The rule of law on the Internet and in the wider digital world

Executive summary
and Commissioner's recommendations

Issue paper

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

The rule of law on the Internet and in the wider digital world

Issue paper published by the Council of Europe Commissioner for Human Rights

Executive summary and Commissioner's recommendations

Council of Europe

Issue papers are published by the Commissioner for Human Rights to contribute to debate and reflection on important current human rights issues. Many of them also include recommendations by the Commissioner for addressing the concerns identified. The opinions expressed in these expert papers do not necessarily reflect the Commissioner's position.

The full Issue paper in English can be obtained at: commissioner@coe.int; the electronic version is also available at http://www.coe.int/web/commissioner/publications

Cover photo: © Shutterstock
Cover and layout: Documents and Publications Production Department (SPDP) Council of Europe

Printed at the Council of Europe

Acknowledgements:

This issue paper was prepared by Professor Douwe Korff, Visiting Fellow, Yale University (Information Society Project), and Oxford Martin Associate, Oxford Martin School, University of Oxford, UK. He and the Commissioner are also grateful to Joe McNamee of European Digital Rights, EDRi, for the very useful comments and additions he provided to the draft version of this issue paper, in particular on privatised law enforcement.

Contents

Executive summary

This issue paper addresses a pressing question: how can we ensure that the rule of law is established and maintained on the Internet and in the wider digital world? Section 1 describes the range of online activities and the threats to this environment; section 2 discusses the emerging "Internet governance" principles, and notes the special control exercised over the digital world by the USA (and the UK, in respect of Europe), which could lead to fragmentation of the Internet in response. Section 3 sketches the international standards of the rule of law, and some problems in the application of law in this new environment. Section 4 looks in some more detail at the main issues emerging from the earlier sections – freedom of expression, privatised law enforcement, data protection, cybercrime and national security – and discusses the delicate balances that need to be struck.

The Council of Europe Commissioner for Human Rights has formulated a number of recommendations on the basis of the issues raised by this issue paper; these are set out after this executive summary.

A new environment for human activities

We live in a global digital environment that has created new means for local, regional and global activities, including new types of political activism, cultural exchanges and the exercise of human rights. These activities are not virtual in the sense of "not truly real". On the contrary, they are an essential part of real citizens' lives. Restrictions on access to the Internet and digital media, and attempts to monitor our online activities or e-communications, interfere with our fundamental rights to freedom of expression and information, freedom of association, privacy and private life (and possibly other rights such as freedom of religion and belief, or the right to a fair trial).

The new global digital environment of course also creates a new space for unlawful behaviour: for the dissemination of hate speech or child pornography, incitement to violence, breaches of copyright ("piracy"), fraud, identity theft, money laundering and attacks on the e-communications infrastructure itself through malware (such as Trojans and worms) or "denial of service" attacks. Cybercrime and cybersecurity have become major concerns.

These threats are increasingly transnational, and there is a broad international consensus on the need to deal with cybercrime, cybersecurity and terrorism, but there is much less agreement on specifics – or even what constitutes a threat.

Four issues stand out. First, state actions aiming to counter cybercrime, threats to cybersecurity and threats to national security are increasingly intertwined; the boundaries between such activities are blurred, and the institutions and agencies dealing with them work more closely together. Second, states are now co-ordinating their actions in all these regards. Third, the work of national security and intelligence agencies increasingly depends on monitoring the activities of individuals and groups in the digital environment. Fourth, instead of *ex post facto* law enforcement, the emphasis is now on intelligence and prevention, with law-enforcement agencies using techniques – and technologies – previously reserved for secret services.

The nature of the digital environment

Dangerous data

In an age of "Big Data" (when data on our actions are shared and/or exploited in aggregate form) and the "Internet of Things" (when more and more physical objects – things – are communicating over the Internet), it is becoming difficult to ensure true anonymisation: the more data are available, the easier it becomes to identify a person. Moreover, the mining of Big Data, in ever more sophisticated ways, leads to the creation of profiles. Although these profiles are used to spot rare phenomena (e.g. to find a terrorist in a large set of data, such as airlines' passenger name records), they are unreliable and can unwittingly lead to discrimination on grounds of race, gender, religion or nationality. These profiles are constituted in such complex ways that the decisions based on them can be effectively unchallengeable: even those implementing the decisions do not fully comprehend the underlying reasoning.

The digital environment can by its very nature erode privacy and other fundamental rights, and undermine accountable decision making. There is enormous potential for undermining the rule of law – by weakening or destroying privacy rights, restricting freedom of communication or freedom of association – and for arbitrary interference.

Global and private, but not in the sky

Because of the open nature of the Internet (which is its greatest strength), any end point on the network can communicate with virtually any other end point, following whatever route is calculated as being most efficient, the data flowing through all sorts of switches, routers and cables: the Internet's physical infrastructure. The electronic communications system is transnational, indeed global, by its very nature; and its infrastructure is physical and located in real places, in spite of talk of a Cloud. At the moment, many of these physical components are in the USA and many of them are managed and controlled by private entities, not by governmental ones.

The main infrastructure for the Internet consists of high-capacity fibre-optic cables running under the world's oceans and seas, and associated land-based cables and routers. The most important cables for Europe are those that run from continental Europe to the UK, and from there under the Atlantic to the USA. Given the dominance of the Internet and of the Cloud by US companies, these cables carry a large proportion of all Internet traffic and Internet-based communication data, including almost all data to and from Europe.

Who is in control?

Internet governance

Important Internet governance principles have been put forward, by the Council of Europe and others, that stress the need to apply public international law and international human rights law equally online and offline, and to respect the rule of law and democracy on the Internet. These principles recognise and promote the multiple stakeholders in Internet governance and urge all public and private actors to uphold human rights in all their operations and activities, including the design of new technologies, services and applications. And they call on states to respect the sovereignty of other nations, and to refrain from actions that would harm persons or entities outside their territorial jurisdiction.

However, these principles still remain largely declaratory and aspirational: there is still a deficiency in actual Internet governance arrangements that can be relied on to ensure the application of these principles in practice.

Also, Internet governance must take account of the fact that – partly because of its corporate dominance, and partly because of historical arrangements – the USA has more control over the Internet than any other state (or even all other states combined). Together with its close partner, the UK, it has access to most of the Internet infrastructure.

The former US National Security Agency contractor Edward Snowden has revealed that the USA and the UK are using this control and access to conduct mass surveillance of the Internet and of global electronic communications systems and social networks. There are fears that states may respond to the Snowden revelations by fragmentation of the Internet, with countries or regions insisting that their data are routed solely through local routers and cables, and stored in local clouds. This risks destroying the Internet as we know it, by creating national barriers to a global network. Unless the USA improves compliance with international human rights standards in its activities that affect the Internet and global communication systems, the movement towards such a truncated Internet will be difficult to stop.

Private-sector control

Much of the infrastructure of the Internet and the wider digital environment is in the hands of private entities, many of them US corporations. This is problematic because companies are not directly bound by international human rights law – that directly applies only to states and governments – and it is more difficult to obtain redress against such companies. In addition, private entities are subject to the national laws of the countries where they are established or active – and those laws do not always conform to international law or international human rights standards: they may impose restrictions on activities on the Internet (typically, on freedom of expression) that violate international human rights law; or they may impose or allow interference, such as surveillance of Internet activity or e-communications, that is contrary to international human rights law; and such actions may be applied extraterritorially, in violation of the sovereignty of other states.

The application of national law to the activities of private entities controlling (significant parts of) the digital world is extremely complex and delicate. Of course states have a right, and indeed a duty, to counter criminal activity that uses the Internet or e-communication systems. In this, they naturally enlist the help of relevant private actors. Responsible companies will also want to avoid their products and services being used for criminal purposes. Nonetheless, in such circumstances, states should in their actions both fully comply with their international human rights commitments and fully respect the sovereignty of other states. In particular, states should not circumvent constitutional or international law obligations by encouraging restrictions on human rights through "voluntary" actions by intermediaries; and companies, too, should respect the human rights of individuals.

The rule of law in the digital environment

The rule of law

The rule of law is a principle of governance by which all persons, institutions and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced, independently adjudicated and consistent with international human rights norms and standards. It entails adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in applying the law, separation of powers, participation in decision making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.

The basic "rule of law" tests developed by the European Court of Human Rights

The European Court of Human Rights has developed elaborate "rule of law" tests in its case law, and these have also been adopted by other international human rights bodies. To pass these tests, all restrictions on fundamental rights must be based on clear, precise, accessible and foreseeable legal rules, and must serve clearly legitimate aims; they must be "necessary" and "proportionate" to the relevant legitimate aim (within a certain "margin of appreciation"); and there must be an "effective [preferably judicial] remedy" against alleged violations of these requirements.

"Everyone", without discrimination

It is one of the hallmarks of international human rights law since 1945, and one of its greatest achievements, that human rights must be accorded to "everyone", to all human beings: they are humans' rights, not just citizens' rights.

Thus, subject to very limited exceptions, all laws, of all states, affecting or interfering with human rights must be applied to "everyone", without discrimination "of any kind", including discrimination on grounds of residence or nationality.

Because of the unique place of the USA and US companies in the functioning of the Internet, the constitutional and corporate legal framework in the USA is of particular importance. However, in contrast to the above-mentioned principle of international human rights law, many of the human rights guarantees in the US Constitution and in various US laws relating to the digital environment apply only to US citizens and

non-US citizens residing in the USA ("US persons"). Only "US persons" benefit from the First Amendment, covering free speech and freedom of association; the Fourth Amendment, protecting US citizens from "unreasonable searches"; and most of the (limited) protections against excessive surveillance provided by the main pieces of legislation on national security and intelligence (FISA Amendment and Patriot Acts).

"Within [a contracting state's] [territory and] jurisdiction"

The duty of states to comply with their responsibilities under international human rights law also when acting extraterritorially

The main international human rights treaties, including the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR), oblige states to "ensure" or "secure" the human rights laid down in those treaties to "everyone subject to their jurisdiction" (or "within their jurisdiction"). This requirement is increasingly given a functional rather than a territorial meaning – as has recently been reaffirmed by the Human Rights Committee and the European Court of Human Rights. In other words, each state must ensure or secure these rights to anyone under its physical control or whose rights are affected by its (or its agencies') actions.

Thus, states must comply with their international human rights obligations in any action they take that may affect the human rights of individuals – even when they act extraterritorially, or take actions that have extraterritorial effect.

This obligation has specific consequences for data – what the digital world is made of – and especially for personal data, as is recognised by European data-protection law, which protects all individuals whose data are processed by European controllers, irrespective of their place of residence, nationality or other status. However, the USA formally rejects this application of international human rights law. In view of the predominance of the USA (and of US corporations that are subject to that country's jurisdiction) in the digital environment, this poses a serious threat to the rule of law in that new environment.

The difficulty of competing and conflicting laws applying simultaneously to online activities, with particular reference to freedom of expression

The problem of competing – and conflicting – application of different national laws to Internet materials and Internet activity is an issue that needs to be addressed urgently to guarantee the rule of law on the Internet.

The issue at stake is not the right of governments to take actions that comply with international law and that are necessary and proportionate in a democratic society. Within these limits, governments should of course remain free to make decisions on regulation within their jurisdiction. The issue is the ability and right of national governments or courts to take measures that have the effect of imposing restrictions in third countries where the individuals in question are acting in accordance

with the laws of their own country of residence which, unlike foreign laws, should be known (or "knowable") to them and foreseeable in their application.

In principle, individuals and companies that make information available from their country of residence or establishment should have to comply only with the laws of that country; and individuals who access or download materials from foreign websites when they could and should know that the materials are illegal in their country of residence can be expected to adhere to the laws of the latter country. States should in principle only exercise jurisdiction over foreign materials that are not illegal under international law in limited circumstances, notably when there is a clear and close nexus between the materials or the disseminator and the state taking action.

Human rights and private entities

Human rights law and the Ruggie Principles and Council of Europe and other guidance

International human rights law essentially applies only to states, and to actions (or omissions) of public authorities. However, new international standards are emerging, intended to be applied by companies. The most important are the UN "Guiding Principles on Business and Human Rights" (the Ruggie Principles), drafted by the United Nations Secretary-General's Special Representative for Business and Human Rights, Professor John Ruggie. However, the Ruggie Principles still focus on the duty of host states to act against human rights violations by companies. They do not deal in detail with the converse situation, where states make demands of companies that would lead companies into violations of international human rights law.

It seems important that further guidance be developed, by the Council of Europe and others, on the responsibilities of businesses that face (or that put themselves in situations where they may well face) demands from governments, or from other private entities, to support measures that may violate international human rights law (as further detailed under the section on privatised law enforcement).

Filtering and blocking by Internet and e-communications companies on the instructions of – or on the basis of "encouragement" by – states

Apart from criminalising material on the Internet – which increasingly happens when the materials are produced in another country, *ex post facto*, after the materials have been published and accessed – states are also increasingly trying to prevent (block) access to certain materials and information online. Such blocking or filtering is performed by software or hardware that reviews communications and decides on the basis of pre-set criteria whether to prevent the materials from being forwarded to an intended recipient, often someone browsing the Internet.

It is perhaps not surprising that repressive states try to block access to opposition websites, and that theocratic regimes do the same with websites they deem to be blasphemous. But increasingly states that supposedly respect the rule of law – including Council of Europe member states – are also trying to block access to materials they regard as unacceptable. Or, in a more insidious and less accountable

framework, they "encourage" the gatekeepers to the Internet (ISPs and MNOs) to do this "voluntarily", outside a clear public-law legal framework.

Usually, in democratic countries, blocking or filtering measures have, at least officially and initially, been mainly aimed at strongly legitimate targets: racist or religious "hate speech" or child pornography. However, the systems suffer from major flaws in the way they work:

- blocking is inherently likely to produce (unintentional) false positives (blocking sites with no prohibited material) and false negatives (when sites with prohibited material slip through a filter);
- the criteria for blocking certain websites, but not others, and the lists of blocked websites, are very often opaque at best, secret at worst;
- appeals processes may be onerous, little known or non-existent, especially if the decision on what to block or not block is – deliberately – left to private entities;
- blocking measures are easy to bypass, even for not very technically skilled people;
- crucially, in particular in relation to child pornography, blocking totally fails to address the actual issue: the abuse of the children in question.

The above problems are compounded by the fact that, once states have introduced blocking against the most serious issues such as child pornography and hate speech, they tend to extend it to all sorts of other matters that they disapprove of. Globally, including in Europe, there have been attempts by states to block sites containing not only hate speech and advocacy of terrorism, but also, for instance, political debate or information on sexual or minority rights.

It is useful to distinguish between two different situations: law-based and non-law-based blocking of content. It is unquestionably the case that there is certain content that is a legitimate target for blocking measures (law-based blocking of illegal content). However, the aim of the blocking measure and the actual technical means used to carry it out remain crucial to determining whether the measure is proportional and therefore lawful – for example, if there is no evidence of significant levels of accidental access to the content in question and if deliberate access remains easy after the blocking measure, the proportionality of the blocking is more questionable.

The matter gets more complicated if the decision of what sites to block is left to private entities, "encouraged" by states that nonetheless claim to bear no responsibility for the blocking (non-law-based blocking of content). Some countries, such as the UK and Sweden, have introduced blocking systems based on voluntary arrangements with ISPs. While all considerations concerning effectiveness and proportionality of the measure remain relevant for this type of blocking, it raises a more general and fundamental question that needs to be addressed: how far are these blocking measures really voluntary and/or do they entail state responsibility? The fact that Article 10 of the ECHR only refers to interferences with this right "by public authorities" does not mean that the state can simply wash its hands of measures by private entities that have such effect – especially not if the state *de facto* strongly encouraged those measures. In such circumstances, the state is responsible for not placing such a system on a legislative basis: without such a basis, the restrictions are not based on "law".

In recent case law, the European Court of Human Rights has clearly noted the dangers of indiscriminate blocking. In its judgment in the case of *Yildirim v. Turkey*, the Court observed that the measure in question – blocking access to all websites hosted by Google Sites from Turkey in order to block a Google site that was regarded as disrespectful of Kemal Atatürk – had produced arbitrary effects and could not be said to be aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all sites hosted by Google Sites. Moreover, the judicial review procedures concerning the blocking of Internet sites were deemed to be insufficient to meet the criteria for avoiding abuse, as domestic law did not provide for any safeguards to ensure that a blocking order in respect of a specific site was not used as a means of blocking access in general. The Court therefore found a violation of Article 10 of the ECHR.

Indiscriminate deep packet inspection (DPI) by companies under court orders issued at the request of other companies, to enforce copyright

Intellectual property rights holders are increasingly asking for filters or blocks, similar to the ones described above, to be imposed on sites that are allegedly facilitating the sharing of pirated content; and are increasingly demanding access to Internet users' details in relation to such alleged sharing, including through the compulsory use of DPI by ISPs to detect probable (or possible) rights-infringers.

DPI requires the "inspector" to examine not just the broad metadata related to the origin or destination of the "packet", but also the content of those communications. "Packets" are singled out on the basis of a pattern or algorithm linked to specific content. For the intellectual property rights-holders, that will be the particular markers of a particular copyright-protected video or photograph. But the same technology allows for searches of essentially anything: a certain political speech, a certain revolutionary song, a trade union banner. These measures are highly intrusive, as they require surveillance of all users of an ISP (or mobile phone network), with the aim of trying to identify the few that are probably (or possibly) infringing copyright, and thus they raise serious issues of necessity and proportionality.

Both the European Court of Human Rights and the Court of Justice of the European Union have issued important judgments that strongly suggest that indiscriminate filtering of all the communications carried by an ISP (or an MNO) – that is, general monitoring or surveillance – for the purpose of identifying possible rights-infringers from the mass of innocent users is contrary to human rights law.

Exercise of extraterritorial jurisdiction by states

A state that uses its legislative and enforcement powers to capture or otherwise exercise control over data that are not held on its physical territory but on the territory of another state – typically by using the physical infrastructure of the Internet and the global communications systems to extract those data from servers in the other state, or by requiring private entities that have access to such data abroad to extract those data from servers or devices in another country and hand them over to the state – is exercising its jurisdiction extraterritorially within the jurisdiction of the other state.

Under general public international law, in the absence of treaties that grant powers of extraterritorial enforcement jurisdiction to foreign agencies, it is not lawful for the first state to do this without the consent of the second state.

The issues, and the balance between them

The issues

Establishing the rule of law on the Internet and in the wider digital world will require clarification of the rules affecting freedom of expression, private entities (particularly corporations) and human rights, data protection and cybercrime; and then the question must be addressed: how are the balances between all of these to be struck in this new environment?

Freedom of expression

National laws relating to activities on the Internet and the wider digital environment, especially laws relating to freedom of expression, often compete and conflict: under the laws of many states, persons making statements online or in electronic communications in, or from, one country can be held liable for that under the laws of another country if the statements violate the latter laws, even if they are lawful where they were made. This poses a fundamental threat to the rule of law on the Internet and in that environment. This has not yet been fully addressed in the case law of the European Court of Human Rights.

As suggested above, the only way to resolve this would be if states and national courts were to show clear restraint by not imposing their domestic legal standards on expressions and information disseminated over the Internet from abroad, unless these are unlawful under international law or present clear links that justify the exercise of the state's jurisdiction.

A further important issue is the liability of individuals or companies managing a website, or even ISPs, for content posted on a website. Here, too, the case law at European level has been limited to date. At the moment, private companies appear to be caught between clear obligations (remove content or face punishment) and unclear obligations (to guarantee access to lawful content to users). As a result, private companies may tend to choose over-compliance and prevent all users from accessing perfectly lawful materials while at the same time protecting themselves against possible claims from affected users by imposing on them loose terms and conditions. These are core issues that need to be resolved.

Privatised law enforcement

The fact that the Internet and the global digital environment is largely controlled by private entities (especially, but not only US corporations) also poses a threat to the rule of law. Such private entities can impose (and be "encouraged" to impose) restrictions on access to information without being subject to the constitutional or international law constraints that apply to state limitations of the right to freedom of expression. These private entities can also be ordered by domestic courts, acting at the request of other private entities, to perform highly intrusive

analysis of their data to detect probable (or just possible) infringements of private property rights, often intellectual property rights. They can be ordered to "pull" data, including governmental, commercial and personal data, from servers in other countries, for law enforcement or national security purposes, without obtaining the consent of the other country – or the consent of the companies or data subjects in the other country – in violation of the sovereignty of the other country, the commercial confidentiality that companies are entitled to, and the human rights of the data subjects.

The United Nations' Ruggie Principles, while indicating the importance of addressing these issues, do not provide the answers. As mentioned, new approaches and guidelines are therefore needed. The Council of Europe has made important contributions to this debate by suggesting that states could be held accountable for failing to ensure that private entities do not violate the human rights of their citizens and that states have an obligation to ensure that general terms and conditions of private companies that are not in accordance with international human rights standards must be held null and void.

Data protection

European data-protection law is founded on a set of basic principles (fair processing; purpose specification and purpose limitation; data minimisation; data quality; and data security) and a set of rights (data subject rights) and remedies (supervision by independent data-protection authorities) that are special reflections of the general "rule of law" principles developed by the European Court of Human Rights. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108) and the EU rules on the matter specify how compliance with the general requirements of human rights law should be ensured in the specific context of the processing of personal data. The European data-protection model is increasingly being taken up outside the Council of Europe area: Convention No. 108 (currently under a process of modernisation) is becoming the global gold standard in guaranteeing the international rule of law in this specific respect, which is crucial for the Internet and the wider digital world.

European data protection has been further strengthened by a judgment of the Court of Justice of the European Union, which has rejected compulsory, suspicionless, untargeted data retention. In connection with the debate on the practices of intelligence and security services prompted by Edward Snowden's revelations, it is becoming increasingly clear that secret, massive and indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security. Such interferences can only be accepted if they are strictly necessary and proportionate to a legitimate aim.

Data protection on European lines provides the first and most important cornerstone for the rule of law on the Internet and in the wider digital world. As a result, it will be crucial to ensure that the review (modernisation) of Convention No. 108, currently under way, does not lead to any lowering of the standards. Accession by the USA to Convention No. 108 would be particularly valuable, not just for US citizens,

but as a move towards a more comprehensive global approach to respect for the fundamental right to data protection and the rights that it enables.

Cybercrime

The Convention on Cybercrime (Cybercrime Convention, ETS No. 185) requires states parties to make certain acts – such as illegal access to computer systems (hacking), illegal interception of electronic communications, the sending of malware, copyright violations and the production or dissemination of child pornography – criminal under their national law; its Additional Protocol requires states parties to criminalise the dissemination of racist and xenophobic material (hate speech). It also makes extensive provision for international co-operation in fighting such crimes, including mutual legal assistance in investigation and preservation of evidence, extradition and similar matters. The convention is open to non-European states and has been ratified by five such states, including the USA.

While the need for an agreement to counter crime in the global digital environment is beyond doubt – and the Council of Europe is to be commended for initiating such a process – the convention is not yet fully geared to ensuring compliance with the rule of law in its implementation by states parties.

One reason for this is that the convention does not contain a comprehensive human rights clause, and so it does not provide protection against states imposing unduly wide criminal offences, or failing to include exceptions or defences in their substantive law (such as a public interest defence for whistleblowers); nor does it protect against double jeopardy or the provision of (formal or informal) assistance to states parties when this could violate human rights.

Another reason is that the convention is not linked to other major instruments developed by the Council of Europe that support the rule of law in digital and/or transnational contexts. Such a linkage seems all the more necessary because the convention is open to states that are not party to the ECHR or have not fully accepted the comparable requirements of the ICCPR (such as the USA in respect of its extraterritorial activities or the rights of "non-US persons"). From the perspective of the rule of law in Europe, accession to the Cybercrime Convention should require both full acceptance by states of their obligations under the ECHR and/or ICCPR and ratification of the Data Protection Convention, the European Extradition Convention, and the European Convention on Mutual Assistance in Criminal Matters.

Finally, Articles 26 and 32 of the convention appear to support the tendency of law-enforcement agencies to resort to "informal" means of information gathering, even across borders, without laying down clear safeguards (for instance, that such informal measures should not be used for intrusive information-gathering activities that normally, in a state under the rule of law, require a judicial warrant); and those two articles also seem to support the tendency of such authorities to increasingly "pull" data directly from servers in other countries, or to demand that companies within their jurisdiction – particularly the main Internet giants – do this for them, without recourse to formal, inter-state mutual legal assistance arrangements, arguably in violation of the sovereignty of the state where the data are found.

The principle – established in Article 16 of Convention No. 108 in relation to mutual assistance between data-protection authorities – that there are clear limitations to the circumstances in which personal data may be collected and/or passed on in transnational activities, should also better inform the Convention on Cybercrime. A number of recommendations and declarations of the Council of Europe Committee of Ministers provide useful guidance on how to strike the balance between upholding data-protection principles and allowing appropriate law enforcement. Compliance with these instruments by member states who are parties to the Convention on Cybercrime should be strengthened.

The drafting of the proposed new additional protocol to the Convention on Cybercrime provides an opportunity to resolve at least some of these issues. With these improvements, the Cybercrime Convention could provide a second cornerstone for the rule of law on the Internet and in the wider digital world.

National security

The European Convention on Human Rights and the Council of Europe Data Protection Convention both in principle apply to all activities of the states that are party to them: although both include some special rules and exceptions, issues of national security are not explicitly excluded. In this, the mandate of the Council of Europe and the scope of these instruments differ from EU law, which expressly excludes national security from the competence and jurisdiction of the Union. This means that, when it comes to international legal regulation of the activities of national security and intelligence agencies, the Council of Europe must take the lead role, if not globally then at least in Europe.

The need to secure the rule of law in relation to the activities of national security and intelligence agencies has become obvious in the light of the revelations of Edward Snowden about the global surveillance operations of the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) and their partners in the 5EYES group (Australia, Canada and New Zealand) in particular. These revelations have shown that these agencies are routinely tapping into the high-capacity fibre-optic cables that form the backbones of the Internet, and are also intercepting mobile and other communications worldwide on a massive scale, for instance by intercepting radio communications, using "back doors" they have installed in major communications systems and exploiting security weaknesses in such systems.

In European and international human rights law, national security is not a card that trumps all other considerations. Indeed, the very question of what legitimately can be said to be covered by the concept of "national security" is justiciable: it should be up to the courts to determine, in the light of international human rights law, what is – and what is not – legitimately covered by the term. Useful guidance on this is provided in the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information,* drafted by the NGO Article 19 but endorsed by various international forums including the UN Special Rapporteur on Freedom of Opinion and Expression. These principles make clear that states can only invoke national security as a reason to interfere with human rights in relation to matters that threaten

the very fabric and basic institutions of the nation. Sometimes, terrorism can reach this level, but in most cases it is a phenomenon that should be dealt with by law enforcement rather than within a national security paradigm. This also applies to actions of states that relate to the Internet and e-communications.

There is a lack of clear treaty rules governing the actions of national security and intelligence agencies, and the basis on which they operate and exchange data. In many countries, there are few clear, published laws regulating the work of these agencies. In some, there are no published rules at all. Until the rules are known under which these agencies and services operate – domestically, extraterritorially or in co-operation with each other – their activities cannot be said to be in accordance with the rule of law. Another matter of serious concern is the manifest ineffectiveness of many supervisory systems.

In other words, in relation to national security, there is as yet no real cornerstone to uphold the rule of law – although there are at least basic principles that could form the foundation of such an essential part of the universal human rights edifice.

Given the increased partnerships between law enforcement and intelligence and security agencies, this negation of the rule of law threatens to spread from the latter to the policemen and prosecutors. The absence of clear legal frameworks in this regard, domestically and internationally, is a further threat to the rule of law on the Internet and in the global digital environment.

The Commissioner's recommendations

Taking into account the findings and conclusions of this issue paper, the Commissioner makes the following recommendations, with the aim of improving respect for the rule of law on the Internet and the wider digital environment.

I. On the universality of human rights, and their equal application online and offline

1. The basic requirements of the rule of law apply, and should be made to apply in practice, equally online and offline. This means in particular that:

- the European Convention on Human Rights (ECHR) and all Council of Europe data-protection rules apply to all personal data-processing activities by all agencies of all Council of Europe member states, including the member states' national security and intelligence agencies;
- rule of law obligations, including those flowing from Articles 8 (right to respect for private and family life) and 10 (freedom of expression) of the ECHR, may not be circumvented through ad hoc arrangements with private actors who control the Internet and the wider digital environment;
- Council of Europe member states should strive to ensure that non-European states similarly comply with their international human rights obligations in anything they do that affects individuals using the Internet or otherwise active in the wider digital environment; and
- no states (and none of their agencies, including their law enforcement and national security and intelligence agencies), European or otherwise, should access data stored in another country – or passing through the Internet and e-communications "backbone" cables running between countries – without the express consent of the other country or countries involved, unless there is a clear, explicit and sufficiently circumscribed legal basis in international law for such access and provided that such access is fully compatible with international data protection and other human rights standards.

II. On data protection

2. Member states which have not yet done so should ratify the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108). This convention is also open to non-member states and, if adopted widely, can become the most important cornerstone of the rule of law on the Internet and in the wider digital environment.

3. Member states which have already ratified this convention should ensure that it is fully implemented at the national level.

4. The review of Convention No. 108, currently under way, should not lead to any lowering of European or global data-protection standards. On the contrary, it should lead to a clarification and better enforcement of the rules, especially in relation to the Internet and the wider digital world, and in relation to surveillance for national security and intelligence purposes.

5. In the context of the current reform of the EU data-protection rules, existing rules which might undermine the rule of law, such as those relating to consent, profiling or foreign law-enforcement access to personal data, should be clarified and brought into line with international human rights obligations, including those flowing from Convention No. 108, and the relevant Council of Europe recommendations and guidance.

6. Suspicionless mass retention of communications data is fundamentally contrary to the rule of law, incompatible with core data-protection principles and ineffective. Member states should not resort to it or impose compulsory retention of data by third parties.

III. On cybercrime

7. States parties to the Council of Europe Convention on Cybercrime must fully comply with their international human rights obligations in anything they do (or do not do) under the convention, be that in defining the relevant crimes (and elements, exceptions and defences relating to them), in any criminal investigations or prosecutions, or in relation to mutual legal assistance and extradition.

8. If any state party takes actions that affect individuals outside its territory, this does not exempt that party from its obligations under the Convention on Cybercrime or under international human rights treaties (in particular, the ECHR and the ICCPR); on the contrary, those obligations equally apply to such extraterritorial acts.

9. All states parties to the Convention on Cybercrime should also ratify and rigorously implement the Data Protection Convention, the European Extradition Convention and the European Convention on Mutual Assistance in Criminal Matters.

10. Member states, including their law-enforcement agencies, should implement Recommendation No. R (87) 15 of the Council of Europe Committee of Ministers regulating the use of personal data in the police sector, its Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, and its 2013 Declaration on

Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies.

11. Member states should ensure that their law-enforcement agencies do not obtain data from servers and infrastructure in another country under informal arrangements. Rather, they should use the mutual assistance arrangements, and the special arrangements for expedited data preservation, created by the Convention on Cybercrime. Law-enforcement agencies in one country should not rely on the fact that private entities – such as Internet service providers, social networks or mobile network operators – in other countries have obtained authority to disclose their customers' data under their general terms and conditions.

IV. On jurisdiction

12. There should be limits on the extraterritorial exercise of national jurisdiction in relation to transnational cybercrimes. These limits should take account of the effect of substantive limitations to the crimes, and of exceptions or defences, in the individual's home country (or the country where the acts were committed) in relation to jurisdiction claimed by other states that do not acknowledge such limitations, exceptions or defences.

13. In relation to the right to freedom of expression in particular, individuals and companies that make information available from their country of residence or establishment should in principle have to comply only with the laws of that country; while individuals who access or download materials from foreign websites (when they could and should know that the materials are illegal in their country of residence) should be expected to adhere to the laws of the latter country. Apart from content that is illegal under international law, states should only exercise jurisdiction over foreign digital materials in limited circumstances, notably when there is a clear and close nexus between the material and/or the disseminator and the country in question.

V. On human rights and private entities

14. Member states should stop relying on private companies that control the Internet and the wider digital environment to impose restrictions that are in violation of the state's human rights obligations. To that end, more guidance is needed on the circumstances in which actions or omissions of private companies that infringe human rights entail the responsibility of the state. This includes guidance on the level of state involvement in the infringement that is necessary for such responsibility to be engaged and on the obligations of the state to ensure that the general terms and conditions of private companies are not at variance with human rights standards. State responsibilities with regard to measures implemented by private parties for business reasons, without direct involvement of the state, also need to be examined.

15. Building on the UN "Guiding Principles on Business and Human Rights" (the Ruggie Principles), further guidance should be developed on the responsibilities of business enterprises in relation to their activities on (or affecting) the Internet or in

the wider digital environment, in particular to cover situations in which companies may be faced with, or may have put themselves in situations in which they may well face, demands from governments that may be in violation of international human rights law.

VI. On blocking and filtering

16. Member states should ensure that any restrictions on access to Internet content affecting users under their jurisdiction are based on a strict and predictable legal framework regulating the scope of any such restrictions and affording the guarantee of judicial oversight to prevent possible abuses. In addition, domestic courts must examine whether any blocking measure is necessary, effective and proportionate, and in particular whether it is targeted enough so as to impact only on the specific content that requires blocking.

17. Member states should not rely on or encourage private actors who control the Internet and the wider digital environment to carry out blocking outside a framework meeting the criteria described above.

VII. On national security activities

18. The ECHR and Convention No. 108 must be applied to all activities of the states that are party to these conventions, including states' national security and intelligence activities.

19. Specifically, in order to achieve respect for the rule of law on the Internet and in the wider digital environment:

- states should only be allowed to invoke national security as a reason to interfere with human rights in relation to matters that threaten the very fabric and basic institutions of the nation;
- states that want to impose interferences with fundamental rights on the basis of an alleged threat to national security must demonstrate that the threat cannot be met by means of ordinary criminal law, compatible with international standards relating to criminal law and procedure;
- the above also applies to actions of states that relate to the Internet and e-communications.

20. Member states should bring the activities of national security and intelligence agencies within an overarching legal framework. Until there is increased transparency on the rules under which these services operate – domestically, extraterritorially and/or in co-operation with each other – their activities cannot be assumed to be in accordance with the rule of law.

21. Member states should also ensure that effective democratic oversight over national security services is in place. For effective democratic oversight, a culture of respect for human rights and the rule of law should be promoted, in particular among security service officers.

We exercise a significant part of our human rights today using the Internet and the wider digital environment. But our human rights can also be breached using these very same means.

There is general agreement that human rights should be enjoyed online as they are offline. In practice, however, the actors who can ensure that we enjoy human rights are not exactly the same in the two environments. In particular, the disproportionate influence and control that certain states and certain private companies exercise on the Internet and its physical infrastructure at the global level, are two essential elements of this difference.

This issue paper looks at how the rule of law can be maintained in an environment characterised by these specific governance issues, focusing on some policy areas of particular human rights relevance: freedom of expression, data protection and privacy, cybercrime and national security. It suggests possible ways forward to ensure that we can trust the rule of law to apply to our online activities.

www.commissioner.coe.int

PREMS 176214 ENG

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE