PRIVACY IN THE NETWORKED SOCIETY

Data Protection principles for the digital remaking of society
## INDEX

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>A Balancing Act</td>
<td>8</td>
</tr>
<tr>
<td>Data Protection Principles</td>
<td>10</td>
</tr>
<tr>
<td>&gt; Targeted and transparent</td>
<td>12</td>
</tr>
<tr>
<td>&gt; Technology-neutral</td>
<td>12</td>
</tr>
<tr>
<td>&gt; Role-specific</td>
<td>12</td>
</tr>
<tr>
<td>&gt; Flexible</td>
<td>13</td>
</tr>
<tr>
<td>&gt; Efficient</td>
<td>14</td>
</tr>
<tr>
<td>&gt; Cross-border tolerant</td>
<td>16</td>
</tr>
<tr>
<td>Conclusion</td>
<td>18</td>
</tr>
<tr>
<td>References</td>
<td>19</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

The world cannot realistically expect a global policy consensus on the right to privacy to emerge within the foreseeable future. The importance and performance of Information & Communication Technology (ICT) will however continue to increase rapidly, fueled by continuing advances.

This shift will have numerous effects, including the increasing digitization of industries, economies, social activities and societies at large. Demands for data protection must be reconciled with the realities of a world in which data is stored and handled in a global, borderless system. End-user trust and data protection are inherently intertwined in the digital remaking of our economies and societies, and cannot be separated.

Under these circumstances, reforming a rights-based regulatory framework such as data-protection regulation involves maximizing societal benefits while safeguarding appropriate levels of data protection. This requires a delicate balance: between the utilitarian promotion of market efficiency, the public-interest aspects of increased social equity/solidarity and the protection of individuals’ rights.

As the name implies, any rights-based regulatory framework must be anchored in the recognition of certain human rights – in this case, the right to privacy and in particular data protection, both of which rely on the commitment of the state to these rights. Additional complications arise in a globally-networked, digitally-interconnected environment. Geographically-contingent demand for data privacy requires a progressive, rights-based regulatory response. Such a response should be:

- targeted
- transparent
- technology-neutral
- role-specific
- flexible
- efficient
- cross-border tolerant.

In addition to these principles, a progressive approach should adopt a holistic view and reconcile the tensions between market-based, public interest-based and rights-based regulatory approaches. It must also recognize that promotion of market efficiency delivers outcomes that contribute to the fulfillment of several different categories of human rights. It has no zero sum preconception that technological progress automatically comes at the expense of privacy or with an increased need for data protection. It also refrains from adopting a laissez-faire stance on safeguarding privacy. A progressive approach is a delicate balancing act.
Baby heart rate: 140 bpm
The concept of a right to privacy is a relatively modern phenomenon that gained importance in Europe in the years following the Second World War, the Cold War and the US human rights movement of the 1960s and 1970s. The genesis of a modern form of privacy – “the right to be let alone” – can be traced to Samuel Warren and Louis Brandeis who in 1890 formulated their now-famous article “The Right to Privacy” arguing for legal recognition of the right. That article is seen by many as the foundation of privacy law in the United States.

Today, there appears to be a worldwide consensus regarding the importance of an individual’s right to privacy and the need to safeguard it. The most obvious evidence is the explicit or implicit recognition of privacy as a fundamental right in the constitutional law of many countries. In addition, the UN Universal Convention of Human Rights, the EU Convention on Human Rights, the OECD Privacy Guidelines and the APEC Privacy Framework have inspired the passage of thousands of privacy laws in many countries.

For the foreseeable future, however, we cannot realistically expect that there will be a global policy consensus on the concept of the right to privacy, nor on the balance to be struck in the regulation of privacy, such as in data protection regulation. Even within an individual jurisdiction, the concept of privacy is often open to interpretation.

The rapid development of ICT over the past three decades, including the rise of a borderless internet, has challenged territorially based law-making, but perhaps not to the degree cyber-libertarians had anticipated. This has put pressure on the globally fragmented concept of privacy. Far-reaching technological advancements have also enabled the creation of new business models that increase the commercial value of private information.

“The rapid development of ICT over the past three decades, including the rise of a borderless internet, has challenged territorially based law-making, but perhaps not to the degree cyber-libertarians had anticipated. This has put pressure on the globally fragmented concept of privacy. Far-reaching technological advancements have also enabled the creation of new business models that increase the commercial value of private information.”

“Personal data is the new oil of the internet and the new currency of the digital world.”

The increasing pressures have been evident in several recent cases where the rapid rise of ICT and the increased commercial value of personal data have come into conflict with a growing risk of privacy invasions and the loss of privacy. These have led to new policy initiatives, but in such circumstances good intentions can also result in misguided regulatory interventions, such as:

- a mismatch between the justification for a policy intervention (why regulate) and its policy objectives (the ends)
- failing to target regulatory objectives with the appropriate regulatory instruments
- inefficient regulatory implementation strategy.

“Privacy problems are often not well articulated. We frequently lack a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve this problem.”
These tensions have not halted the ICT-led transformation of society. On the contrary, the use of ICT has been recognized as enhancing productivity and is a key source of economic growth, empowerment and the creation of new businesses and jobs. ICT has been shown to produce important benefits and multipliers\(^7\) such as:

- **Increased multifactor productivity growth.** This includes the impact of intangible investments such as organizational changes, new distribution and production processes, and new methods of doing business related to the use of ICT.

- **GDP growth 1.** For every 10 percentage point increase in broadband penetration the isolated economic effect on GDP growth is around 1 percentage point of GDP, with estimates varying from 0.5 to 2 points.

- **GDP growth 2.** Doubling the average attained broadband speed for an economy increases GDP by 0.3 percentage points.

- **Job growth.** For every 1,000 additional broadband users, around 80 jobs are created, with estimates ranging from 20 to 130.

Over the coming years, ICT performance will continue to improve, fueled by rapid technology advances and the subsequent continued digitization of economies and society. This will in turn bring new opportunities for people and businesses to create and learn, to improve innovation and sustainability, leading to positive impacts across the planet. Ericsson believes the world is at an inflection point, poised for a significant change in competitive opportunities for nations, business, societies and individuals. This change will lead to the emergence of what Ericsson calls the **Networked Society.** It will produce economic shifts and significant societal benefits.\(^8\) It will also result in new strains on existing regulatory frameworks\(^9\) and, in the context of privacy, new pressures for the evolution of progressive data-protection regulatory frameworks.
A BALANCING ACT

The fundamental and legitimate desire to ensure appropriate levels of privacy and, by extension, data protection (see Box 1) has been and still is largely dealt with in the cultural, political and territorial contexts.

The demand for data protection – given its intangible, global and borderless nature – must be reconciled with these contexts. The accompanying issues of trust and legitimacy are also essential for the continued digital development of economies and societies. The desirability of continued digitization is not the question per se. On the contrary, its associated socio-economic benefits – such as economic growth, job creation, individual empowerment and sustainability – are both acknowledged and actively promoted by many policy makers around the world. Particularly in a rights-based regulatory context, digitization can increase the transparency of public and governmental affairs, increase individuals’ involvement in public matters and increase their ability to achieve richer lives. Such outcomes help satisfy a range of human rights and needs, where privacy is often an essential consideration. The protection of privacy is then a necessary component for satisfying a wider set of human rights, but is insufficient on its own.

The socioeconomic benefits associated with the digital revolution – as with any technological revolution that has fundamentally reshaped society – also bring new risks, and aggravate or mitigate some existing ones.

Any improvement of a rights-based regulatory framework such as data-protection regulation should concentrate on maximizing societal benefits while safeguarding appropriate levels of protection. This is a delicate balancing act between the utilitarian promotion of market efficiency, the public-interest promotion of increased social equity and solidarity, and the rights-based promotion of individual rights. While a rights-based approach may at times be at odds with market efficiency and the promotion of social equity, that very tension highlights the need to adhere to certain principles for safeguarding privacy in a networked society.
DATA PROTECTION PRINCIPLES

The starting point of a regulatory framework for data protection, as in any rights-based regulatory framework, must be fundamentally anchored in the recognition of and commitment to protection of a certain set of human rights, in this case the right to privacy and certain subsequent obligations to protect personal data.

Additional complications arise in a globally-networked, digitally-interconnected environment. Devising a progressive rights-based regulatory framework is the appropriate policy response to meet legitimate but geographically contingent needs for data protection. Such a framework should be:

- targeted
- transparent
- technology-neutral
- role-specific
- flexible
- efficient
- cross-border tolerant.

In addition to these principles, a progressive approach should adopt a holistic – cross-sector – view when balancing the market-based, public interest-based and rights-based regulatory approaches. Because the Networked Society and the digital economy combine previously separate situations into a common context (a shift referred to as convergence), a limited perspective – be it from technology, business, service or regulation – is no longer sufficient. This does not mean that a specific category of human rights such as privacy should be subordinate to, for example, the public interest but neither are they always superior.

Invasion

CONTROLLER

PROCESSOR

Territorial jurisdictions

Figure 1: Modeling data privacy – activities and stakeholders

Source: Ericsson Adaptation: Solove, Understanding Privacy, Harvard Press 2008. Controller and Processor may or may not be independent legal entities.
“...the value of privacy must be determined on the basis of its importance to society, not in terms of individual rights. Moreover, privacy does not have a universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance of the activities that it facilitates.”

A progressive approach recognizes that improved market efficiency helps satisfy several different categories of human rights. The right to privacy can sometimes be an integral part of these rights, but may be insufficient on its own to achieve them. A business-friendly regulatory framework that stimulates innovation, transformation, industry growth and commercial freedom, for example, is desirable from a broader rights-based perspective as well as from a public-interest perspective.

A progressive approach should advance national digital-policy goals that aim to increase capacity for structural change in societal, economic and individual terms in the best way possible. A progressive approach explicitly refrains from a zero-sum assumption where technological progress comes automatically at the expense of privacy or with increased need for data protection. It avoids a laissez-faire view of privacy where increased utility is all that matters. This approach is not focused on one particular individual right, but recognizes rather that advances in ICT can contribute to greater fulfillment of a variety of human rights.

**BOX 2: SOLOVE’S VIOLATION RISKS AND INFORMATION MANAGEMENT ACTIVITIES**

1. **Surveillance** – watching, listening or recording an individual’s activities  
   **Interrogation** – various forms of questioning

2. **Aggregation** – combination of various data about a person  
   **Identification** – linking information to a particular individual  
   **Insecurity** – carelessness in protecting stored information from leaks and improper access  
   **Secondary use** – the use, without the subject’s consent, of collected information for a purpose other than the use for which it was collected  
   **Exclusion** – the failure to allow the data subject to know about the data held by controller and processor

3. **Breach of confidentiality** – failure to comply with an undertaking to keep material confidential  
   **Disclosure** – the revelation of truthful information about a person that affects the way others judge that person  
   **Exposure** – revealing another person’s intimate emotions or states, such as nudity, grief or bodily functions  
   **Increased accessibility** – making information more widely or easily accessible  
   **Blackmail** – using the threat to disclose personal information to influence a person’s behavior  
   **Appropriation** – the use of the data subject’s identity to serve another’s aims and interests  
   **Distortion** – disseminating false or misleading information about data subjects

4. **Intrusion** – invasive acts that disturb a person’s tranquility or solitude  
   **Decisional interference** – incursion into the data subject’s decisions regarding his or her private affairs
Before going into the details of the proposed data-protection principles, it is important to put them into the context of key stakeholders, activities and data flows. The purpose is to identify crucial steps, from an information-management perspective, where the right to privacy might be compromised and adequate data-protection measures are therefore required.

Figure 1, using the concepts described in Box 1, is an adaptation of Solove’s model. It identifies key activities and stakeholders potentially posing risks to privacy, and specifies a taxonomy (see Box 2) of recognized privacy violations tied to each activity. Inspired by Solove’s approach to defining roles, activities, data flows and privacy violations, Ericsson has identified key privacy principles that should be included in a progressive regulatory framework for data protection.

**TARGETED AND TRANSPARENT**

A well-targeted regulatory framework should focus on the purpose of data processing, including data collection and the use of that data. Data processing and collection must respect jurisdictional legal requirements, which must include clear definitions of what is classed as personal data as well as sensitive data that may not be collected.

Personal data should be relevant, accurate and up to date in terms of its purpose. It must have been obtained with the knowledge of, and where appropriate the clearly formulated consent of, data subjects. Consent must be obtained before collection and any subsequent use, and data subjects must have the option to withdraw their consent. Data usage must be limited to the scope of the original consent or in line with the relevant legal authority or judicial order. Controllers, those legally entitled to collect data, need to provide easily understood privacy notices describing how the organization will use and disclose personal information.

A framework should also support data subjects’ right of access, rectification, ‘do-not-track’ provisions and erasure in terms of public and private data controllers, who should ensure clear contact points for the exercise of such rights. Controllers should also provide prompt responses to requests from data subjects. However, data controllers should be protected from frivolous and unreasonable requests as well as blanket regulations which could stifle new services and business opportunities. Data controllers could specify a system for making requests for records and record corrections, possibly involving a nominal upfront fee to deter frivolous claims.

**TECHNOLOGY-NEUTRAL**

A progressive framework should be technology neutral – it should treat platforms, business models and business processes in an even-handed way and not include legal requirements for specific technologies. The principle of technology neutrality assumes that the choice of technology is not used to circumvent regulatory objectives. Technology neutrality is a flow-on from the fact that a well-targeted framework focuses on the purpose of collection and use of the data. (Concerns specific to technologies and future developments are discussed in the efficiency section below.) A technology neutral approach should involve:

- the legal and regulatory framework design
- the choice of regulatory instruments
- the implementation strategy of regulatory instruments.

**ROLE-SPECIFIC – THE KEY CONCEPT OF DATA CONTROLLERS AND DATA**

The responsibilities of data controllers and data processors should be clearly divided and defined in statutory provisions. The legal concept of data controller and data processor under EU Directive 95/46/EC should be maintained within the EU and...
considered by policy makers elsewhere. This legal distinction promotes innovation and evolution of an open, responsible, dynamic and competitive information management value chain. In Figure 1, the dotted line surrounding the data controller and data processor roles highlights the fact these two roles may or may not be performed by the same entity. When these two activities are performed by independent entities, the framework must assure that legal responsibility cannot be contractually outsourced from data controller to data processor. A proper framework avoids the risk of a race to the bottom with respect to privacy protection. However, in certain cases there might be further need for clarification to manage the often-complex relationship between data controllers and data processors. In principle, the deciding factor in deciding the roles and responsibilities should be the purpose for which personal data are collected and processed.

**FLEXIBLE**

Any regulatory framework involves an inherent tension between the need for flexibility to allow for evolution and the demand for predictability and consistency for regulated parties. However, there are areas where a progressive framework can help relieve this tension and provide room for flexibility.

**Sensitive data**

A flexible approach is necessary in dealing with key regulatory issues such as sensitive data, which may have strong national, historical and cultural connotations and be defined differently in different countries. For example, the EU forbids registration of race and religion. South Africa and Malaysia on the other hand require employers to register race and religion in order to safeguard the rights of all races and religions. In such cases, South African and Malaysian companies, for example, should not be prevented from using a service provider in the EU. Authorities should be able to approve solutions that reconcile national requirements without compromising territorial interests.

**Alternatives to top-down hard-law approaches**

A progressive framework should promote alternatives to a top-down implementation strategy by actively encouraging self- and co-regulation frameworks, industry codes of conduct and company certification procedures. The main aim is a framework that can evolve with technology, promote accountability and accommodate global differences in the definition of privacy and in national legal standards, while still protecting the rights of individuals.

**Accountability**

Accountability requirements and ex-post controls should not add new obligations on top of already prescriptive rules, but should instead offer a more flexible, and efficient alternative.

Legislation that promotes accountability starts with a well-targeted framework focusing on the purpose of data collection and use. True accountability provides clear guidance to what should be achieved, instead of focusing narrowly on prescriptive and administrative processes that might not accomplish the ultimate objective of increased data protection.

Accountability is a concept that should underpin the entire framework of data protection, enforcement and supervision. A progressive framework should encourage organizations to be accountable and to have an explicit corporate objective of protecting individual rights, while also ensuring legal compliance. This will make data protection a proactive part of business operations instead of a reactive compliance function.
Co-regulation and self-regulation
In addition to the principles presented elsewhere in this document, accountable companies adhering to Privacy by Design (PbD) principles should develop, implement and enforce internal tools such as:

- A company- and industry-wide information security policy specifying requirements, processes, roles and responsibilities. This policy should ensure appropriate technical and organizational measures to prevent unauthorized or unlawful processing of personal data and the accidental release, loss, destruction of, or damage to, personal data managed by the individual companies.

- A company- and industry-wide privacy policy and instructions protecting the privacy of personal data from end-users, customers, employees and temporary staff. A supplementary implementation plan should specify the policy owner, driver, purpose, target, action requirements and follow-up reporting, including measurements and corrective actions.

Such self-regulatory tools aim to create a robust and effective corporate and industry infrastructure comprising values, competence, incentives, processes and technology.

The use of PbD to instill protection of data privacy into a company’s or industry’s DNA is dependent on company-specific tools as described above. In addition, a company-wide privacy instruction covering products and services must establish how PbD is integrated into the company’s ordinary product and service life cycle including instructions such as privacy safeguards, roles, and responsibilities. A progressive framework must aim to encourage further development of a self-regulatory company/industry-wide regime with substance rather than developing a rigid, top-down regulatory framework.

EFFICIENT
Reduction of red tape
A progressive framework should also be self-simplifying, by including mandatory provisions reducing administrative burdens, as well as sunset provisions. It should contain obligations for periodic policy reviews to keep the framework up to date; this helps avoid a regulatory disconnect that damages efficiency and may ultimately lead to regulatory failure. This approach should allow for periodic reviews to minimize the cost to the public, consumers and businesses and to increase industry certainty by avoiding unexpected major framework revisions.

- EU Directive 95/46/EC should be changed to ease the administrative burden for companies with extensive global business activities. The requirement to enter data-processing and data-export agreements, and make the related DPA filings, should be abolished.

- Articles 13 (Encouragement and support of self-regulation) and 14 (International cooperation regarding cross-border transaction of personal data) of the South Korean Personal Information Protection Act (PIPA) is another example that should be further encouraged and followed up with further policy initiatives with the aim of promoting the expansion of such self-regulatory tools.

Security breach notification
Compulsory reporting of data breaches should encourage data controllers to manage personal data securely and foster confidence in third-party data processing. Reporting requirements should ensure the same rules across different service providers and be coupled with a fast, efficient protection framework. Stringent notification requirements such as a 24-hour notification requirement for personal data breaches are costly, impractical and counterproductive, and should be avoided.
Not all breaches threaten user privacy so the notification requirement must focus on breaches that are likely to have serious negative consequences for individuals. Controllers should be required to notify supervisory authorities and data subjects only when a breach is likely to lead to significant risk of substantial harm to the data subject, when the data subject can be identified, and only if no technical measures have been applied to render the data unintelligible.

Breach notification provisions should take into account the fact that processors do not have a direct relationship with the end user. A clear distinction between controller and processor is therefore crucial. Processors are typically at least one step removed from individuals using the service and therefore should only notify the controller, who may then be required to notify authorities and data subjects. Only the provider with the direct relationship – the controller – should notify the end user of a breach of data privacy.

Any proposal for a horizontal breach notification system should be carefully crafted to prevent the issuance of irrelevant notices, by adopting appropriate trigger criteria. The right balance must be found between notification as a means to improve security measures and actions implemented to minimize harm, disruption and reputational consequences for organizations.
Enforcement
In general, enforcement mechanisms aim to ensure compliance with regulatory frameworks and are therefore an important element of a mature and efficient framework. In a progressive regulatory framework, enforcement measures look at the accountability principles and not just legal compliance. They also rely on alternative top-down implementation strategies, which aim to adapt the framework when conditions change, in order to keep it up to date. Under these conditions an enforcement mechanism should aim to encourage and reward responsible and accountable companies rather than simply threatening offenders with severe penalties.

In particular, undifferentiated use of “compliance by deterrence” brings a risk of severe penalties for incidental and unintended breaches. It is preferable for infrequent and incidental breaches by responsible companies to be detected, swiftly corrected and turned into learning opportunities for the entire industry.

To encourage incident detection, it is better to limit the use of punitive sanctions and instead increase incentives to self-detect and self-correct. An industry-wide code for whistle-blowing can also assist such detections by enabling investigations of breaches and their cause. Lessons from such individual cases could be made anonymous and disseminated publically throughout the industry, a powerful complement to the use of best practice benchmarks.

A progressive framework adopts a more constructive, participatory and probably a more cost-effective approach to prevention than a costly deterrence-based approach.

CROSS-BORDER TOLERANT
Affordable end-user services depend on economies of scale based on free data flows and open trade in ICT equipment and services. This is particularly true for the global collection, storage, distribution and use of information that companies use to improve efficiency. Data-transfer rules, designed to protect citizens, often result in significant administrative burdens and disrupt implementation of legitimate policy objectives.

A progressive framework requires international harmonization efforts that open up, expand and simplify cross-border data flows. Such efforts should also aim to deliver harmonized outcomes in terms of the:

- legal framework
- regulatory instruments including clear legal definitions of key regulatory objects (such as personal data)
- strategy for the implementation of regulations
- enforcement measures, including sanctions.

Steps to simplify international data transfers are important in reducing the administrative burdens on businesses and strengthening international trade. Streamlined data-protection rules and simpler data transfers are also essential elements of a modern open trade environment. World Trade Organization activities in this area are highly relevant.

A progressive framework promotes open, liberal and simplified regulation (less red tape) of cross-border data flows:

- within groups of companies and between independent legal entities, across regulatory harmonized and non-harmonized territories
- by expanding the number of countries and regions adhering to harmonized, open and simplified regulation of cross-border data flows.

Where harmonization cannot realistically be achieved or is expected to take a long time, a progressive framework promotes concepts such as US safe-harbor
company certification, the EU concept of Binding Corporate Rules (BCR) or other initiatives that allow responsible companies to bridge the gap between different standards in national privacy laws.

In parallel with strong consumer protection rules, data protection rules must consider the interests of responsible businesses by safeguarding the international flow of data, rather than cutting them off or restricting them. It is important to simplify the process for adopting BCR, rules that facilitate the global transfer of data among companies, when adequate safeguards are in place for the fair processing of data.

Considering the importance of international data exchange in the global economy, third countries’ standards of personal data protection should be assessed promptly. If such assessments are not made and the gap between national privacy standards cannot be bridged, companies have to adopt strict contracts that require significant resources; this hinders innovation and investment of these resources in other important data-protection issues.
This is fundamental for the continuation of a prosperous and socially-desirable transformation – the digital remaking – of society. Over the coming years, ICT performance will improve further, fueled by continued rapid advances in technology and resulting in benefits such as the continued digitization of economies and societies. We are on the brink of the Networked Society, which holds the promise of a host of societal benefits. Yet the rise of the Networked Society also comes with responsibilities.

A progressive regulatory framework for data protection must be fundamentally anchored in the recognition of a certain set of individual rights and a commitment to protect these rights – both through an adequate policy framework and the proactive actions of responsible and accountable organizations. Additional complications arise in a globally-networked and digitally-interconnected environment. For the foreseeable future we cannot realistically expect that there will be a global policy consensus on a right to privacy nor on the balance that must be struck in the regulation of data protection. Policies that harmonize national and regional data privacy and data protection frameworks are one way to address the current situation.

A progressive, rights-based regulatory framework is the appropriate approach to data protection. The main challenge for such an approach is the requirement to balance different regulatory objectives. Policymakers should consider principles of targeting, transparency, technology neutrality, role specificity, flexibility, efficiency and cross-border tolerance.

A progressive framework should promote alternatives to a top-down implementation strategy. Such alternatives include active encouragement of self- and co-regulation frameworks, industry codes of conduct and company certification procedures. In this way, a progressive framework becomes flexible and adaptable to geographical differences, open to cross-border data flows, business- and innovation-friendly and – importantly – aligned with national data-protection policy standards.

The protection of privacy – and therefore data – is essential in safeguarding the personal right to privacy. But it is also essential to cater for public and market needs, and to gain, strengthen and maintain the trust of consumers, firms, markets and society at large.

CONCLUSION

The protection of privacy – and therefore data – is essential in safeguarding the personal right to privacy. But it is also essential to cater for public and market needs, and to gain, strengthen and maintain the trust of consumers, firms, markets and society at large.
1. Explicit constitutional recognition exists in countries such as Brazil, South Africa and South Korea. Implicit constitutional recognition is granted in Canada, France, Germany, Japan, India and the US.


3. Differing regional attitudes to protecting privacy can be seen between the US, where the key focus is on facilitation of privacy, and the EU, where the focus is on protection of privacy.


8. To find out more about Ericsson’s Networked Society vision, visit: http://www.ericsson.com/networkedsociety.


12. Such as the EU Directive (95/46/EC) and EU member states’ implementation thereof, Australia’s Privacy Act, Canada’s Personal Information Protection and Electronic Act, Japan’s Personal Information Protection Law, APEC Privacy Framework and OECD Privacy Guidelines.


17. According to Solove, Understanding Privacy, Chapter 1, Harvard Press, 2008: “…many existing theories of privacy view it as a unitary concept with a uniform value that is unvarying across different situations…. In other words, most theorists attempt to define privacy by isolating a common denominator in all instances of privacy. I argue that the attempt to locate the ‘essential’ or ‘core’ characteristics of privacy has led to failure… approach to conceptualizing privacy must have a focus… It needs to unravel the complexities of privacy in a consistent manner; otherwise it merely picks at privacy from many angles, becoming a diffuse and discordant mess… I propose a taxonomy of privacy – a framework for understanding privacy in a pluralistic and contextual manner. The taxonomy is grounded in the different kinds of activities that impinge upon privacy. I endeavor to shift the focus away from the vague term ‘privacy’ and toward the specific activities that pose privacy problems. Additionally, the taxonomy is an attempt to identify and understand the different kinds of socially recognized privacy violations, one that I hope will enable courts and policymakers to better balance privacy against countervailing interests. Ultimately, the purpose of this taxonomy is to aid the development of the body of law that addresses privacy.”

18. Some regulation regarding erasure is in place already in several jurisdictions. However clarifications may be needed about what that means in respect of social media. The right to be forgotten is but one example of such a new challenge.


Ericsson is the world’s leading provider of communications technology and services. We are enabling the Networked Society with efficient real-time solutions that allow us all to study, work and live our lives more freely, in sustainable societies around the world.

Our offering comprises services, software and infrastructure within Information and Communications Technology for telecom operators and other industries. Today more than 40 percent of the world’s mobile traffic goes through Ericsson networks and we support customers’ networks servicing more than 2.5 billion subscribers.

We operate in 180 countries and employ more than 100,000 people. Founded in 1876, Ericsson is headquartered in Stockholm, Sweden. In 2011 the company had revenues of SEK 226.9 billion (USD 35.0 billion). Ericsson is listed on NASDAQ OMX, Stockholm and NASDAQ, New York stock exchanges.