The future direction of EU Data Protection and privacy regulation

Views of Vodafone

Executive summary

A robust, effective and sustainable regulatory framework for privacy and data protection is one of the most important requirements for the health of our information economy.

The information society has evolved in ways that were not anticipated when the existing Directive was adopted. Attitudes, behaviours and expectations concerning privacy are changing rapidly; the regulatory framework needs to keep pace if it is to retain its legitimacy. And these changes will only accelerate over the next 15 years. It is already clear that we need to fundamentally re-think the privacy framework, which is looking increasingly clumsy and out of step with the requirements of both consumers and business.

The current 'first-generation' framework introduced privacy and data protection regulation for the first time in Europe. **We now need to design a 'second-generation' framework, with the broader and more ambitious goal of establishing a culture of privacy**.

This involves several key steps:

1. **The regulatory model needs to be reoriented towards an 'accountability model'**, which:

    - provides more proportionate responses to risks and is more adaptable as new technologies, risks or behaviours emerge (and old ones recede);
    - is technologically neutral and evidence-based;
    - incentivises and rewards innovation in finding solutions to privacy problems and harms; and
    - recognises globalisation and allows us to adopt workable strategies to advance privacy globally, whilst the political community continues to seek consensus.

2. **A 'multi-tiered' approach is needed which recognises that non-enterprise users now have a substantial impact on privacy.** In addition to enterprise data controllers, many 'non-data' handlers play a vital role in creating the tools and capabilities for information processing (*e.g.,* software providers, social media companies and other intermediaries). A multi-tiered approach means different actors in the information society bear levels of responsibility depending upon their roles. In particular, 'non-data' intermediaries need to become active stakeholders within the regulatory framework alongside data 'controllers'.

3. **A number of core concepts need re-evaluation:**

    - Dependence on the definition of personal data has produced an 'all or nothing regime' where everything depends upon its meaning and has impeded our understanding of how to protect privacy. Similarly, the controller / processor relationship is too binary to reflect the myriad relationships we now see.
    - We need to ensure that the assessment of legitimacy is proportionate and risk-based. Excessive reliance on consent de-values it. We need to better understand how to attain a fairer value exchange for the individual, but not at the expense of inhibiting the very products and services that give so much value in other ways.

- We need technological neutrality. The ePrivacy Directive discriminates against electronic communications operators and is arguably harming the protection of European citizens' privacy in a number of areas.

4. Create workable solutions to globalisation:

- 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. Binding Corporate Rules have made important progress, but if they are to offer a realistic model for wider use beyond the corporate group, we need to find alternative options for approval and assurance. Independent assurance models should be explored.

- Co-regulatory mechanisms 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.

- Even in the absence of any wider international cooperation or standardisation, EU policy makers must engage with the US on privacy reform.

The future of privacy

Vodafone's perspective on the future direction of EU Data Protection and privacy regulation

Introduction

A robust, effective and sustainable regulatory framework for privacy[1] and data protection is one of the most important requirements for the health of our information economy. This paper sets out Vodafone's view on the future for privacy regulation. Europe has a legacy of almost 15 years of data protection and privacy regulation, and a great deal of insightful work has already been produced on how well this has served European citizens and how this regime can be adapted for the future[2]. This paper does not attempt to survey the existing privacy and data protection framework, or to repeat what we believe has been adequately addressed by other contributors to the debate, but rather focus on how privacy regulation should be adapted for the challenges we believe we will face in the next 15 years.

Key trends

The privacy of individuals has been and will continue to be affected by a number of key trends:

- The need to process personal information for economic and social reasons, such as the delivery of e-commerce, remote working and e-government.
- Technological developments, most significantly in the ever-increasing importance and popularity of the internet and its convergence with mobile technologies and platforms.
- Continued globalisation of the economy and society, facilitated by these technological developments.

While we look back at the last 15 years in wonder at how the information society has changed, Vodafone believes this will accelerate over the next 15 years through continued changes in technology, user behaviour and market dynamics:

Technology

- Our information society will be characterised by always-on ultra-broadband connectivity, constantly present with the user wherever they are through highly mobile and personal devices powerfully supported by applications, services and data running in the 'cloud'. Expressions like 'going on the internet' will be outmoded – the internet will be part of the present, augmenting it. We will use mobiles to make payments, access healthcare, and gain access to buildings or roads.
- Technology platforms, including mobile, will continue to become more open, with seamless login between applications and domains, enabling the user to search for, discover and use an ever-expanding range of interoperable services and applications.
- This will be a user-centric environment, where the network and services will adapt and be personalised to the user, based on openly available user attributes like presence, context and location. Intelligent networks and services will be capable of learning and adapting – performing simple everyday tasks intelligently in the background, liberating the user to do more meaningful tasks.

[1] Throughout this paper we refer to 'privacy', rather than data protection. We don't attempt to define privacy (which tends to evade satisfactory definition) , but intend for it to encompass matters of data protection while recognising that there may be other privacy concerns impacted that do not necessarily involve data processing.

[2] Rand Europe report (http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf); European Commission Legal analysis of the Single Market for an Information Society.

User behaviours

- Users will access content from any device or platform, co-create and mashup their personal content, like photos and videos and text with commercial content, while interacting with each other.
- Greater connectivity between user communities will enable all manner of activities to be framed by peer groups and the 'wisdom of crowds', changing established relationships between individuals and companies, Governments, regulators. This will challenge established notions of trust, as users become more assertive and activist, relying upon authentic and trusted peer groups for authority, and less upon corporate or Governmental sources, and in turn contributing their own viewpoints.
- Digital natives will grow into digital nomads, expecting and demanding a seamless convergence of the internet and mobile worlds.

Market dynamics

- Innovative or disruptive technologies will continue to surface, challenging established business and regulatory models, and offering new possibilities (and risks) for consumers.
- The network effect of billions of potential online and mobile users reachable by service providers and developers with low development costs will witness a huge spur to innovation. This innovation will seek to leverage the technological capabilities of mobile devices, networks and open and interoperable platforms to create intelligent and compelling applications that are personalised, location aware and context sensitive.

Futurology is a difficult science. But whatever the future holds, it is certain that these developments will continue to have profound implications, both for user expectations and the culture of privacy, and for the regulatory framework that should reflect and support them.

These developments have brought, and will continue to bring, enormous economic and social value to societies around the world – helping businesses large and small[3], improving access to healthcare[4], facilitating social change and engagement[5]. But it doesn't take too much imagination to see that there are important challenges for the continued protection of privacy. For instance:

- Ever-present connectivity, which brings so many benefits, also creates the potential for constant monitoring of identities and locations, leaving digital footprints throughout our lives and ever expanding 'digital dossiers'.
- Almost every individual has the capability to harness enormous computing power at any time to create, capture, manipulate and share information about others and themselves, making each of them a controller of data about others as well as being the subject of data about themselves.
- The intelligent and intuitive applications that help us organise and run our lives can be created by developers from anywhere around the world, with perhaps little or no attention given to European privacy values.

But these trends also point towards new possibilities:

- Greater connectivity and engagement among users may lead to increased peer group support mechanisms, helping users navigate the digital environment and accelerating media literacy and awareness of privacy and other online risks.

[3] Upwardly Mobile In Africa – Business Week Special Report; 24 September 2007 (http://www.businessweek.com/magazine/content/07_39/b4051054.htm?chan=rss_topEmailedStories_ssi_5).
[4] mHealth for Development – a UN / Vodafone Foundation publication (http://www.globalproblems-globalsolutions-files.org/unf_website/assets/publications/technology/mhealth/mHealth_for_Development_full.pdf).
[5] Wireless Technology for Social Change: Trends in Mobile Use by NGOs – UN / Vodafone Foundation publication (http://www.globalproblems-globalsolutions-files.org/unf_website/PDF/wireless_tech_social_change_trends_in_mobile%20use.pdf).

- Increased activism using the viral effect of the network ensures that collective voices are heard by corporations, governments and regulators[6].

A vibrant and innovative information economy is critical to our society's progress. The challenge that we face is ensuring that the protection of privacy, so important to our information society, "*does not constrain the innovation that's around the corner*"[7].

The need for change

We need to reorient the existing 'first-generation' privacy framework towards a 'second-generation' framework designed to meet the challenges in protecting and safeguarding privacy in an ever more dynamic information society

The existing legal framework for the EU has established a vital basis for data protection and privacy, and has been more influential in shaping approaches towards privacy and data protection around the world than any other framework. However, this 'first-generation' framework needs to change if it is to remain fit for purpose.

Change must not reduce the obligations on organisations to manage and protect privacy. But what is needed is a reorientation of the framework to cope with the fundamental changes that have already occurred and accommodate the changes to come, many of them unforeseen and with unknown consequences. We refer to this as a 'second-generation' framework. If privacy is to survive, this second-generation framework should have as its broad and ambitious goal the emergence of a culture of privacy across all sectors of society.

How much change, and how soon?

We need to seize the opportunity now for significant reform if we are to determine the future direction of privacy in the information society

A number of reports have been commissioned that have asked about the scale and timing of change[8] – should we just amend now but leave the bulk of the Data Protection Directive intact, or undertake a wider review?

We believe we are on the verge of dramatic changes in the information society. If we do not act quickly, perhaps the question will not be 'what is the future of privacy', but 'does privacy have a future?' Change will take time; policy makers need to be wary of doing too little, too late. If we tinker at the edges, we will miss the most important opportunity to reorient European privacy law for the future.

The following areas highlight key changes we believe are essential to creating a second-generation regulatory framework for privacy that is fit for purpose for the next phase of growth in the information economy. These are interrelated and interdependent:

1. The Regulatory Model
2. A Multi-Tiered approach
3. Underlying Concepts
4. Globalisation

[6] In February 2009, Facebook backed down from making changes to its terms that impacted its users' privacy after its users protested – "Facebook backs down on privacy terms", ZDNet UK, http://news.zdnet.co.uk/internet/0,1000000097,39616157,00.htm.
[7] Tim Berners-Lee, 1 March 2007, speaking before a panel at the US House of Representatives.
[8] RAND report; European Commission Legal analysis of the Single Market for an Information Society.

1. The Regulatory Model

We support the core principles of data protection, as set out in international instruments and in the Data Protection Directive. But the existing model should be re-orientated towards an accountability model better suited to protecting privacy in a dynamic information-based economy

The principles on which the Data Protection Directive is founded remain sound – legitimacy, purpose specification, collection limitation, transparency, data integrity, information security, access and correction. These have a common heritage with other international privacy principles – the OECD Guidelines[9], the Council of Europe Convention[10] and the more recent APEC Privacy Framework[11]. In this, we concur with a number of reports on the Directive[12].

But many of the mechanisms through which the principles are imposed have been exposed as overly prescriptive, paternalistic and inflexible, with an excessive focus on notification, legal formalities and regulatory approvals. The lack of a data protection / privacy risk management methodology has meant that to many businesses, the burden of compliance is out of all proportion to the benefit to the individual or society as a whole[13]. Some studies reveal a mismatch in perceptions of privacy concern between regulators and consumers[14]. Wide variations across Member States in the implementation of the Data Protection Directive and its application by national regulators, and inequalities in enforcement, add to this sense that the regime is unbalanced.

All too often, the response to a privacy problem is to paper it over with another contract, another boilerplate disclosure, another tick box for consent. This generally leads to less user attention and comprehension, less knowledge of practices, more obfuscation and confusion. There has been a notable lack of innovation in the 'privacy dialogue' between individuals and organisations that collect their data, and this arguably comes from a stalemate between companies and regulators.

Reorientation

Vodafone believes the model of regulation needs to be reoriented towards what is often referred to as a principles-based 'accountability model'[15]. What this means in general terms is that the European privacy framework should reiterate the principles upon which privacy is to be respected (and here we see little need to diverge substantially from the principles as we find them in the Data Protection Directive and other international instruments). However, rather than defining the means and mechanisms by which organisations achieve conformance with the principles, the framework needs to identify the outcomes that are expected.

Beneath this over-arching framework of principles and outcomes, there needs to be established a 'tool-kit' of measures and regulatory instruments that will equip regulators to play an active role, working with industry, civil society and other stakeholders, to identify and agree proportionate and effective measures that ensure outcomes are achieved using risk management methodology. An example of this approach is the use of regulatory covenants, or co-regulation. In this case, regulators and industry would identify areas of risk within given industries or across whole sectors, and thrash out a regulatory framework that would represent an agreed method of achieving the outcomes based on the principles.

[9] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[10] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
[11] Asia-Pacific Economic Cooperation (APEC) Privacy Framework. http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html.
[12] RAND Europe report.
[13] A typical example is the storage of personal data on unsecured excel spreadsheets locally, rather than uploading to a remote but secure server, to avoid difficulties with international transfers.
[14] Osborne Clarke, March 2009.
[15] Variations on this have been advocated by others, such as the recent multi-stakeholder report from the Centre for Information Policy Leadership (October 2009), and the RAND Europe report.

A core part of any such dialogue should be the hearing of evidence from interested parties, including consumer and user groups. This is particularly important as we witness shifting attitudes, behaviours and understanding among consumers about privacy. Attitudes amongst users are changing faster than those amongst regulators, leading to the risk that the legal framework is ignored or loses legitimacy. This approach will enable all stakeholders to frame the dialogue according to the actual evidence of risks presented, and therefore ensure the regulatory framework is proportionate. Failing a deal, regulators must be empowered to act, but the hearing of evidence will remain a vital component in any subsequent unilateral determination of appropriate and proportionate regulatory action.

Finally, organisations must be held to account for their record in implementing the principles and achieving the outcomes, by whatever means they have adopted.[16]

The benefits of this type of approach are that:

- It enables a more dynamic, responsive and focused treatment of privacy risks as they emerge (or even recede), tailoring solutions to the specific characteristics of particular industry sectors or technologies, to specific risks posed by types of data and the way they are handled, or to user behaviours
- It incentivises and rewards innovation by involving industry and other stakeholders in developing solutions to common privacy problems, such as 'privacy by design', creating tools and options for user choice and control, communicating meaningfully with users, and PETs.
- It facilitates 'internationalisation' through the activities and influence exerted by global participants, such as international companies, civil society organisations and consumer groups. Greater harmonisation may be achieved horizontally (*i.e.,* across international sectors or industries) than vertically (*i.e.,* through national cooperation). We touch upon this further under 'globalisation' below.

While the possibility for regulatory covenants already exists in Article 27, it has largely been ignored by industry and regulators, particularly at the pan-European level. This may be due to the perceived lack of freedom from the existing constraints of the Data Protection Directive. However, we believe the spirit of Article 27 should be extended and strengthened through provision of a clearer institutional framework, empowering the Article 29 Working Party to require national privacy regulators to observe agreed codes of conduct.

More generally, we need to explore alternatives to direct supervision by regulators. National regulators frequently cite lack of resources as an impediment to their providing an effective supervisory role. One solution could be a framework for independent monitoring and assurance. For instance, the Working Party could be empowered to certify independent assessors to conduct assurance monitoring and reporting, and organisations could be encouraged (or even required, in some circumstances) to retain such independent assessors to monitor and report on their compliance with the principles set out in any second-generation framework. Such approaches have been used successfully in other sectors. There is also an extensive practice of voluntary corporate responsibility reporting through independent assurance standards, such as AA1000 APS (Principles Standard), launched in 2008[17], which provide a recognized basis for organisations to report on their compliance with principles[18].

In a similar vein, 'privacy seals' and trust programmes can provide independent assessment on a more limited basis, such as for specific products or technologies, as illustrated by the work of organisations like EuroPrise[19].

The challenges faced by policy makers in the privacy sphere are not necessarily unique. Policy makers can learn from other sectors, such as corporate governance or environmental regulation[20].

---

[16] One of the most popular examples of increased accountability is the introduction of security breach notification regulations. We support breach notification requirements for all organisations entrusted with the handling of personal information regardless of business sector, where proportionately defined and implemented, including appropriate assessments of risk involved in exposure of data, likelihood of misuse, presence of encryption and other mitigating controls, and recognition of multiple possible modes of communication to subjects when harm is likely to occur.

[17] http://www.accountability21.net/.

[18] For Vodafone's Corporate Responsibility programme see here - http://www.vodafone.com/start/responsibility.html. See also Vodafone's site on independent assurance reporting - http://www.vodafone.com/start/responsibility/our_approach/assurance/aa1000_assurance_standard.html.

[19] https://www.european-privacy-seal.eu/press-room/press-releases/20080714-europrise-press-release-en.html.

2. A Multi-Tiered approach

Protecting privacy in the 21st century information society will require a framework that recognises that many different participants have an impact on how privacy is managed and protected, beyond data controllers

Limitations of the current approach

Europe's data protection framework did not anticipate many of the profound changes that have taken place since its adoption. In particular, this first-generation framework is limited in two vital respects:

i. It treats private or public enterprise as the principal target of regulation. The end user / consumer is largely out of the frame by virtue of the 'household exemption'[21]. But if the logic of the Article 29 Working Party is followed, then almost everyone is a controller of other people's information[22]. How is it possible to regulate where almost every individual has in their pocket the power to discover, capture, manipulate or publish information about other people, stored on a server anywhere around the world? In the participatory web, every citizen is as much a contributor to a privacy problem as the victim of it. Resolving this is a social policy issue as a legal one. We need to do more than clarify the 'household exemption'– we need a fundamental re-think.

ii. It is 'data centric'. The first-generation framework is built almost entirely on the foundation of 'control' over data, and hence the principal target of regulation is the 'controller' (leaving aside the specific role and appointment of processors). There are no mechanisms for applying any responsibility towards other actors that may not be controllers (or processors) but nevertheless play a critical role in influencing how privacy is handled, such as software providers, social media providers and other intermediaries. As the ease increases for individuals or organisations (many of which will be small enterprises or just loose associations of like-minded individuals pursuing a common economic, cultural or political aim) to provide interactive online services or create and distribute applications, how is it possible to require this rapidly growing and globally diverse community to create services or write applications that respect EU privacy law or values?

Take the following real-world illustration:

- An EU-based mobile user may purchase a phone from a mobile network operator established in the EU. The phone is manufactured by a Taiwanese company and the Taiwanese company determines the operating system and most of the application software running on the device.
- Independent of the operator or the manufacturer, the consumer may download a mobile application from a third party's 'application store'. The application store operator is established in the USA and provides open access to applications supplied by independent application developers.
- Application developers may be established in any country around the world, and often may be no more than an amateur software developer. The application developer will sometimes work collaboratively with communities of other developers around the world, sharing code that may be incorporated into his application.
- That code may access the mobile consumer's GPS location information to deliver location-sensitive features in its software. Other information about the mobile user may also be accessed from the device, such as mobile number, contact information, etc.
- This information may automatically be shared with the application developer and other third parties, to improve the application or for secondary uses like serving advertising to the user.

Under the existing framework, who is responsible for handling the user's personal information, including sensitive data like location?

- The network operator has no control over the data, but in this context merely provides the connectivity – the location data is based on GPS positioning data and therefore would fall outside the ePrivacy Directive and is also not under the operator's control.
- The device manufacturer has some influence over the way the device interfaces with applications, including the exposure of GPS data, but it does not in any way 'control' or even have access to any data.
- The application store provider has some influence over the conditions it places on application developers, but it does not wish to

[20] Some have argued that there are similarities between the challenges faced by sustaining the environment and the challenges for the information society, and that policy makers could learn from experiences in the more mature field of environmental regulation (Dennis D. Hirsch , Capital University Law School, 'Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law', *Georgia Law Review, Vol. 41, No. 1, 2006*).

[21] Article 3(2) Data Protection Directive.

[22] Article 29 Working Party opinion on social networking, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf.

overly regulate its growing developer community and in any event is not subject to EU law as it has no connection with Europe and is not handling any data.

- The application developer maybe completely unaware of any such thing as privacy regulation, and even if it could be said that he is subject to the jurisdiction of any EU country, he is an unlikely target for enforcement action. If the developer has used code from other sources, he may even not be aware of its impact; the code may give control to some unknown third party.

What is patently clear from this example is that the first-generation model of privacy regulation is not designed to address this problem.

The existing data protection model can be described as 'single tiered', in that it does not differentiate responsibility according to the role different actors play in impacting privacy. It is therefore architecturally unsuited to tackle the problems we now face, as the Working Party has found in trying to apply the principles to social networking.

An alternative - a multi-tiered approach

An alternative approach is a multi-tiered approach. Such a framework would recognise that different actors in the information society should bear levels of responsibility for safeguarding privacy depending upon their roles. So for instance, end users[23] handling personal information should be bound to behave in accordance with the core principles that already form the foundation of privacy and data protection law. However, it is unrealistic to expect this to result in better privacy in practice if end users (particularly consumers and small enterprises) are not provided with the information, tools and means to do this. Without exception, end users will depend upon software providers, social media providers and other intermediaries in the information economy to assist them. These other actors may not process personal information at all, or at least in the sense of making them a controller (or even a processor), yet may be in a position to provide the necessary information, tools and means to the end user.

In a multi-tiered model, these 'non-data' handlers become active stakeholders within the regulatory framework alongside data 'controllers', in building the tools and capabilities to ensure better protection of privacy. But the regulatory approach must avoid commanding and dictating solutions, and instead work to create the conditions for industry to use its energy for innovation to find solutions to privacy challenges as it does to so many other issues.

Tiers as regulatory agents

Importantly, in a multi-tiered model, different 'tiers' in the information economy can act as regulatory agents themselves, particularly companies and other organisations that provide the core technology, connectivity or platforms needed by other service providers to provide services to end users or other intermediaries. These 'first tier' actors can apply or require privacy principles to be observed among their user and developer communities or require adherence to industry codes and practices through relationships with partners. Regulators should also play a critical role in assisting with the establishment of these mechanisms to achieve the desired outcomes without unnecessarily constraining enterprises in what are fast-moving and highly competitive fields. Alternative forms of enforcement and sanctions can be conceived, such as utilising reputation schemes and peer approval that is already a common feature of web-based trust mechanisms, in addition to traditional regulatory or private enforcement mechanisms (like contractual terms). Compliance with privacy norms can be internalised by users or developers themselves in these circumstances.

The illustration we outlined above is deliberately simplistic. In reality, there will be multiple, interconnected layers of private and public enterprises that enable the processing of personal information or create other privacy impacts. Nevertheless, if our objective is to establish a culture of privacy across all sectors of society, we need to set proper expectations about the rights and obligations of different parties, which can only be achieved with a differentiated 'multi-tiered' approach according to the role a relevant actor plays.

This multi-tiered approach is essentially one aspect of the accountability model. Importantly, we believe this approach may also contribute to addressing some of the fundamental problems of globalisation – see more below.

[23] Note that 'end users' in this context will include enterprises, large and small.

3. Underlying Concepts

Core concepts and the way they are reflected in the framework need reform

Personal data

Although it took until 2007 before the Working Party produced a fully reasoned opinion on the meaning of personal data[24], the concept of 'personal data' is a critical component of the regulatory framework. However, the criticality of the definition has impeded our understanding of privacy and how best to protect and enhance it, leading to interminable debates about whether this or that piece of information is personal, rather than what safeguards are proportional to ensure protection of privacy[25]. Difficulty arises not so much with the definition itself and the concepts behind it, but the fact that the whole framework of data protection law hinges upon its meaning. If any particular data set is found to be outside the definition, then no ensuing obligations follow; a contrary finding and the whole regime kicks in. This all-or-nothing approach has undermined the ability for regulators and industry to best direct efforts where the risk of harm is greatest. One consequence is a disincentive to innovate around anonymising / pseudonymising data – if the same regime applies even where data is pseudonymised, why bother?[26]

What is needed is less focus on definitions of personal data or even on the meaning of identity *per se,* and more on the contexts (including technical and commercial) in which a given identifier is used and how it may impact the privacy of the individual concerned. This should not necessarily result in data relating to a given identifier falling outside the regulatory framework entirely, but rather a lighter and more proportionate set of safeguards. Impact assessments should be based upon evidence as technologies and practices evolve (for example, a contextualised and risk-based approach could have usefully created a proportionate and workable framework for the handling of IP addresses by online service providers). In addition to the categories of sensitive data that may attract a higher level of protection, there should be wider recognition that some data may not in some contexts be particularly sensitive even if a user is identified, and should correspondingly attract a lower level of protection. The use of impact assessments rather than strict definitions of personal data will strengthen the regime and should form a core part of any second-generation privacy framework.

Legitimacy and Consent

In a number of jurisdictions, the foundation of legitimacy remains focused on consent. However, it is often disproportionate for consent to be the primary justification for processing of personal data in an information economy where data must be processed for almost every ordinary transaction. Greater focus must be given to proportionality, with the flexibility to allow the handling of personal information with safeguards other than consent where this is justified. This is already featured in Article 7(f), although not uniformly implemented by Member States. Organisations should be able to make these 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.

The legitimacy foundation in privacy law must reflect the reality of the information economy, *i.e.,* many of the most popular services people use today would not exist if it were not for the fact that these services are funded by advertising and a certain amount of data about users. We need to explore how to attain a fairer value exchange for the individual, but not at the expense of encumbering the very products and services that give us so much value in other ways. The strict notion of 'opt in' consent for many purposes no longer necessarily reflects what users expect – provided there are adequate safeguards.

Indeed, excessive user interaction through continual consent prompts can erode valuable safeguards for users. 'Privacy fatigue' causes users to click through consent boxes without thinking. This should never be an excuse for

[24] Article 29 Working Party opinion on personal data, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.
[25] The debates around IP addresses online typify this, leading to a particularly legalistic approach to the question of personal data.
[26] And in fact, applying the requirements of data protection may *require* that data be identifiable (for example, authenticating for rights of access, correction or deletion).

poor user control and notification. But there needs to be a more sparing use of consent and a more user-focused understanding of the interface between users and information collection and handling systems. Greater participation in this process can lead to more innovation around legitimacy.

Roles and responsibilities - controller and processor

As we described above, the focus of regulatory attention on the controller alone is too rigid and limited. But more particularly, the relationship between controllers and processors also needs addressing. While certain relationships do still fall into these categories, increasingly controllers are making use of off-the-shelf 'cloud based' solutions and software- or infrastructure-as-a-service, where the controller has limited ability to realistically determine the way the 'processor' handles data, in particular as regards the level and form of security. At the same time, the vendor cannot be said to be acting in the capacity of a controller. For EU-based parties, it should be possible to identify alternative categories of processor, with attendant obligations relating to issues such as security. We support the replacement of legal formalities, such as the need for written (and in some cases, preapproved) contractual arrangements between controllers and processors, with obligations on both parties under the legal framework itself. For international arrangements, see below on globalisation.

In addition, it is imperative that Member States be precluded from adopting varying security requirements, as is the case in eight EU member states, plus one EEA state[27]. This approach makes pan-European operations unnecessarily complex and is counter to best security practice by 'hard coding' requirements into law. State-of-the-art should mean state-of-the-art.

Technological neutrality and ePrivacy

Technological neutrality has long been a cornerstone of European policy making. As technology evolves, often in ways that disrupt established business and regulatory models, the privacy framework must be ever-adaptive to these changes. A range of current technologies already challenge existing regulatory approaches[28].

We have nevertheless had for a number of years a parallel privacy regime for electronic communications networks and services that increasingly highlights the blurred distinction between information society services and electronic communications services. The ePrivacy Directive[29] imposes additional obligations only on electronic communications service providers for certain kinds of information thought to be particularly sensitive. But information about consumers' activities online (which would in the hands of a mobile operator be protected as traffic data) and about their geographical location (otherwise, location data) can, in today's digital world, be obtained from many other sources. As a concrete example, location data obtained from a cellular network is protected under the ePrivacy Directive, while location data obtained from GPS, WiFi location or open Cell ID, freely available to companies who provide other internet applications, is protected only by the Data Protection Directive (and only then to the extent that the Data Protection Directive has any impact on entities outside the EU that collect and use this data – as illustrated in the example above). This regime places discrepant burdens on the use of functionally equivalent data based solely on the industry sector the data controller finds itself in. This has a distorting effect on the market by applying higher standards on local electronic communications providers than it does on other kinds of service providers who may be based outside of the EU entirely and not regulated by the ePrivacy directive or the Data Protection Directive[30]. Not only is this ineffective at improving privacy, we believe it has created a competitive advantage for 'unregulated' technologies and service providers.

Vodafone believes the response to this rapidly evolving technological environment is not to 'hard code' solutions into the legal framework, but rather to provide regulators with the means to work with industry to resolve these sector or technology-specific challenges, within an over-arching 'principles and outcomes' based framework.

[27] In the EU, Austria, Germany, Greece, Ireland, Italy, Latvia, Poland and Spain; in the EEA, Norway.
[28] For example, NFC, ambient intelligence and other semi-autonomous technology agents.
[29] http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.
[30] The vast majority of location-aware applications on the market utilise GPS, WiFi location or open Cell ID, which are essentially unregulated by the ePrivacy Directive.

4. Globalisation

The solution to protecting privacy in a global information society is global standards. However, there are important and effective steps we can take in the absence of international political alignment to improve privacy protection globally.

No feature of the existing framework has received more attention than the challenges presented by globalisation, found in today's borderless digital environment, where users can access services from anywhere and where their data flows freely across the globe according to the data storage and processing decisions of the organisations that handle their data. But while individuals have become increasingly willing to communicate, interact, purchase and do many other things online regardless of borders, and as enterprises work globally within their own organisations or in partnership with others, the political and regulatory institutions that govern privacy remain bounded by geography.

International transfers

Global data flows are an essential economic reality. Outsourcing and off-shoring have led to enormous cost advantages for enterprises and have created entire industries that depend upon the flow of data. Software-as-a-service, infrastructure-as-a-service, cloud computing, and other developments in remote service provision are a major area of innovation and account for significant increases in productivity, economies of scale, and access for small businesses to computing resources that were previously only accessible to large multi-nationals. These developments depend upon the movement of data without regard to geographic boundaries.

The principle of our first-generation privacy framework is 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. We support this concept and believe it's an essential requirement for a robust and sustainable privacy regime. The challenge is finding a model that achieves this in practice, without imposing disproportionate burdens on organisations, economic development or innovation.

The extent to which the existing regulatory structure for international transfers has provided any real increase in privacy protection has to be questioned. It has 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. The approaches embedded in the existing framework reflect a very different world to the one we are in now. Without adding to the lengthy debates surrounding the mechanisms for approving international transfers, they are no longer fit for purpose. 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, one which is more clearly built upon the concept of corporate accountability. However, it remains limited to the corporate group and therefore of limited use. It will remain of limited use even if BCRs in their current formulation could be extended beyond the corporate group, if the national regulator has a monopoly on the ability to approve or provide external assurance on BCRs; the model is simply not scalable for the dynamic and mass-market information processing environment we are already witnessing. The limited resources and technical know-how of national privacy regulators will act as a continual brake on progress.

Regulators can and should play a vital role in defining the principles for BCRs. However, building on the proposals outlined above for a second-generation framework, one response to the challenge of adequate external oversight is to allow companies the flexibility to create BCRs for their specific market requirements, but require independent assurance of BCRs against the principles. Such a requirement would encourage the creation of a secondary market in 'BCR assurance', *i.e.*, 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.

Applicable law

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.

Nevertheless, the second-generation framework described in this paper provides some important levers that may assist in deflecting some of the impacts of globalisation:

- Co-regulatory mechanisms 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.
- European organisations that provide the core technology, connectivity or platforms needed by other service providers (including those who may be established outside the EU) to reach European users could act as regulatory agents themselves, setting standards and codes of conduct for their user and developer communities, in accordance with the principles of the framework and reflecting EU privacy values.

Global standards

We need to create the foundation of a borderless privacy environment to safeguard consumer confidence and avoid competitive distortions. Privacy as a concern and as a social issue is increasingly changing, and arguably becoming more 'globalised', or at least attitudes may be diverging less along national lines and more along linguistic or demographic lines.

Vodafone supports the Madrid Resolution and the initiative led by the Spanish AEDP to create a process for seeking international standardisation of privacy regulation. Even in the absence of any wider international cooperation or standardisation, EU policy makers must engage with the US on privacy reform. Transatlantic cooperation is the single most important priority, and has the potential not only to create early benefits for users, but to establish a single reference model for further collaboration with the wider international community.

30 December 2009