome an explicit reference to data minimisation in a revised directive as well as an explicit reference to, and clarification of, the right to be forgotten, which is particularly relevant in the context of social networking sites and cloud computing. We also suggest that the right to not be identified in the first place would be more effective in preventing future unnecessary data collection. There are many circumstances in which identification is not necessary at all for the provision of a service, and technologies are available that enable people to prove they are 'bona-fide' without the need to reveal personal information.

We support also looking at the ways that subject access, correction and deletion of personal information can be ensured without pain (for example through introduction of maximum response time limits and charge-free access) and looking at how to achieve better consistency in this respect between different member countries and data controller practices, which vary enormously at the moment, with the result that it is often very difficult for ordinary people to identify and correct errors.

Finally data portability is highly desirable, though it is a tall order to achieve it through data protection legislation alone – as essential prerequisites include software interoperability between various platforms, and open standards. We believe that this is absolutely essential in the context

of cloud computing and social networking, and we are pleased to see some leadership from industry, though there are worrying battles brewing in this space that may harm consumers.

2.1.4 Raising awareness

While not averse to raising awareness, we are doubtful that such exercises can be successful unless they involve high cost strategic, targeted multi-media campaigns over a period of time and using social marketing techniques. Lessons should be learned, for example, from other socially-related issues, such as drinking and driving and smoking awareness exercises. We suggest it would be more effective to target training and awareness raising campaigns at types of data controllers, and particularly small businesses or sole traders who increasingly monetise data without being aware of rights and obligations.

We believe that regulators have an important role in raising awareness of their own powers. Too often we are approached by European citizens seeking assistance and guidance, though are unaware of their own national regulator. We have even countered government departments with weak relationships with the regulators. Much more work is needed on promoting both privacy and the regulators. For instance, see the European Commission commissioned research on the promotional activities of national regulators.[1]

2.1.5 Ensuring informed and free consent

We agree with the analysis in the Communication regarding current Directive rules on consent (freely given, specific, informed) and consider that this is a fundamental issue to be resolved if data protection, especially online, is to have real teeth. So we strongly support the intention to examine, strengthen and clarify the rules on consent, including ensuring much greater harmonisation between practices and interpretation in different countries. We ask the Commission to consider specific banning of unfair trading practices such as requiring consent as a condition of receiving goods and services, as well as introducing the concept of 'revocability', i.e. the possibility to take away consent previously given (similar to a 'cooling off period' available in online shopping or consumer credit contracts).

2.1.6 Protecting sensitive data

We consider that any data can become sensitive in certain circumstances and/or if linked to other available data; modern technology makes it possible to use information that is not considered sensitive under the terms of the current Directive for discriminatory purposes. So in an ideal world we consider that all personal information should be treated equally and have strong protection. However, if current distinctions are retained, we would urge the Commission to add the following categories of personal information to the list: genetic, biometric, family history, mi-

1 KANTOR Management Consultants S.A., 'Evaluation of the Means Used by National Data Protection Supervisory Authorities in the Promotion of Personal Data Protection – Final Report, European Commission: Directorate-General Justice, Freedom and Security. Contract JLS/2007/C4/040: 30-CE-0185875/00-79.

nors, financial data, granular energy consumption data from smart meters. This list should be made non-exhaustive to allow for future technological developments.

2.1.7 Making remedies and sanctions more effective

We strongly agree with the proposal to ensure more effective enforcement, including redress, as this is the main weakness of the current data protection legal regime. Alongside other organisations, we have been advocating for the establishment of a judicial collective redress mechanism, both at national and European levels, as an efficient tool for consumer empowerment and business compliance. This should include representative actions by authorities, consumer and other civil society associations on behalf of individuals, as well as collective redress.

We also support strengthened sanctions, but a graduated range commensurate with the seriousness of data breach.

2.2 The internal market dimension

2.2.1 Increasing legal certainty and providing a level playing field for data controllers

Privacy International agrees that further harmonisation of national laws should take place given the cross-border nature of data flows, and not just European but generally global. However, we want to ensure that further harmonisation does not result in reducing the protection of individual privacy to the level of the weaker national laws, such as the UK. Examination of means to achieve further harmonisation of rules should have a clear preference for 'levelling up' to the highest common standards.

2.2.2 Reducing the administrative burden

We agree with the analysis in the Communication that the current system of notification should be simplified. Any such review should result in more coherent rules across member countries; the development of a 'model' notification should be considered. We would not support however abolition of the notification system, as it can have an impact both on enforcement and transparency.

2.2.3 Clarifying the rules on applicable law and Member States' responsibility

We strongly agree with the expressed need to ensure the same degree of privacy protections of EU data subjects, regardless of the geographic location of the data controller, and therefore support review and clarification of existing provisions. We believe that if services are targeted at EU citizens, the law of the person's (data subject's) country of residence should apply.

We support further clarification of applicable law, and note in this context the valuable Opinion 8/2010 issued in December 2010 by the Article 29 Working Party.

2.2.4 Enhancing data controllers responsibility

We would support the introduction of a specific 'accountability principle' for both data controllers and data processors as appropriate, providing this is not a substitute for responsibility to comply with data protection legislation, but an additional obligation. Such an obligation would mean that data controllers would have to demonstrate compliance with the legislation, and take appropriate measures to do so.

We would also urge the Commission to consider and clarify the roles and responsibilities of all those responsible for data processing, as in practice it is difficult for individual people to distinguish between a 'controller' and a 'processor', or a third party or a non-third party. Such relationships are increasingly complex, for example with the advent of cloud computing or in multinational companies. Therefore we consider that data protection obligations and liability for breaches should be extended to data processors and third parties. This can also be achieved through specific contract terms, as it is now the case in other types of consumer contracts. So for example, social networking sites can be required to have contracts providing minimum standards of data protection when engaging third party service providers.

Regarding PETS and privacy by design as mentioned in the general remarks above, we do not consider that the Communication gives these issues a fair hearing. We strongly believe that technical means and technological solutions can help people to be in control of their personal information and also help the enforcement efforts. Therefore we urge the Commission to include privacy by design as an explicit and mandatory principle in any new framework for data protection. This would include both processes and technologies and give the necessary spurs both to ICT manufacturers and data controllers.

2.2.5 Encouraging self-regulatory initiatives and exploring EU certification schemes

We do not believe that self-regulation is the right approach in the field of data protection, and not compatible with the nature of data protection as a fundamental right in Europe. Furthermore, since the natural self-interest of service and goods providers is to gather and share as much data as possible, and much of this can be done without the knowledge of the individual, self-regulation without any firm controls for its effective implementation would be the equivalent of putting the wolf in charge of the sheep. A good example of this is the self-regulatory proposal in the field of behavioural advertising which is widely considered by consumer organisations and others as a poor response to privacy protection needs. We do however strongly support co-operative ap-

proaches, and forms of so-called co-regulation, for e.g. industry codes that clarify and support binding rules.

We suggest that such initiatives are only truly effective when they are backed up by the prospect of strong enforcement action by independent supervisory authorities.

We have strong reservations about the value of 'privacy seals', which can often create an illusion of privacy protection without delivering anything additional to legal obligations, and we especially question the value of privacy seals operated by for-profit companies when the profits of the seal program are wholly dependent on the revenues from seal holders.

2.3 Police and judicial co-operation in criminal matters

We strongly support the proposed consideration of extending general data protection rules to the areas of police and judicial activity, and of harmonisation of any specific provisions considered necessary in this area. We suggest that 'blanket' across-the-board exemptions from data protection rules can rarely be justified for entire agencies or sectors – instead, specific exceptions or provisions can address particular difficulties that the normal application of data protection rules may pose for other important public interests such as law enforcement and national security.

A recent judgment from the UK National Security Tribunal[2] (with Privacy International) concluded that the Tribunal only had jurisdiction if the complainant was "a person directly affected" by the processing. By this, the Tribunal meant somebody like a data subject undertaking a subject access request and who was refused access to his personal data. By contrast, Privacy International was raising an issue not concerned with about subject access but about the general application of the 2nd and 8th Data Protection Principles (dealing with incompatibility of purpose and transfers outside the Europe) applying to the privacy of thousands and thousands of data subjects. The result was that, because of a technicality, Privacy International could not progress their appeal.

The revised Directive must ensure that a regulator in the area of national security can take effective action whenever he raises a matter of substantial public interest concerning the application of the national security exemption. The safeguard has not got to be limited to action by the "person directly affected" but should be extended to the regulator so that the regulator can intervene in cases when there is a serious data protection issue to resolve. The problem in the UK framework is that there is often "no person directly affected" available because national security actions are, by their nature, covert. Any person who is "directly affected" is very unlikely to become aware of such covert action unless the national security agencies make a blunder. And that is why the UK privacy protection in this national security area is so inadequate.

2 http://www.informationtribunal.gov.uk/Documents/nsap/PrivacyInternationalweb.pdf - For issues with respect to the Second and Eighth Principles, see details on http://amberhawk.typepad.com/amberhawk/2009/10/can-national-security-agencies-disclose-communications-data-or-anpr-images-to-anybody.html

2.4 The global dimension of data protection

2.4.1. Clarifying and simplifying rules for international data transfers

We agree with the analysis that the adequacy assessments are have not been satisfactory, and that the procedures need to be clarified and streamlined. The issue of export of EU consumer and citizen personal information to third countries is increasingly acute given the almost total globalisation of data flows, including expansion of cloud computing services and the extensive use of call centres outside the EU. At the same time experience with existing international agreements has not been so good. We suggest that the EU-US Safe Harbor Framework be included in this review, as several studies have documented massive compliance failures and lackluster enforcement.

So we support the review of these provisions, and would urge that any future international agreements between the EU and third countries should reflect the high level of protection of privacy in the EU.

We also recommend that greater resources be expended on capacity building on privacy and data protection in third countries. Already vast resources are applied to helping other countries with policing powers, amongst other regimes of law, and we believe similar work is required to help third countries develop an understanding of privacy and data protection laws and regulations. Particular attention is required for developing countries where the need for accountability and transparency in processing by both the public and private sectors is vital to the protection of democratic values.

2.4.2 Promoting universal principles

We strongly support the continuation of a strong leadership role for the EU in promoting effective international data protection standards. We also believe in the need to develop universal principles and global standards, and as such are active civil society players in the work of the OECD and APEC, and have contributed to the development of the civil society Madrid Declaration as part of the International Privacy Commissioners 2010 Conference effort to promote global privacy standards. We particularly ask the Commission to support and actively contribute to the current revision of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal data, as an opportunity to ensure greater convergence with the EU framework and enhanced protection for individuals.

2.5 Stronger Institutional arrangement for better enforcement

We have been campaigning for a long time for enhanced powers for the Information Commissioner in the UK, and therefore welcome the intention in the Communication to both strengthen the roles of the Data Protection Authorities (DPA), and the co-operation between them. We ask that there is greater harmonisation of standards for DPAs powers and particularly for their independence both material and in terms of who they answer to. We believe they should be answerable to Parliament rather than particular government policy departments. This would ensure both greater transparency and accountability to the public at large. We also believe that the appointment process should be considered within this review.

We would also support enhancing the role of Article 29 Working Party as a means to ensuring greater consistency within the EU. In particular its Opinions should take the form of Guidance to be adopted both in the Commission proposals and by DPAs on national levels.

Conclusion

We support the proposed next steps and look forward to discussions and co-operation with the Commission, the Parliament and the Council on the detail of the proposed framework.