

A comprehensive approach on personal data protection in the European Union

European Commission Communication COM(2010) 609

Vodafone's response

For more information, please contact:

Eirini Zafeiratou
Head EU Affairs
Rue Archimede 25
1000 Brussels
eirini.zafeiratou@vodafone.com
+32 478 319 807

Contents

Executive summary	1
Creating a truly comprehensive approach to personal data protection in the European Union – Vodafone's recommendations	1
<i>Introduction</i>	1
<i>Vodafone's recommendations</i>	1
1. A revised directive must continue to meet the original purpose of facilitating the international flow of data so essential for the development of the information economy.....	1
2. Europe needs a regulatory model that is principles-based, adaptable and accountable.....	1
3. A new directive must take a multi-tiered approach to regulated actors and facilitate the emerging role of the data intermediary.....	1
4. A new approach to data protection requires that we rethink the current directive's underlying concepts	1
5. In the absence of international political alignment, there are important and effective changes we can make to the Directive to improve privacy protection globally.	1
6. A deeper reliance on Privacy Impact Assessments can provide the flexibility necessary for all of these proposals.....	1
Vodafone's comments on the Communication	1

Executive summary

This paper, a follow-up to Vodafone's Future of Privacy white paper¹ from December 2009, is in two parts. The first part sets out thematically what we believe are the key areas of focus for the Commission as it deliberates the future of European data protection and privacy regulation, and makes a number of concrete recommendations. The second part responds specifically to the points raised by the Commission in its communication.

Here are the key themes for our recommendations to the Commission:

- 1. A revised directive must continue to meet the original purpose of facilitating the international flow of data so essential for the development of the information economy.** The Commission must further consider the role of regulation in helping to foster the sustainable development of the personal information economy – one that is open, competitive and secure – as well as respecting individuals' fundamental right to privacy.

[Click through to read our recommendations on international data flows](#)

- 2. Europe needs a regulatory model that is principles-based, adaptable and accountable.** The current approach does not create the right incentives for corporate cultures to understand the intrinsic value of privacy, invest resources in the creation of senior roles for privacy officers, develop privacy risk management programmes, or embed privacy in the design of technologies, products and services. The Commission must take account of research that points to principles-based approaches engendering better practices than rules-based approaches, and consider how to revise the Directive to ensure accountability without prescribing how organisations develop their privacy programmes or internal governance.

[Read recommendations on principles-based regulatory models](#)

[Read recommendations on adaptability](#)

[Read recommendations on accountability](#)

- 3. A new directive must take a multi-tiered approach to regulated actors and facilitate the emerging role of the data intermediary.** The roles that different organisations play in the information economy have expanded far beyond the simple classification in the Directive. To address this, we propose the introduction of the concept of the data intermediary. But the data intermediary is not a fixed concept. Different intermediaries will play different roles, and correspondingly, different types of requirements can be applied. This is best achieved through a principles-based and adaptable framework, as proposed above, that empowers regulators and industry to agree regulatory covenants for more specific circumstances, such as particular types of data intermediary or technology as they arise.

[Read recommendations on data intermediaries](#)

- 4. A new approach to data protection requires that we rethink the current directive's underlying concepts.** The meaning of personal data needs to be broadened, but accompanied by safeguards that are proportionate to the risks presented in any given context. The concept of legitimacy must remain open and flexible, and reduce the reliance on consent. And the entire European privacy framework must support technological neutrality – the ePrivacy directive is a contradiction of this principle and should be repealed and folded into a single revised and more neutral Directive.

[Read recommendations on personal data](#)

[Read recommendations on legitimacy and consent](#)

¹ http://www.vodafone.com/content/index/about/about_us/privacy/future_privacy.html. The Future of Privacy white paper was submitted to the Commission in response to the previous request for comment on the review of the directive.

[Read recommendations on technological neutrality and ePrivacy](#)

5. **Globalisation – While the solution to protecting privacy in a global information society is global standards, there are important and effective changes we can make to the Directive in the absence of international political alignment to improve privacy protection globally.** International transfers require a more effective means of regulation than the current methods. *Ex ante* approvals are unsustainable and deliver questionable protection for data in real terms. Binding Corporate Rules have the potential as a widespread mechanism for achieving better global information governance, but the Commission must: a) expand them beyond the corporate group; b) ensure they are flexible and adaptable to different business and governance models; and c) remove the monopoly of the national regulators in approving and supervising them. Instead, encourage the emergence of independent accredited assessors to assist with the review, approval and provision of assurance of organisations' BCR programmes. With regard to the review of applicable law, we call on the Commission to consider regulatory mechanisms beyond the law itself, such as the utilisation of regulatory covenants and the role that European organisations can play in helping to apply European privacy values to non-domiciled organisations.

[Read recommendations on international transfers](#)

[Read recommendations on global standards](#)

6. **A deeper reliance on Privacy Impact Assessments can provide the flexibility necessary for all of these recommendations.** The regulatory framework should create incentives for industry to adopt and use PIAs, and regulators should encourage the use and implementation of PIAs as part of the privacy management culture.

[Read recommendations on PIAs](#)

Creating a truly comprehensive approach to personal data protection in the European Union – Vodafone’s recommendations

Introduction

The principles upon which the Data Protection Directive is based remain germane and provide a sound foundation for privacy regulation even in the face of dramatic societal change. But rapid developments in technology have brought to light fundamental shortcomings with Europe’s regulatory framework for privacy. It is overly process-orientated, too heavily reliant on consent and legal formalities, and inflexible. And it places a significant burden on European businesses, giving them a competitive disadvantage to their competitors elsewhere in the world, and puts European consumers ultimately at a disadvantage in achieving real privacy.

Industry must indeed do better.² But the regulatory framework must create the right incentives for it to do so.³ If personal information is the new oil of the information economy⁴, the European regulatory framework as it is cannot provide the support that is needed to ensure sustainable economic development, nor keep pace with protecting the rights of individuals.

A new state of play is in its infancy – characterised by an evolving range of intermediaries, fast changing user behaviours, and new opportunities for consumer choice and control.⁵ While this new environment can support and facilitate the fundamental human right to privacy, it does not fall neatly within the conceptual framework of the current Directive, such as the notion of controllers and processors,⁶ nor does the current Directive any longer create the necessary conditions to deliver the best possible privacy outcomes for European citizens.

The Commission’s proposals to date have only reflected the existing state of play – they do not anticipate or accommodate the changes in technology, business models and behaviours that we can already see developing. But with a change in approach in this review of the Data Protection Directive, the Commission has an opportunity not just to correct the shortcomings of the privacy framework in Europe for today’s information economy, but to create a framework that can facilitate and shepherd emerging models of data use and ensure that the fundamental right to privacy can be protected in the long-term future.

We provided detailed commentary on the existing privacy regulatory framework in our [Future of Privacy white paper](#)⁷ and a related [discussion paper](#).⁸ In this document, we take that commentary

² FTC staff report, <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

³ Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books and on the Ground, *Stanford Law Review*, Vol. 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385. Available at SSRN: <http://ssrn.com/abstract=1568385>.

⁴ Meglena Kuneva keynote speech, Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/156>.

⁵ See, for example, the work of the Internet Identity Workshop, <http://www.internetidentityworkshop.com/about/>, the presentations of Microsoft’s Mark Davis, <http://www.networkworld.com/community/blog/microsofts-davis-privacy-your-digital-life-da>, or the work of Tim Berners Lee and W3C on the semantic web and policy languages for privacy, http://news.cnet.com/8301-1023_3-10195902-93.html.

⁶ Indeed, it is possible that a new conceptual framework for privacy could benefit from a reconsideration of the instrument for regulation within the EU, such as that proposed by European Data Protection Supervisor Peter Hustinx in advocating for a regulation rather than a directive. See http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf.

⁷ http://www.vodafone.com/content/index/about/about_us/privacy/future_privacy.html.

⁸ http://www.vodafone.com/content/index/about/about_us/policy/privacy.html.

one step further by making some concrete recommendations and responding specifically to the Commission's communication. In particular, we explore the emerging role of data intermediaries and propose concrete solutions that can create the right incentives for industry while continuing to ensure that European laws encourage a respect for the fundamental human right to privacy.

Vodafone's recommendations

1. A revised directive must continue to meet the original purpose of facilitating the international flow of data so essential for the development of the information economy.

There were two drivers behind the Data Protection Directive. One was to ensure a high level of protection for personal information across the European Union. But the other – indeed primary – driver was to ensure that Europe did not create unnecessary barriers to the international flow of data so essential to our economic development.

In the nascent information economy of the 1990s, this was an important first step. In the rapidly evolving and maturing information economy of 2011, this has become a critical requirement. In particular, personal information is now increasingly a vital economic asset in itself, of enormous value to the individual to whom it relates, to our wider economies, and to society as a whole. It can be used to authenticate the identities of those we deal with online; it can reduce the friction and complexity of dealing with multiple providers all collecting the same information; it can stimulate intelligent delivery of services by predicting behaviour and potentially reducing market waste; it can reduce cost and increase speed and convenience. We are seeing the emergence of a *personal* information economy.

The sustainable development of this personal information economy will depend upon creating the right regulatory framework. New concepts and safeguards will be required where the objective is not solely the protection of fundamental rights (although that will continue to be of ever greater importance), but equally the creation of a competitive, open and secure economic environment for the development of the ecosystem, such as ensuring data portability. This will also have important implications for the role of regulators.

Recommendations

- Explicitly recognise in the Directive the importance of personal data to the functioning and economic development of the information society.
- Explicitly recognise the role of the Directive and regulators in supporting the regulatory framework for the development of a competitive, open and secure personal information ecosystem.

[back to summary](#)

2. Europe needs a regulatory model that is principles-based, adaptable and accountable.

Principles-based. The European framework for privacy must incorporate a clearer statement of core principles and their intended outcomes that can provide the guiding direction of the law. The 2009 Madrid resolution is a good starting point, built upon solid international foundations.

There should be explicit recognition of the principle of proportionality in interpreting and applying the principles – activities that present greater risks to privacy should be subjected to heavier safeguards than those that do not. For example, the collection of pseudonymous information that is (in the context in which it is being collected, used or processed) not easily connected with another identity belonging to the individual concerned (such as their personal name, email address, or government issued identity number), should in principle be subjected to

a lighter set of safeguards concerning legitimacy and transparency than sensitive personal information in the clear.

Recommendations

- Include a clear statement of the core principles that provide the guiding direction of the law. The requirements for how the principles are to be applied must remain light and flexible – see recommendations below on adaptability.
- Include explicit recognition of the principle of proportionality in interpreting and applying the principles.

[back to summary](#)

Adaptability. The framework needs to be adaptable to cope with a changing environment. Rather than dictating fixed and precise rules for how industry can address privacy harms, it must focus on creating the right incentives for industry to develop creative solutions to privacy harms, such as through implementation of Privacy Impact Assessment methodologies, developing privacy-by-design principles in their product development processes and investing in privacy enhancing technologies.

To achieve this, the framework should embrace an effective system for creating covenants agreed with regulators to implement the Principles. Under such a system, regulators, companies, sectors or industries can work with regulators to agree specific regulatory covenants that implement the Principles. Regulators should be bound to review applications for such covenants within an open and accountable process (including, for instance, the hearing of evidence from interested parties) and issue determinations. Determinations should be subject to appeals to a tribunal or court, in turn helping to create case law interpreting the Principles. Once a covenant is approved, compliance with the covenant will meet the requirements of the Principles, unless and until it is challenged and overturned by a court.

The initial makings of such a system were incorporated into the existing Directive in Article 27, although they have not attracted sufficient interest. We believe this is primarily because the current Directive adopts an overly prescriptive, rules-based approach, leaving relatively little room or flexibility, and therefore little incentive to invest the time and resources.

Recommendations

- Include a system for creating regulatory covenants that enable more fine-tuned application of the principles to particular sectors, technologies or contexts.
- Include an obligation on regulators to conduct formal reviews of proposals for regulatory covenants in an evidence-based and open environment. Determinations must be subject to appeal.
- Treat compliance with an approved covenant as compliance with the Principles unless and until overturned by a court

[back to summary](#)

Supervision and accountability. Much has been said and written lately about the importance of accountability in improving the performance of industry in meeting the requirements of data protection and privacy law. Vodafone believes that accountability, as the outward assumption of responsibility, has a very important part to play in engendering the internal governance and assurance processes that will deliver better privacy outcomes in practice.

However, supervision is currently the monopoly of the national regulator, and this creates both a resource and skills bottleneck. What is more, the increased use of regulatory covenants, as we call for above, would place further pressure on the scarce public resources of our regulators. An

effective regulatory framework calls for effective framework of supervision. Therefore, we propose that regulators be required to accredit independent assessors who can be commissioned by companies to review their privacy programmes. Such assessors could also be empowered to provide reports available to regulators and even to the public.

The framework must also provide incentives for organisations to retain independent assessors and publish reports on their overall compliance; one strong incentive would be removing other filing, approval or notification requirements for those organisations that do so. This would be a far more effective mechanism in creating transparency and accountability than the existing documentary process of notification to regulators.

Importantly, this proposal would stimulate the creation of a secondary market in privacy compliance assessment, reducing the pressure on regulators as a resource bottleneck, but remaining accredited and approved by the regulator. It will lead to the development of a professional community of skilled privacy assessors with the goal of helping enterprises (public and private) develop the internal culture and professional support structures necessary to embed privacy compliance within their organisations.

Independent assessors would also be in a position to gather feedback and learning from the assessment process that can, without compromising the confidentiality of individual companies, act to inform and educate both the regulator and policy makers more generally about what is happening on the ground.

Recommendations

- Create a system empowering and obliging regulators to accredit independent assessors, for both whole-enterprise assessments and product- or technology-specific assessments.
- Develop incentives for industry to retain independent assessors to assess an organisations' compliance with the principles and publish reports in place of other regulatory formalities.

[back to summary](#)

In conclusion, the goal of the regulatory model should be to deliver better privacy management by organisations. In fast-changing and dynamic environments, prescriptive, rules-based frameworks do not allow room for organisations to innovate and adapt, such as by using impact assessments, privacy-by-design and the development of privacy enhancing technologies (recognised by the Commission as a high-priority goal). Instead, rules-based models engender a legalistic and formalistic approach.

The Commission must therefore seek to create a more clearly principles-based approach, allowing flexibility in implementation and providing incentives for organisations to embed the principles within their corporate culture. The above recommendations are essential to achieving this.

3. A new directive must take a multi-tiered approach to regulated actors and facilitate the emerging role of the data intermediary.

Classification of regulated actors. The current Directive places the onus of responsibility on data controllers. We believe the meaning and role of the controller remains relevant. However, the concept of the processor needs to be replaced with the wider and more adaptable concept of a 'data intermediary'. A data intermediary is an entity that does not control personal data but handles, or facilitates the handling, of personal data by another. That 'other' maybe another regulated controller, or it may be a private individual acting in their personal capacity. That 'other' may also be an entity outside the directive's jurisdiction.

The data intermediary represents one of the most dynamic and important areas of growth in many aspects of our information economy. Data intermediaries today play a wide range of

different roles – IT hosting, support and maintenance companies, cloud computing providers, social network providers, software application developers and so on. These data intermediaries often provide the capability for managing data by other persons, but do not conform to the more limited notion of a processor.

Equally, data intermediaries will often be both dependent on, yet independent of, other data intermediaries and actors, creating a complex web of relationships, many of them distributed across the world. Regulating the behaviour of data intermediaries in this environment will be a highly complex task, as we've discussed previously.⁹

Here are a few examples to consider:

Data intermediary examples

A data intermediary may host or process personal data on behalf of another, much as many IT companies do today. If the other entity is a controller, the data intermediary should have much the same obligations as apply today to a processor – it takes instructions from, and its role is subsidiary to, the controller, a chain-of-command form of accountability flowing from the controller down to the intermediary. If the other entity is not a controller (for example, a non-enterprise user), then the intermediary should still be subject to certain basic obligations.

Social network: A typical social network is another form of data intermediary. It provides a platform for a user to create a personal profile and to link that profile with other services and applications. It also provides a platform for users to upload, share and publish information about other people. The person directing this handling of data on the social network is not the provider but the end user. Of course, the provider will also be collecting in a more traditional sense (often as a controller) personal data about users – registration information, account-related activity, metadata, and so on).

Identity broker: Another example of the data intermediary is the data or identity broker. The data or identity broker is an entity that enables a consumer to host their data with the intermediary and to take the benefit of a number of services, such as data- or attribute-sharing, single-sign-on, identity federation, and so on. Such entities would be specifically set up to allow the consumer to control their own identity and personal data, and hence they would not fall into the category of controller for the data hosted as broker. Yet neither does classification as a 'processor' necessarily apply or provide adequate safeguards.

At the time of writing, the data or identity broker is a less well-developed business concept than the social network, although many years of technology and business standards development have been invested in bringing this model about for the benefit of consumers, businesses and the wider economy. And yet it represents just one of a number of valuable and important roles for data intermediaries.¹⁰

⁹ See our discussion paper on the Future of Privacy, available at http://www.vodafone.com/content/index/about/about_us/policy/privacy.html.

¹⁰ Vodafone has further explored these business models, and the regulatory issues they raise, in its white paper *Rethinking Personal Data: New value through end-user control, transparency and trust*, available at www.vodafone.com/privacy.

The responsibilities of the data intermediary. New forms of data intermediary are continually arising, and therefore the precise nature of the regulatory obligations that may be appropriate will not be known at the outset. The framework therefore needs to establish some universal safeguards for all data intermediaries, while creating the structure to flexibly create new regulatory requirements, and methods of enforcing those requirements, for new classes of data intermediary as they arise and as new risks emerge.

All data intermediaries that host or process personal data on behalf of another should be globally required to maintain adequate security and to be accountable for the management of data 'downstream'. Unlike under the existing Directive, these obligations should flow directly from the law, rather than requiring the controller to impose them via contract where both parties are subject to European data protection law.

Beyond these basic obligations, other safeguards and standards will often be required depending upon the type of role the intermediary plays. For instance, a typical social network must not only provide users with a secure platform for their data, but must also give users appropriate controls and settings for managing their online profiles. These are not the obligations of a controller (as it is the user that controls their online profile) but obligations particular to that type of intermediary.

Similarly, the social network intermediary should play an important role in helping end users act responsibly when posting information about *others* online. While the decision to post information online about someone else might be the decision of the end user, the social network provider, as the data intermediary, can act as a 'regulatory agent' for its own users through its relationship with them and through the terms, controls and features it provides. By requiring the social network provider to take steps to educate users and to provide tools and capabilities to end users, the end user's behaviour downstream can be appropriately regulated to comply with the principles.

Once again, this is a rapidly evolving field and it would be inappropriate for the law to fix in advance what these standards, safeguards or controls should be. To identify the most effective way to achieve conformance with the principles, regulatory covenants can develop more specific obligations implementing the principles and applying them to data intermediaries (or to particular classes of intermediary), with the participation of civil society and industry.

Recommendations

- Create a new category of 'data intermediary' as a regulated actor. This will encompass the current concept of the 'processor', but also provide for a wide range of other actors.
- Establish a baseline set of minimum obligations for data intermediaries, such as the need to maintain adequate security for data processed on behalf of others.
- Additional obligations for classes of data intermediaries should be developed via regulatory covenants.

[back to summary](#)

4. A new approach to data protection requires that we rethink the current directive's underlying concepts

Personal data. The Directive should place less emphasis on the importance of the definition of personal data. The ways in which information is connected with personal identities, and with the range and nature of identities themselves, will continually place stress on our understanding of what makes information 'personal', or how information can 'relate to' a person or in some way be 'about' a person. We propose that the definition of personal data be revised to be far broader than it is today. Correspondingly, the attendant obligations about how the principles are to be observed should therefore reflect, and be proportionate to, the nature and sensitivity of the data.

Such an approach would encourage a very different set of behaviours to those we see today. Rather than controllers examining the definition of personal data - and if on the view that that data is not personal data, ignoring the question of what obligations apply - they would be forced to make an assessment of the impact that any particular set of information, in a particular context, has for the individuals' concerned. This naturally introduces greater uncertainty for controllers. But this uncertainty should not be seen negatively; on the contrary, one of the frequent criticisms of European data protection in practice is that it is driven by form rather than substance, and often produces requirements that are disproportionate to risks. By broadening the definition of personal data, but providing for greater flexibility in how the principles are then applied, will require judgement on the part of those entrusted with ensuring compliance. The need for judgement will correspondingly foster the development of processes, such as privacy impact assessments, that will require a nuanced understanding of privacy risks and harms, rather than a formalistic "check-box" approach by applying rigid definitions and rules.

Recommendations

- Keep the definition of personal data wide and inclusive, but create a more flexible obligations regime. Regulators and industry need to use regulatory covenants to provide greater certainty on a case-by-case basis, providing clarity for given types of data and given contexts
- Eliminate the distinction between sensitive and personal data, and the fixed determination of additional safeguards for sensitive data (note – we accept that sensitive data should be treated with greater caution and higher safeguards, but we do not agree that the Directive should prescribe: a) what is sensitive, nor b) how we address fairness and legitimacy)
- All personal data should be processed fairly and lawfully
- Personal data to be processed only for legitimate purposes. In determining whether personal data is processed fairly and legitimately, the Directive should set out determining factors. For example, regard shall be had to certain factors, to include:
 - How sensitive is the personal data?
 - Was the data encrypted, anonymised or pseudonymised?
 - Was the individual informed?
 - Did the individual consent?
 - Was the use and collection part of a transaction to which the individual is a party or beneficiary?
 - Is the individual a child or of impaired understanding?

[back to summary](#)

Legitimacy and consent. The grounds of legitimacy should be open and should not lean upon consent as the default basis upon which personal data can be processed. Aside from the disruption this can cause to everyday processes, it places too great a burden on the individual. The role of consent in legitimising data processing reflects essentially a passive role for the data subject, as consent is by its nature permissive.

Today individuals are active participants in the information economy, publishing information about themselves, signing up for many services online and seeking ways of managing their own data for a wide range of benefits. This trend looks set to increase. In particular, the use of personal information now powers a significant portion of the online economy, as services are offered without charge to the end user but in return for the use of personal information and the display of advertising. The regulatory framework needs to offer an appropriate and proportionate means of legitimising this use of personal information that safeguards the individual's rights.

Excessive reliance on consent also forces organisations and individuals into dialogues that are forced and unnatural. If users are continually invited to consent in circumstances where they do

not feel they have much choice in providing or allowing their information to be used, then the act of consenting is de-valued and users' experience "privacy fatigue", clicking through consent boxes without paying attention to what it is they are presumably permitting. In such cases, alternative grounds for legitimacy must be identified.

Organisations should be able to make assessments of legitimacy but be held accountable for their decisions and actions. In addition, regulators should be empowered to work with industry where necessary to agree the circumstances and safeguards in which the legitimate use of data can happen. This will provide organisations and regulators with a more dynamic and flexible framework that can respond to new forms of use of personal information, but also adapt to the changing attitudes, knowledge and behaviours of individuals.

The framework needs to acknowledge that it is legitimate for organisations to collect personal information in return for other benefits provided to the individual, which may not go so far as to be part of a contractual relationship. The key to ensuring legitimacy is to find a fair and transparent value exchange and to develop other safeguards to protect the individual's rights.

The existing Article 7(f) of the Data Protection Directive provides a mechanism to enable a risk-based assessment of legitimacy, but it has often been poorly implemented (if at all) by Member States, and so there is reluctance by organisations in practice to utilise it.

Recommendations

- Keep the grounds of legitimacy open, even if there are pre-identified certain legitimate purposes. Consent must not be the default.
- Express acknowledgement that it is legitimate for organisations to collect personal information in return for other benefits provided to the individual, even where this falls short of a contractual relationship. Legitimacy may be based on a fair and transparent value exchange, and provision of other safeguards to protect the individual's rights.
- Give regulators the responsibility and power to work with industry where necessary to agree the circumstances and safeguards in which the legitimate use of data can happen. Again, this could be achieved through the use of regulatory covenants.

[back to summary](#)

Technological neutrality and ePrivacy. The existence of a specific directive for the electronic communications sector contradicts the stated desire by the Commission to ensure our regulatory framework is technologically neutral. The ePrivacy Directive creates a supplemental set of obligations based entirely on a fixed understanding of technologies and how those technologies are used, and this creates a distortion of the market to the detriment of users .

We recognise, however, that regulatory solutions must adapt to different technologies, business models, and service environments. The problem with addressing this at the level of a specific Directive is that it is inflexible, creates tensions with the main Directive and inevitably cannot respond quickly enough to changes in technology, business environments or user behaviours and attitudes.

We propose that the ePrivacy Directive be folded into the revised Data Protection Directive, but, as outline above, regulators need to be empowered and obliged to create regulatory covenants to address specific risks within sectors, in relation to technologies or particular business or operational environments. Such covenants must be based on evidence, and be capable of adapting to a changing environment.

Recommendations

- Repeal the ePrivacy Directive but ensure the revised Data Protection Directive is conceptually broad and encompasses the privacy risks that are sought to be addressed in the ePrivacy Directive. Embracing a wider range of data intermediaries will broaden the

reach of the Data Protection Directive and enable greater technological neutrality

- Empower and oblige regulators to create regulatory covenants to address specific risks within sectors, in relation to particular technologies or particular business or operational environments.

[back to summary](#)

5. In the absence of international political alignment, there are important and effective changes we can make to the Directive to improve privacy protection globally.

International transfers. While the solution to protecting privacy in a global information society is global standards, there are important and effective changes we can make to the Directive in the absence of international political alignment to improve privacy protection globally

We support the principle that that data protection should follow the data wherever it travels, and that accountability for ensuring this outcome should rest with the organisation exercising control over the data. But we question the extent to which the current regulatory mechanisms for approving international transfers have provided any real increase in privacy protection. They have certainly absorbed enormous resources in establishing formal legal arrangements intended to achieve that end, but in our view, at the expense of adequate attention to operational realities and effective global information governance. In particular, *ex ante* controls on international transfers must cease.

The Binding Corporate Rules model has only recently begun to provide a more workable model, built upon the concept of corporate accountability, but it remains limited to the corporate group and therefore of limited scope. It also remains heavily focused on forms, documents and rules, rather than on evidence of operational information governance in practice. But the potential of BCRs also remains stunted by the monopoly exerted by national regulators in conducting approvals of BCRs. This model is simply not scalable and will forever be held back by the limited resources and technical know-how of national privacy regulators.

Regulators can and should play a vital role in defining the principles for BCRs, but companies must have the flexibility to create BCRs for their specific business and operational requirements. They should also be able to retain independent accredited assessors to review and provide assurance as to their appropriateness and implementation. This will incentivise the creation of a secondary market in BCR assurance, thereby taking the strain away from national privacy authorities and allowing the market to create a skills and resources pool that can meet the demand for this model.

Recommendations

- *Ex ante* approvals of international transfers should cease to be a part of the framework.
- The concept of BCRs should be extended beyond the corporate group
- Independent assessors, accredited by the regulator, should be empowered to conduct BCR assurance reviews, thereby relieving the current resource and skills bottleneck.

[back to summary](#)

Global standards. Vodafone supports the Madrid Resolution and the initiative led by the Spanish AEDP to create a process for seeking international standardisation of privacy regulation. However, aside from re-considering the rules concerning applicable law, we encourage the Commission to look at alternative regulatory mechanisms that can help achieve greater international alignment, such as the widespread use of regulatory covenants. We believe formulated correctly, regulatory covenants are a flexible mechanism that can enable

engagement with a diverse cross-section of global companies, industry organisations, civil society and consumer groups. Even non-domiciled organisations often need the support of EU based partners in order to do business in Europe. These relationships can be utilised, and European organisations incentivised, to extend European privacy values to non-domiciled organisations.

Recommendations

- Embrace the use of regulatory covenants as a tool to help internationalise European privacy values by bringing together international companies and organisations in a constructive dialogue to achieve better privacy outcomes for European citizens.

[back to summary](#)

6. A deeper reliance on Privacy Impact Assessments can provide the flexibility necessary for all of these proposals.

Many of the proposals we have put forward above will require organisations to focus less effort interpreting strict and inflexible rules (a legalistic approach) and instead shift resources and focus on a deeper understanding of privacy risks and in developing effective solutions to address those risks (a risk based approach). The methodology increasingly talked about is the Privacy Impact Assessment. Vodafone believes that the effective use of PIAs can deliver better privacy practices and can incentivise innovation in approaches to privacy risks. The regulatory framework should create incentives for industry to adopt and use PIAs and regulators should encourage the use and implementation of PIAs as part of the privacy management culture.

One way to encourage organisations to implement PIAs and create a privacy management culture is to reward their use. For example, if an organisation could show (*e.g.*, through the use of independent assessors as proposed above in relation to supervision and accountability) that it has implemented and applied a PIA diligently; this should act as a mitigating factor when examining any alleged breach of the principles.

Recommendations

- Expressly acknowledge that a diligent implementation of PIAs should act as a mitigating factor in the event of any breach of the regulations.

[back to summary](#)

Vodafone's comments on the communication

The Commission has been accurate in its evaluation of the shortcomings of the existing European framework for the protection of privacy. Time and again, representatives of the Commission, consumer protection bodies, national regulators, and indeed industry commentators themselves have stressed the need for a more innovative, more flexible, more consumer-friendly approach to privacy protection. But innovation and flexibility cannot be prescribed through precise regulations – they are achieved when a regulatory framework sets expectations, identifies desired outcomes and creates the right incentives for these outcomes.

With this Communication, the Commission appears to have thoroughly considered the desired outcomes, but it also appears to be leaning in the direction of a more prescriptive, more rules-based approach to achieve them. Below, we identify areas where different approaches may better achieve those outcomes, and provide real-life examples from the corporate environment of where misaligned incentives are hindering achieving the Commission's goals and the real protection of privacy rights.

The Commission will consider how to ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms and the objective of ensuring the free circulation of personal data within the internal market.

Vodafone supports the Commission's recognition of the need to ensure that the data protection framework provides adequate protection for consumers in light of emerging technologies. But it is important to recognise that the most recent Commission activity on privacy, the ePrivacy Directive, is far from technology-neutral. That directive applies only to electronic communications providers, yet there are a range of technologies and – more importantly – significant market players, who fall outside its scope, creating an unlevel playing field that significantly hinders innovation by those industries it regulates while placing no barriers before other industries working with functionally equivalent data.

For example, regulated entities seeking to offer location-based services are subject to strict obligations imposed by the ePrivacy Directive when they use network data. But those exact services can be provided using unregulated data sources like GPS without the same onerous restrictions. In this directive, the Commission must recognise that calling out specific technologies or industries, rather than the purposes to which those technologies operate, will always create this unlevel playing field and will always suffer in the pace of technological evolution.

The Commission will consider:

introducing a general principle of transparent processing of personal data in the legal framework;

introducing specific obligations for data controllers on the type of information to be provided and on the modalities for providing it, including in relation to children;

drawing up one or more EU standard forms ('privacy information notices') to be used by data controllers.

Increasing transparency for data subjects and standard 'privacy information notices'

Vodafone supports and encourages the movement towards more transparency in the processing of personal data. We caution the Commission, though, to consider that prescriptive obligations and regulatory requirements up to date have not led – and cannot lead – to better, more functional privacy interfaces.

Any additional prescriptions on the provision of privacy information must take into account recent knowledge, acquired through quantitative and qualitative research, about the nature of consumer relationships with form disclaimers and disclosures. This research has well established

that consumers don't read 'privacy information notices'¹¹ and therefore any standard notice fails to achieve the transparent processing objective – the very reason the notice is served.

Such an approach must acknowledge the growing trend away from lengthy privacy notices and instead toward privacy icons, 'just-in-time' notices and other more innovative forms of 'notice' that may better meet the objective of a transparency principle (especially in increasingly small and mobile interfaces).¹² This evolution in design is occurring without any regulatory intervention at all – in spite of it, rather than because of it, with traditional data protection lawyers at every step of the way objecting that such approaches do not meet the requirements of their country's laws.

In this vein, the Commission's reference to considering the different 'modalities' for providing a privacy notice is welcomed, but no single 'modality' for delivery of privacy information should be prescribed by law, unable to keep pace with developments in technology and user experience that will impact the delivery of such notices in the future.

Additionally, before enacting any rules specific to children's privacy, the Commission should consider the difficulty in determining whether any individual in the online environment is a child. Although it might be possible to predict a rough age of a user through the analysis of usage patterns, this is not an exact science (and further would have its own privacy implications relating to profiling) and we would be unable to achieve the certainty required for legal compliance.

The Commission will examine the modalities for the introduction in the general legal framework of a general personal data breach notification, including the addresses of such notifications and the criteria for triggering the obligation to notify.

Given the Commission's commitment to technological neutrality, we would urge any breach notification obligations adopted here to create a level playing field with those imposed upon electronic communications service providers in the ePrivacy Directive's recent revision.

The Commission will therefore examine ways of:
strengthening the principle of data minimisation;

As written, the directive's terms provide strong safeguards against the collection of excessive personal data: It can be collected only for a specified, explicit and legitimate purpose; the collection must be adequate, relevant and not excessive; and once it is no longer needed for the specified purpose, it must be destroyed or anonymised. It is not the principle that requires strengthening but perhaps organisations' awareness of the principle and how it should be implemented in practice, and the enforcement actions available to national regulators where instances of a breach occur.

improving the modalities for the actual exercise of the rights of access, rectification, erasure or blocking of data (*e.g.*, by introducing deadlines for responding to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle);

The fundamental purpose behind the right of access is to allow an individual to know what data an organisation holds about them, and to therefore be able to correct any inaccuracies or request the removal or deletion of irrelevant information. In this way, the right of access is

¹¹ See, for example, George Milne, Andrew Rohm & Shalini Bahl, "Consumers' Protection of Online Privacy and Identity" 38(2) *The Journal of Consumer Affairs* 2004, 217 at 224. See also George Milne, Mary Culnan & Henry Greene, "A Longitudinal Assessment of Online Privacy Readability" 25(2) *Journal of Public Policy & Marketing* 2006, 238.

¹² Taking into account, for example, the qualitative research done by the members of the Carnegie Mellon CyLab Usable Privacy and Security Lab, <http://cups.cs.cmu.edu/>, and other researchers into privacy nudges and behavioural economics.

interconnected with the privacy rights of the individual; the right works as a deterrent from collecting excessive or unnecessarily intrusive information and as an incentive to keep records accurate and up to date. While the right to access, correction and deletion is fundamental to an individual's ability to exercise his or her fundamental privacy right, the actual practice of Subject Access Requests has become a quagmire of expensive compliance mechanisms at great cost to companies with little associated benefit to individual privacy.

For example, the Vodafone UK privacy team receives (and complies with) approximately 2000 SARs per year. More than 50 percent of the headcount of the Vodafone UK privacy team is diverted to dealing exclusively with these requests, and approximately 50 percent of its budget is dedicated to pure compliance with this specific principle (to the great expense of all others). Vodafone UK monitors the nature of the requests received and has found that a majority of them could be described as frivolous, in the sense that the spirit of the request is not consistent with the purpose of the rights granted by the directive.

Instead, SARs are made in cases where the reason for requesting access is completely unrelated to privacy rights. For example, pay-as-you-go customers (by definition) do not receive itemised bills; instead, they tend to make a SAR anytime they require a copy of their call records. Similarly, customers use a SAR to request phone records for use in civil litigation, visa applications or employment disciplinary matters. Months of raw network call records will typically run into the hundreds or thousands of pages. The time and cost of retrieving and providing these records costs Vodafone UK hundreds of pounds per request, yet under UK regulations, Vodafone may only charge a £10 fee for this service.

The disproportionate burden of complying with SARs is further compounded for Vodafone as an organisation subject to the European Council's Data Retention Directive. Because of obligations imposed by this directive, Vodafone has no choice but to retain a massive amount of traffic data – including call logs – for the mandated period of time. Once retained, Vodafone must provide this personal data to any subject who requests it, and the provision of these records to the requestor is a costly and time-consuming exercise. Where an organisation is legally obliged to retain such a large amount of data, that organisation should be entitled to charge a higher statutory fee for providing access to the data.

clarifying the so-called 'right to be forgotten', *i.e.*, the right of individual to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired;

It is hard to argue that consumers don't deserve a right to be forgotten. What is up for debate, though, is the extent to which consumers don't currently enjoy this right. For example, data is subject already to the requirement that it be deleted when no longer necessary for the justification for which it has been collected. Similarly, consumers enjoy the existing rights of data correction and data deletion. If consumers do not currently exercise these rights, or if companies do not adequately respect these rights, what is needed is not additional rights, but better awareness and enforcement of those that exist. Without awareness and enforcement, any new right will be similarly inadequate to meet the goal of true privacy.

We are concerned in particular that this proposal is merely a 'Facebook clause', being driven by a concern with a particular category of services. Indeed, as we discuss above, the problem is really with the categorisation of social networking within the existing framework. In our view, social media platforms are a new form of data intermediary. What is needed is not new or additional rules for controllers regarding the deletion of data, but a new approach to regulating these new forms of service provider. As we discuss in the example above, the focus for social networks should be less about rules relating to the retention of users' profiles (as users are generally in control of their own profiles), but instead about how to incentivise the development of features, tools and awareness provided to users to help them manage their privacy online.

Some advocates have also posited that a right to be forgotten must include the technical capability for data to automatically age out of existence, a requirement that could have significant unintended consequences for our historical record. Keep in mind that much of our knowledge of history is based on the lucky happenstances of the survival of data. If data automatically deteriorates, then there may be no 21st century equivalent to, for example, *The Diary of Anne Frank*.

complementing the rights of data subjects by ensuring 'data portability', *i.e.*, providing the explicit right for an individual to withdraw his/her own data (*e.g.*, his/her photos or a list of friends) from an application or service, as far as technically feasible, without hindrance from the data controllers.

Vodafone strongly supports the concept of data portability' and believes this is one proposal for additional individual rights that could in fact increase the sum total of privacy innovation and improve competition in the information economy.¹³ Data 'lock-in' decreases company willingness to compete on privacy protectiveness and makes them willing to change the rules of the game on data use for existing users of their services. If that service has reached the happy equilibrium of network effects, no interoperability, and no portability, then a significant breach of consumer trust must occur before their users will change their custom (and even then, as recent controversies show, users may not depart). On the other hand, if users can vote with their business, and can go elsewhere with ease and without losing the benefits accrued, then they can and will cause greater commitment to and investment in privacy-protective interfaces from the companies they do business with.

The Commission will examine ways of clarifying and strengthening the rules on consent.

As discussed above, current interpretations of the Directive overly rely on consent as the sole justification for processing personal data. That is not to say that there is no need for adequate notice and information to be provided to individuals about data processing. Notice must be given so that individuals understand how their information will be collected and used and – where unforeseeable or particularly intrusive use of personal data is contemplated – consent should form the basis for this type of processing. But clarity is necessary in the limits to which consent is the appropriate justification for certain types of processing.

We've discussed the consent issue above, so let us provide here an example of how the over-reliance on consent plays out in the real world of industry. As an example, Vodafone UK receives a significant number of requests to cease processing data on the grounds that to do so would cause damage or distress (for example, data from a credit reference file). The individuals who assert this right believe that, once they withdraw their consent for Vodafone to process their personal data, any further processing will be contrary to their rights under the directive. But Vodafone and other entities – like credit reference agencies and credit providers – have a legitimate interest in the processing of that data even after the individual has withdrawn consent, – industry needs reliable information upon which to assess credit risk.

In this context, Vodafone UK is able to rely on articles in the UK Data Protection Act 1998 that provide for processing without consent where necessary in the legitimate interests of the data controller or third parties, provided such processing does not prejudice the legitimate rights or freedoms of the data subject. But in other countries where Vodafone operates, the legitimate interest justification is given significantly varying degrees of effectiveness depending on its national implementation. Vodafone operating companies throughout the rest of Europe are required to rely on consent to record information on a customer's credit file (even after that customer has attempted to withdraw consent). Where individuals are not able to withdraw their consent for legitimate processing activities, then consent should not be the legal mechanism upon which that processing is based. This is just one example of instances where member states

¹³ Vodafone's CEO made this point at the Mobile World Congress in February of last year.

have misinterpreted and mis- implemented the justifications for legitimacy of processing. Clarity around this point would be very welcome.

The Commission will explore different possibilities for the simplification and harmonisation of the current notification system, including the possible drawing up of a uniform EU-wide registration form.

While a simplification of notice requirements would be a step in the right direction, the Commission must consider the shortcomings of existing notification and approval regimes. Multi-year backlogs in the approval process and onerous filing requirements direct company resources toward compliance in this one area at the expense of programmes that could create true consumer privacy, and divert regulator resources away from their appropriate oversight and enforcement roles. Neither industry nor regulators can continue to operate in this manner, and consumer privacy is not furthered by these regimes. This effect is particularly felt in countries where every international transfer of information must be notified and approved.

We believe that a greater and more meaningful contribution to transparency can be achieved via independent assessment and reporting of organisations' privacy programmes, as proposed above in relation to our recommendations on supervision and accountability. Such assessments can take a more holistic view of an organisation's overall programme, including governance and accountability mechanisms, use of impact assessments and commitment to embedding privacy risk management within the corporate culture.

The Commission will examine how to revise and clarify the existing provisions on applicable law, including the current determining criteria, in order to improve legal certainty, clarify Member States' responsibility for applying data protection rules and ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller.

In a digitally connected and increasingly mobile world, it's not just that users interact with service providers or other users across geographic borders, or that their data constantly moves across borders, but users themselves are mobile and take their mobiles (and services) with them. The effectiveness of nationally based legal regimes for regulating privacy will remain challenged in a global and mobile information economy. International cooperation and standardisation is the best hope for addressing the geographic limitations of applicable law.

But the Commission should also take account of alternative regulatory mechanisms beyond law. For instance, incentivising and encouraging Europe-based organisations to reflect the requirements of European privacy law and values in their dealings with suppliers, partners and other industry participants can act as a powerful influence on the way non-domiciled organisations address these issues, without necessarily always finding a jurisdictional hook. In addition, inclusive co-regulatory mechanisms such as we have discussed above can enable global companies, civil society and consumer organisations, including non-EU regulatory bodies, to work collectively to find solutions to privacy challenges that extend the reach of EU privacy principles beyond the geographic boundaries of Europe.

The Commission will examine the following elements to enhance data controllers' responsibility:

Making the appointment of an independent Data Protection Officer mandatory and harmonising the rules related to their tasks and competences, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;

Including in the legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;

Further promoting the use of PETs and the possibilities for the concrete implementation of the concept of 'Privacy by Design'.

The Commission, clearly unhappy with the progress companies have made in embedding respect for privacy within their wider corporate cultures, proposes to achieve such innovation by

mandating it through regulation. But more regulation won't result in more innovation – it is likely to be the converse. When the motivation for solving privacy shortcomings is rules-based, it is run by lawyers. And compliance-oriented motivations do not prompt companies to allocate resources or engineers correctly to aim for groundbreaking business methods, governance processes or technical solutions. The proposal for a mandatory Data Protection Officer is an example of a line of thinking that more regulation will force organisations to internalise privacy requirements and create a more privacy-respectful culture. Similarly, privacy-by-design is not something that, in itself, can be mandated by regulation. But intelligently crafted regulatory incentives can be built to encourage this movement. Instead, in today's world of global data flows, organisations need to see the value of appointing an officer in charge of privacy programmes and compliance, or in an approach to privacy risk management that seeks to engineer solutions through better product design, rather than the legalistic 'bolt-on' approach favoured today by most lawyers. The Commission must think through the most effective options for incentivising these decisions within organisations, not simply coming up with additional prescriptive rules.

The right approach, therefore lies in determining the right outcomes companies are expected to achieve, incentivising the right behaviours and admonishing the wrong, but not in being overly prescriptive with respect to the methods companies use to achieve them. We fear that the proposals here do not further that approach.

The Commission will:

examine means of further encouraging self-regulatory initiatives, including the active promotion of Codes of Conduct;

explore the feasibility of establishing EU certification in the field of privacy and data protection.

As discussed in our Future of Privacy white paper, the active promotion of Codes of Conduct or regulatory covenants is essential to creating a second-generation privacy framework and the only way to ensure that a sustainable, global privacy framework can thrive.

Vodafone supports the concept of an EU privacy certification, as discussed above in relation to supervision and accountability. Independent experts who are able to assess and provide a privacy seal of approval is going to alleviate the burden on regulators and foster consumer confidence in the safety and protection of their personal information.

The Commission intends to examine how:

to improve and streamline the current procedures for international data transfers, including legally binding instruments and 'Binding Corporate Rules' in order to ensure a more uniform and coherent EU approach via-à-vis third countries and international organisations;

Global data flows are an essential economic reality; almost every business innovation in recent years has depended upon the movement of data without regard to geographic boundaries. Data protection should of course continue to follow the data wherever it travels, and accountability for ensuring this outcome should continue to rest with the organisation exercising control over the data.

The challenge is finding a model that achieves this in practice without imposing disproportionate burdens on organisations, economic development or innovation. The existing regulatory structure for international transfers has absorbed enormous resources without providing any real increase in privacy protection. Binding Corporate Rules have only recently begun to provide a more workable model built upon the concept of corporate accountability. But limitations on its use – within one corporate group, solely for controller to processor transfers within that group – make it only a partial solution. Subject as it is to national regulator approval and their limited resources and technical knowledge, the model is simply not scalable for today's dynamic and mass-market information processing environment.

It is time to move away from ex ante controls or formalistic and documentary solutions for trans-border data transfers and instead create conditions for accountable global information governance. If Binding Corporate Rules are to offer a realistic model for wider use beyond the corporate group, we need to find alternative options for approval and assurance. Any new framework for international transfers must allow companies the flexibility to create BCRs for their specific market requirements, but require independent assurance of BCRs and thereby encourage the creation of a secondary market in 'BCR assurance': A market for independent assessors accredited by regulators to conduct assurance monitoring and reporting for organisations on commercial terms, thereby taking the strain away from national privacy authorities.

Vodafone strongly supports greater use of co-regulatory mechanisms, which can encourage internationalisation through involvement of global companies, civil society and consumer organisations, including non-EU regulatory bodies. And within a multi-tiered framework, European-based organisations that provide the core technology, connectivity or platforms needed by other service providers to reach European users could act as regulatory agents themselves, setting standards and principles for their user and developer communities that reflect EU privacy values. Global organisations can achieve global standards in ways and at speeds that governments cannot, while government enforcement can give teeth and encourage participation in these standards in ways that have been inadequate up to now. Greater utilisation of these mechanisms, and a framework that encourages and enforces them, could go a long way in addressing the many of the problems of the existing framework.

#