an introduction to

DATA PROTECTION

EUROPEAN DIGITAL RIGHTS

This booklet is intended to provide an overview of some of the key issues and jargon surrounding data protection in the digital environment.

At its core, data protection is about preserving a fundamental right that is reflected in the Charter of Fundamental Rights of the European Union, Council of Europe Convention 108, as well as other international agreements and national constitutions.

The processing and re-use of citizens' data has become increasingly important from an economic perspective. It has lead to pressure to weaken this fundamental right and also to change the legislative framework to make legal protections less predictable.

We hope that this document will be a positive contribution to the debate, and that the outcome of the review process will ensure predictable and proportionate protection of privacy in the digital age – reinforcing the European Union's global leadership on this topic.

CONTENTS:

Booklet written by:

EDRi's members and observers

Edited by:

EDRi and Digital Courage (Germany)

Design by: CtrlSPATIE

Photography: Marnix Petersen

European Digital Rights (EDRi) is an association of 30 privacy and digital civil rights associations from 20 Countries.

European Digital Rights
20 Rue Belliard
1040 Brussels
tel: + 32 (0)2 274 25 70
brussels@edri.org

PERSONAL DATA

WHAT IS IT? WHY SHOULD WE CARE?

Written by:

Digitale Gesellschaft, Germany
http://digitalegesellschaft.de

The issues of privacy and personal data protection have frequently been in the news in recent years, especially in the context of social networking, consumer profiling by online advertising companies and cloud computing (which are all explained in detail in this booklet). But before we go any further, it is important to understand what kinds of data are personal data.

Roughly speaking, personal data means any kind of information (a single piece of information or a set of information) that can personally identify an individual or single them out as an individual. The obvious examples are somebody's name, address, national identification number, date of birth or a photograph. A few perhaps less obvious examples include vehicle registration plate numbers, credit card numbers, fingerprints, IP address (e.g. if used by a person rather than a device, like a web server), or health records.

It also has to be noted that personal data is not just information that can be used to identify individuals directly, e.g. by name – it is enough if a person is "singled out" from among other people using a combination of pieces of information or other "identifiers". For instance, online advertising companies use tracking techniques and assign a person a unique identifier in order to monitor that person's online behaviour, build their "profile" and show offers that could be relevant for this person. Such an advertising company does not need to know that the person in question is a John Smith – it is enough to know that user 12345678 repeatedly visits certain websites, "likes" certain websites, etc. In this case such a unique identifier is considered personal data, along with all the information concerning this user collected (browsing history, "likes"...) by the advertising company.

"There is little doubt that the growing amount of data will change the world in the coming years in ways that we can scarcely imagine today."

With the amount of data growing exponentially, there is little doubt that it will change the world in the coming years in ways that we can scarcely imagine today (the trend known as Big Data, described in this booklet). Processing reliable data can help discover certain trends, which can

"In the long run, citizens and democratic societies as well as businesses can only profit from strong safeguards."

contribute to reducing the waste of resources and improve policy-making. However, data can also be used to put people under complete surveillance, in breach of their fundamental rights. In an interconnected electronic world, individual pieces of data can no longer be regarded in isolation. With data being stored for very long periods, your online behaviour as a teenager might affect your professional career later. Citizens are increasingly aware that they are being constantly "watched" by public authorities and private entities. This challenges their trust in both, particularly as electronic data collection is often done invisibly. This growing lack of trust is damaging for democracy and for business.

This is why the protection of personal data is so crucial. Safeguards are necessary to give citizens and consumers trust in administration, business and other private entities. If data are the new currency, we need to learn the painful lessons of the banking industry – weak regulation and excessive faith in the market will lead to catastrophic loss of trust, with consequences for every single citizen.

A strong and intelligent approach to creating a value-driven set of European norms and principles on data collection, processing and sharing, together with adequate rules protecting citizens against short-sighted (though understandable) business interests is both necessary and inevitable. In the long run, citizens and democratic societies as well as businesses can only profit from strong safeguards. ■

ANONYMISATION

YOU ARE NOT A NUMBER

Whenever we browse the internet or send data over networks, we leave electronic traces. These traces can be used to identify us and the people with whom we communicate. Anonymisation means removing or obscuring information from these electronic traces that would allow direct or indirect identification of a person.

One of the big advantages of anonymisation is, for example, to allow research that would otherwise not be possible due to privacy concerns. For instance, using everyone's medical records to find disease patterns could improve health care, but could also seriously infringe on people's privacy. It is claimed that the solution is to remove direct identifiers such as names, birth dates, and addresses, so that the data cannot be traced back to individuals. Governments, industry and researchers tend to claim that effective anonymisation of personal data is possible and can help society to ensure the availability of rich data resources whilst protecting individuals' privacy.

Written by:

Foundation for Information Policy Research, UK
http://fipr.org

Unfortunately, this is simply not the case – as scientists have known for a long time. For example, in 1997, researchers were already able to re-identify individual patients from a large set of medical records reduced to post code and date of birth. In 2006, a study found that if you know how a user rated just six films, you can identify 99% of the users in the Netflix (an online video rental service) database.

How is this possible? The main problem is that effective anonymisation does not just depend on stripping away direct identifiers (name, address, national identification number, date of birth) from a data set. Instead, the relevant measure is the size of the "anonymity set" – that is, the set of individuals to whom data might relate. If you are described as "a man" the anonymity set size is

"Anonymisation means removing or obscuring information from these electronic traces that would allow direct or indirect identification of a person."

"The main problem is that effective anonymisation does not just depend on stripping away direct identifiers [...]. Instead, the relevant measure is the size of the "anonymity set" - that is, the set of individuals to whom data might relate."

three and a half billion, but if you're described as "a middle-aged Dutchman with a beard" it is maybe half a million and if you're described as "a middle-aged Dutchman with a beard who lives near Cambridge" it might be three or four.

Pseudonymisation, that is replacing the name and other direct identifiers with a new identifier – e.g. "John Smith, 1 High Street" becomes "person 45684231" – does not resolve this problem either, irrespective of whether, or how well the pseudonym is encrypted. Suppose we gave everyone in the world an ID card with a unique number. What will happen? You start with a single pseudonymous incident, such as a drug prescription: "human no. 45684231 got penicillin on 3 Feb 2009". The anonymity set size just shrunk from seven billion to a few hundred thousand. Then along comes a second incident: "human no. 3,265,679,016 got codeine on 14 May 2009". Now it's down to a few hundred or even a few dozen. A couple more incidents, and the individual is uniquely specified.

As more and more "Big Data" data sets are released, the possibility of identifying people in any single "anonymised" data set by using data from other large data sets increases greatly. With current – and foreseeable future – technology, it is safe to say that anonymisation no longer works when identities are actively sought. This poses major challenges, in particular in relation to "Big Data", that are insufficiently acknowledged or addressed to date.

As we have seen, we cannot rely on anonymisation to be completely secure. In this context, transparency regarding the technologies being used, open peer review by security engineering experts and responsible disclosure procedures will at least provide early warnings over compromised databases and raise standards. ■

This section draws heavily on advice to a major EU study, provided to the authors of the study (Prof. Douwe Korff and Dr. Ian Brown) by Prof. Ross Anderson, quoted on p. 50 of Working Paper No. 2, produced for that study and on the FIPR submission to the ICO on the latter's draft Anonymisation Code of Practice, also drafted by Prof. Anderson.

http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf

http://www.fipr.org/120823icoanoncop.pdf

THE PURPOSE LIMITATION PRINCIPLE

USE FOR STATED PURPOSE ONLY

Written by:

Bits of Freedom, The Netherlands
http://bof.nl

Every time an Internet user buys a product online, uses a social networking service or makes a request to a government agency, it provides such a company, service or agency with their personal data. Organisations using these data are called data controllers, and they are obliged to handle personal data in accordance with data protection law. This law is based on a number of basic principles, designed to protect personal data in the hands of all parties, no matter to whom the data were provided.

One of the most important principles is called purpose limitation. Purpose limitation is the principle that a data controller can only collect and use personal data for a specific purpose. This purpose must be properly defined and communicated to the person ("data subject") whose data are being processed. This permits the data subject to know what will happen to his/her personal data. Under certain circumstances, a data controller may use personal data for a purpose other than the one for which the data were collected or provided in the first instance. For example, when you buy a product online, a company may keep your personal information on file in order to send you marketing messages – unless you object to that. It may also use your purchase history data in order to improve its communication to you, even though you provided your data only to buy a product. The law states that personal information may not be used for purposes that are incompatible with the original purpose of data processing. That means that certain uses of data are off-limits. For instance, selling personal data of users to another company or institution (without first getting the data subject's authorisation), or combining the data with data obtained from other sources in order to build up that customer's profile.

Without the principle of purpose limitation, a data controller could collect personal data for a certain purpose and continue to use it any way it wishes. The principle is therefore an important pillar to defend privacy, since it defines how much protection personal data receive once they have been collected by a controller. Weakening this principle would result in a major decrease of the protection of privacy of users. ■

"Consent is one out of six legal grounds on which personal data can be processed."

CONSENT TO DATA PROCESSING

WITH YOUR PERMISSION

A data controller can process personal data of users on the condition that users consent to such processing. Consent is one out of six legal grounds on which personal data can be processed. Other grounds include processing in order to carry out contractual obligations or to comply with a law. Consent to processing of personal data must meet a number of requirements in order to be valid.

In the first place, consent must be explicit. Putting consent wording in general terms of use, or asking users to click a button saying "I agree" without supplying the necessary information is not sufficient. Pre-ticked boxes that users have to un-check are also not a valid method of expressing or obtaining consent.

Secondly, consent must be specific and well-informed. This means that users have to be properly informed about the processing they agree to, before the processing takes place. The purposes of the processing must be clear and users must really understand which of their data are being processed. They must also understand the consequences of the processing and how this may affect them in the future. Very often, the information provided to users does not meet this requirement. Processing of data is often complex and involves further combining of data and further use, the consequences of which are unknown.

Written by:

Bits of Freedom, The Netherlands
http://bof.nl

Therefore, information about data processing is uniet, or provided only in very legalistic wording.

Finally, consent must be given freely. This criterion implies that a user has a real choice to consent to processing. This also is often not the case, for instance where there is an imbalance between the data controller and the user. This is the case between an employer and its employees, but can also be the case when a data controller has a great deal of market power and is offering a service that no one else offers.

To sum up, consent should always be meaningful in order to be valid, and with the criteria that consent must be freely given, specific, informed and explicit, users can actually be in a position to give such a meaningful consent. ■

BIG DATA

INDUSTRIAL RAW MATERIAL

Written by:

Privacy International, UK
http://privacyinternational.org

"Big Data" is the popular description of the accumulation of vast and complex information databases. It refers, for example, to the mass of data that comes from millions of sources (such as a search engine's store of Internet searches or Wikipedia's database of changes to its pages) that cannot be managed or analysed through conventional "local" techniques that could be carried out on a single server or desktop computer.

Constantly improving processing power and new techniques for data analysis mean that "Big Data" can be created from countless sources and scrutinised to discover trends and characteristics that might otherwise remain hidden. For example, by pooling and analysing the "communications data" from tens of millions of phone calls, it is possible to discover an almost infinite combination of factors relating to the nature of communications, relationships between users and the behaviour of consumers.

The creation of Big Data therefore permits organisations to create information about data that were never apparent or intended in the source information. In the context of medical research, for example, a health customer may never have intended to reveal genetic relationships with other people, but Big Data enables such connections to be created. Indeed, the power of this technique is such that systems can now handle data measured in exabytes.[01] Thousands of servers may well be required to conduct processing on such scales.

The Gartner group defines Big Data as "high-volume, high-velocity, and/or high-variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization." This can also be expressed as using unprecedented processing power to extract hidden layers of information from masses of "ordinary" data pulled from a variety of different sources.

This technique is becoming exceptionally valuable for companies and governments. For example, Walmart handles more than 1 million customer transactions every hour, which is imported into databases estimated to contain more than 2.5 petabytes[03] of data – the equivalent of 167 times more information than contained in all the books in the US Library of Congress. This information is subject to detailed analysis and can produce behavioural trends and consumer profiling to a level of detail never before imagined. ■

01 An exabyte is 1,000,000,000,000,000,000 or 10^{18} bytes of data. Home computer users will have come across megabytes (one million) and gigabytes (one billion). An exabyte is a billion gigabytes.

02 A petabyte is 10^{15} bytes, or a million gigabytes.

DATA SECURITY & DATA BREACHES

HANDLE WITH CARE

The capacity of computer systems to store and process personal information has been constantly increasing for several decades. The scale of the personal information held by such systems now is so huge that it is almost impossible to understand.

Indeed, it is generally accepted that it is no longer possible to create an audit of information being stored in relation to any single individual. A decade ago, the British newspaper The Guardian commissioned research into this question. Its conclusion was that "details of the average economically active adult in the developed world are located in around 700 major databases – enough processed data to compile a formidable reference book for each person." [03]

Since that era, the amount of personal information being held in computer systems has increased dramatically – not just because of technical improvements, but also because of the emergence of user-generated systems such as online social networking and Web 2.0.

As this mass of personal information increases, and as it moves into new processing environments such as Cloud Computing and Big Data, the resulting security threats also increase. Although substantial work is being conducted to harmonise and improve security measures, the threat continues to create huge challenges for all organisations holding personal information.

03 The Guardian: Private virtue
http://www.guardian.co.uk/uk/2002/sep/07/privacy2

Written by:

Privacy International, UK
http://privacyinternational.org

This tension is never more evident than when large and complex information systems intersect with older and more unstable information techniques such as laptops or portable data devices (such as USB keys or DVDs). Nearly all large organisations experience this security problem, sometimes with disastrous consequences. According the Privacy Rights Clearinghouse, a total of 227,052,199 individual records containing sensitive personal information were involved in security breaches in the United States between January 2005 and May 2008.

In the United Kingdom, the situation is just as alarming. Figures from the UK Information Commissioner's Office show that local government data leaks increased by 1609% over the last five years, while other public organisations recorded a 1380% rise. Private organisations noted a 1159% surge in data leaks.

Perhaps the best known of these incidents occurred in 2007, when two CDs containing details of the families of child benefit claimants stored by Her Majesty's Revenue and Customs (HMRC) went missing in the post. HMRC's handling of data was described by the Independent Police Complaints Commission as "woefully inadequate" and staff were described as "muddling through". Twenty five million people were affected by the leak. ■

DATA PROTECTION BY DESIGN & BY DEFAULT

BUILT WITH PRIVACY AS STANDARD

Written by:

Access, international
https://www.accessnow.org

To facilitate a flourishing Internet economy, consumers need to be able to trust the services they use online. This means that they do not need to worry that they are giving companies more data than necessary for the service being used. Any data that are shared needlessly present a risk.

Therefore, it is increasingly important to ensure that privacy protections are built into the design and implementation of the products and services. This is the concept of data protection by design and by default, which are described in Article 23 of the proposed EU Data Protection Regulation. The core of this approach is to give users greater control over their personal data.

Data protection by design means that controllers of data – whether companies or public bodies – take a positive approach to protecting privacy, by embedding it into both technology (for example hardware like computer chips or services like social networking platforms) and into their organisational policies (through, for example, the completion of privacy impact assessments). This requires thinking of privacy and data protection from the beginning of the development of a product or service: "Do we really need to collect these data? Is there a way to have the same functionality without collecting them?" When such protections are built in from the beginning, they can help to prevent invasions of privacy rights (such as costly data breaches) before they occur and reduce their damage if they do occur - for both citizens and business.

"Everyone is guaranteed a high level of protection, allowing everyone the opportunity to consciously choose the privacy setting that they prefer."

"The key is for users to be in control - how much you share should be your choice and not a choice made for you by the service provider."

Pivotal to this approach is privacy by default, which means that when a user receives a product or service, privacy settings should be as strict as possible, without the user having to change them. This way, everyone is guaranteed a high level of protection, allowing everyone the opportunity to consciously choose the privacy setting that they feel most comfortable with – rather than the service provider making a guess about what they might prefer. Service providers should support their users in this by providing user-friendly methods to change privacy settings. They should also be transparent about their data processing practices and supply understandable privacy policies.

While one could imagine that these concepts may not apply to all services, such as social networks, privacy-friendly default settings can be very easily implemented. For example, when you join a social network, the initial settings on your profile can be set to share only with people you know, and not other unknown parties. Privacy by default is implemented on some social networks, so it is neither a new nor a revolutionary idea. Sharing does not inherently mean an end to privacy. In fact, with effective privacy by design and by default, you can have both. The key is for users to be in control – how much you share should be your choice, and not a choice made for you by the service provider. Privacy by design and by default is putting users in charge of their own data... by design and by default. ■

PRIVACY & DATA PROTECTION ON SOCIAL NETWORKS

SHARING WHILE CARING

Written by:

Access, international
https://www.accessnow.org

Over recent years, social networks have gained an important role in enabling citizens to connect with each other, obtain information quickly and participate in matters that affect them. This is a positive development as social networks allow people to become more active and informed citizens.

Social networking sites are usually free to join, so how do they make money? These sites collect our data – through the information that we share – and use these data to sell 'targeted' advertising. These data include information regarding pictures, articles or status updates, called 'user generated content', who is in our circle of friends, what can be assumed about us based on information that our friends share, advertisements we click on, sites we visit that contain advertising or 'like' buttons loaded from the social network's servers, etc. Our 'traffic data', meaning the times we log in, our location, etc. is also used to make assumptions about what type of person we are and what advertising might be interesting for us. In other words, we 'pay' for the service with information about everything we – and our friends – do on the site and on related sites. Data protection is therefore no longer just a privacy right, because data have also become an economic good, which means it also is property.

As so much information can easily be collected, stored, shared, sold, bought and combined, these companies have very detailed profiles of who we are (or, at least, who they think we are). These assumptions can pose a problem if they are

We 'pay' for the service with information about everything we (...) do on the site and on related sites.

used to discriminate on the basis of assumed health status, age, gender, sexual orientation, etc. The situation gets even more problematic if governments seek access to and use these data, which is happening more and more frequently, often through informal government/industry relationships that do not involve a warrant or judicial authorisation.

Participating on a social network by using a pseudonym (a name that is not directly connected to your legal name) is one way to achieve limited additional protection of your privacy – although this is needlessly banned by some social networks. Also, having control over your privacy settings is important, so you can be sure that you are consciously making a decision about whom you are sharing with.

If users are not happy about the service or the way the company deals with their data, they should be empowered to move all their information away from that service – this is called the right to 'data portability'. Easy transfer of data will increase competition, consumer choice and innovation.

Also, terms of service agreements should be clear and easy to understand so users can make informed decisions about which platforms to use. Ensuring that we have strong privacy protections – and other rights like free expression – on social networking platforms means that we can make technology work for us, and not against us. This will also ensure a trusted and predictable environment for innovation. ■

"Having control over your privacy settings is important, so you can be sure that you are consciously making a decision about whom you are sharing with."

CLOUD COMPUTING

PREDICTABLE PROTECTION IN AN UNPREDICTABLE ENVIRONMENT

Written by:

Privacy International, UK
http://privacyinternational.org

The name 'cloud computing' was inspired by the cloud symbol that is often used to represent the Internet in diagrams and charts. It is a rather unclear term and has many definitions, the most widely accepted of which is the one of the US National Institute of Standards and Technology: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort or interaction with the service provider."[04] In layman's terms, this means using computer services – software or data storage – not at your own computer but somewhere on the Internet, on servers operated and managed by others; examples are web-based email (like Hotmail or Gmail), music and video streaming, photo sharing, social networking, payment services, or online office applications (like word processing or spreadsheets).[05]

Cloud computing itself is not a new technology, but a relatively new way of delivering computing services. It came about because the computing giants (such as Google, Amazon, Microsoft and eBay) built massive data centres with very fast connections to the global Internet to run their own businesses, and then spotted the revenue potential in offering spare data storage and computing services to other companies. These data centres can be located anywhere around the world, inside or outside the EU.

Cloud services can bring many benefits to users, particularly convenience and flexibility, reduced costs, ease of use, improved access to online content, and automatic maintenance and updating. However, there are also important worries which centre on control of the data and their geographical location. Who has access to them? How can they be used? How easy is it to move the data from one cloud service to another? How secure are they? Who is responsible if the data are lost or misused?

Current data protection legislation does not provide adequate answers to all these questions. There are ambiguities regarding the role and responsibilities of cloud service providers; when EU law applies and when it does not; enforcement and redress; transfers to countries outside the EU; and foreign law enforcement authorities' access to data (see page 18). If these issues are not addressed in a comprehensive, effective and "future-proof" way in the review of the data protection framework, it will be effectively impossible to safeguard the fundamental right to privacy provided for in the European Charter of Fundamental Rights. ■

04 NIST: The NIST Definition of Cloud Computing, 2011, p.2
http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf

05 Cloud Computing, How the Internet Works
http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf

PROFILING

USING PERSONAL DATA TO GUESS AT PREFERENCES

Chapter written by:

Foundation for Information Policy Research, United Kingdom
http://fipr.org

Profiling means collecting and using pieces of information about individuals to make assumptions about them and their future behaviour.[07]

For example, someone who buys baby clothes and nappies will often buy a pram. In more abstract terms, "people who did X and Y often also did Z. You did X and Y, so we will treat you as if you are likely to do Z". This logic can either be determined in advance, or be dynamically generated from data collected earlier. The mathematical logic used to make these assumptions are known as profiling algorithms.

With hugely increased data collection and ever-growing computing power, these algorithms are becoming extremely complicated. There are three main problems with profiling:

- The algorithms are not designed to be perfect, and the rarer the activity they are used for, the higher the risk of mistakes. In simple terms: profiling should never be used in relation to characteristics that are too rare to make them reliable, nor to make significant decisions about individuals.[08]

- Almost inevitably, profiling is likely to perpetuate and reinforce societal inequality and discrimination against racial, ethnic, religious or other minorities. Profiling can have these effects even if such information is not directly used. Therefore, both the results of profiling and the underlying algorithms must be diligently monitored.[09]

- Profiling algorithms can be so complex that even the organisations using them are no longer able to understand their logic. In fact, they might not even try or be able to understand that logic at all, particularly because the algorithms are often protected as "trade secrets". There is a serious risk of unreliable and (in effect) discriminatory profiling being widely used, in matters of real importance to individuals and groups, without the required checks and balances to counter these defects.[10]

Profiling poses a fundamental threat to the most basic principles of the rule of law and the relationship between citizens and government or between customers and businesses in a democratic society. ■

07 For a more detailed analysis, see http://protectmydata.eu/topics/limitations/ and Korff, Douwe, Comments on Selected Topics in the Draft EU Data Protection Regulation (September 18, 2012), see http://ssrn.com/abstract=2150145.

08 For a good basic discussion (with further references), see the "security blog" on the issue by Bruce Schneier, Why Data Mining Won't Stop Terror, 3 September 2006 on http://www.schneier.com/blog/.

09 See Oscar Gandy, Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage, 2009, see http://www.ashgate.com/isbn/9780754679615.

10 See the discussion of the (then) most sophisticated systems used by the U.S. national security authorities in Korff & Brown, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2004, and in particular the technologies developed in the so-called "Total Information Awareness" program, discussed in Paper No. 3: TIA & PNR, by Douwe Korff: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/tia_and_pnr.pdf

ACCESS BY FOREIGN LAW ENFORCEMENT

THE LONG ARM OF THE LAW

Chapter written by:

Foundation for Information Policy Research, United Kingdom
http://fipr.org

Internet and communication service providers often process and store data outside their customers' jurisdiction, or in "the cloud". This can lead to situations in which data that could, for example, be useful evidence in investigating a case is stored outside the jurisdiction of the investigating government agency. In such cases, these agencies are increasingly asking cloud service providers directly for such data held outside their jurisdiction, rather than using agreed mutual legal assistance procedures.

This is a big change, compared with what we are used to in the "offline world". The long-established principle is that when law enforcement authorities or national security agencies in one country want to obtain access to evidence in another country, they have to go through "Mutual Legal Assistance Treaties" (MLATs). These can be bilateral (state to state) or multilateral, as in the case of the EU–US Mutual Legal Assistance Agreement.

Usually, these treaties involve a court in the first country requesting a court in the second country to issue an order for the seizure and handing over of the materials. This normally involves legal proceedings to ensure that the rights of all affected persons and entities are respected. MLATs are complex and can be cumbersome in practice. However, bypassing established MLATs usually constitutes an infringement of the sovereignty of the second state (where the data are), and a negation of the legal rights of interested parties under the laws of that state, especially if those parties are headquartered or established in that second state. States can of course, by treaty, allow other states to obtain evidence directly from

"Agencies are increasingly asking cloud service providers directly for such data held outside their jurisdiction"

"procedures need to be streamlined and dramatically accelerated, especially in cases of urgency, such as an immediate risk to life."

controllers in their territory. Similarly, if states abide by such requests for a long time, this can become acceptable under customary international law. However, this is not yet the case for requests for data held by Internet and communication service providers.

States must therefore, under current international law, abide by established MLAT procedures. The increasing tendency to ignore this requirement is a threat to the international legal order in relation to the Internet. States should therefore insist that demands for access to data held on their territory should be made only through the applicable Mutual Legal Assistance arrangements (bilateral or multilateral MLATs), and be clear that extraterritorial demands for access to data in their jurisdiction constitutes a violation of sovereignty. This has been recently strongly reaffirmed by European Commissioner for Justice, Fundamental Rights and Citizenship, Commissioner Reding, who stressed that, if EU-based companies provide data directly to the US authorities on demand, they are likely to be in breach of European data protection law.[06]

That is not to say that there is no need for reform – on the contrary. MLAT procedures need to be streamlined and dramatically accelerated, especially in cases of urgency, such as an immediate risk to life. However, that should be done in full recognition of the need to respect international human rights standards also in relation to transnational police and security service investigations. Otherwise a paradoxical situation could arise in which it would be easier to obtain data about a person by the government of a foreign country, than for that person's own government. ■

This section is based on relevant passages in Ian Brown & Douwe Korff, Digital Freedoms in International Law Practical Steps to Protect Human Rights Online, a report written for the Global Network Initiative in 2012, and available from:

https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

06 European Parliament written question 2430/2012 http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-002430&language=EN

MAKING IT WORK

A GOOD LAW NEEDS GOOD ENFORCEMENT

In the seventeen years since the European Union adopted the current Data Protection Directive, we have learned a lot about the rights and wrongs of upholding the fundamental right to data protection.

The most important lesson is that a good law needs good enforcement. Some countries in Europe have strong data protection laws enforced by adequately staffed and independent data protection authorities, with sufficient legal powers and the necessary technical expertise. Unfortunately, the situation is very diverse across Europe, leaving some citizens with far weaker protections than others and businesses with a very complicated patchwork of rules that they need to follow. This was the reason that the European Commission proposed a single Regulation, for the whole of the European Union.

Effective and predictable levels of enforcement across Europe will serve to enhance and preserve the European Union's global leadership in the area of privacy protection. It will also serve to make privacy protection a reflex rather than an

obligation for businesses and it will transform consumer expectation of privacy from a hope to a demand.

Such a development is crucial today, due to the huge opportunities offered by developments such as social networks, "Big Data" and cloud computing. To get the full benefit from these developments, citizens need to trust them. For this trust to be realised, privacy needs to be built into every stage of the design process – privacy by design – as well as every stage of the implementation process – purpose limitation and privacy by default.

Without a successful reform of the data protection framework, we will be left with a series of legal loopholes, a range of unpredictable enforcement gaps and a "race to the bottom" where nobody – neither citizens nor business – knows what law will be enforced. Now is our one opportunity to develop a strong legal framework, inspiring good practice by business, guided by clear, predictable legal principles and enforcement, creating a maximum of commercial opportunities, in an environment of trust. ■

For a more in-depth analysis of these topics, as well as EDRi's proposed amendments for the review of the data protection framework, please refer to:

http://protectmydata.eu

A comprehensive analysis on selected aspects of the draft regulation is also available from: Korff, Douwe, Comments on Selected Topics in the Draft EU Data Protection Regulation (September 18, 2012).

http://ssrn.com/abstract=2150145

Summaries and proposed amendments:

http://ssrn.com/abstract=2150151

"Now is our one opportunity to develop a strong legal framework"

EUROPEAN DIGITAL RIGHTS

EDRI.ORG/PAPERS

With financial support from the EU's Fundamental Rights and Citizenship Programme.