Global Network Initiative

# Digital Freedoms in International Law

## Practical Steps to Protect Human Rights Online

*A report by Ian Brown & Douwe Korff*

www.globalnetworkinitiative.org

# About this Report

This report was commissioned by the Global Network Initiative (GNI) and was made possible by a grant from the Open Society Foundations. It is an academic work designed to pose questions and bring others into a dialogue. It attempts to tackle some of the most difficult questions around protecting rights to freedom of expression and privacy in the Information and Communications Technology (ICT) sector. We view this report as the beginning, rather than the end of a conversation, and we welcome feedback.

The report was written by Ian Brown and Douwe Korff and is based on extensive interviews with government, civil society and corporate actors involved in these matters, and draws on their practical experiences. We held three workshops, in London, Washington DC and New Delhi, with key stakeholders from all of these groups. Thanks to Eric King of Privacy International for providing the content for the Technology Exports to the Middle East map.

Please direct comments or questions to info@globalnetworkinitiative.org.

**Dr. Ian Brown** is Associate Director of Oxford University's Cyber Security Centre. He has led numerous EU and UK-funded research projects on privacy and information security, including a comparative study for the European Commission on the current revision of the Data Protection Directive, and co-authored with Douwe Korff a 2011 report on "Social Media and Human Rights" for the Council of Europe Commissioner for Human Rights. Dr Brown has consulted for the US Department of Homeland Security, JP Morgan, Credit Suisse, Allianz, McAfee, BT, the BBC, the Cabinet Office, Ofcom and the National Audit Office. He is a member of the UK Information Commissioner's Technology Reference Panel.

**Professor Douwe Korff** is a Dutch comparative and international lawyer. He is both a general human rights lawyer and a specialist in data protection. Following academic research at the European University Institute and at the Max Planck Institutes for comparative and international criminal- and public law, he taught at the University of Maastricht in the Netherlands and at the University of Essex in the UK. He is currently Professor of International Law at London Metropolitan University and visiting professor at the Universities of Zagreb and Rijeka in Croatia. He has carried out extensive work on data protection for the European Commission, the UK Information Commissioner, and industry, often with Ian Brown.

### Disclaimer

The views expressed in this publication are those of its authors.

### About GNI

GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics, who have created a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector. GNI provides resources for ICT companies to help them address difficult issues related to freedom of expression and privacy that they may face anywhere in the world. GNI has created a framework of principles and a confidential, collaborative approach to working through challenges of corporate responsibility in the ICT sector. Learn more at: http://www.globalnetworkinitiative.org

# Executive summary

With around 2.3 billion users, the Internet has become part of the daily lives of a significant percentage of the global population, including for political debate and activism. While states are responsible for protecting human rights online under international law, companies responsible for Internet infrastructure, products and services can play an important supporting role. Companies also have a legal and corporate social responsibility to support legitimate law enforcement agency actions to reduce online criminal activity such as fraud, child exploitation and terrorism. They sometimes face ethical and moral dilemmas when such actions may facilitate violations of human rights.

In this report we suggest practical measures that governments, corporations and other stakeholders can take to protect freedom of expression, privacy, and related rights in globally networked digital technologies. These are built on a detailed analysis of international law, three workshops in London, Washington DC and Delhi, and extensive interviews with government, civil society and corporate actors.

# International law requirements

The International Covenant on Civil and Political Rights and related regional treaties protect online freedom of expression and privacy. States must ensure these protections for anyone within their effective power and control. In many instances they must also protect individuals against violations of their rights by other individuals or companies.

Restrictions on rights must be based on published, clear, specific legal rules; serve a legitimate aim in a democratic society; be "necessary" and "proportionate" to that aim; not involve discrimination; not confer excessive discretion on the relevant authorities; and be subject to effective safeguards and remedies.

In "time of war or other public emergency threatening the life of the nation", states can impose restrictions "to the extent strictly required by the exigencies of the situation", although not discriminate solely on racial or gender grounds. Emergency legislation should be passed in ordinary times when it can be fully debated and understood.

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has recommended that anti-terrorism measures are overseen by the judiciary "so that they remain lawful, proportionate and effective, in order to ensure that the government is ultimately held responsible and accountable." This approach should be used with other breaches of public order that fall short of armed conflict.

Government agencies are increasingly asking Internet companies directly for customer data held outside their jurisdiction. When law enforcement or national security agencies in one country want to obtain access to evidence in another country, they generally have to go through "Mutual Legal Assistance Treaties" (MLATs) that protect the rights of all affected persons. MLATs are complex and can be cumbersome in practice. However, bypassing established MLAT processes constitutes an infringement of sovereignty.

## Emerging company standards

The UN Guiding Principles on Business and Human Rights provide a comprehensive framework in which companies can address their responsibility to respect human rights. Companies faced with state demands that violate human rights have a duty to minimise the extent of any such cooperation. They must assess in advance the human rights risks in countries where they operate, take measures to minimise these risks, and help the victims of any enforced cooperation.

The GNI Principles also stress the need for companies to be pro-active in minimizing the impact of government restrictions on the rights to freedom of expression and privacy of their users; the need to build the principles into companies' basic policies, procedures and processes; and the need for due diligence and risk assessments.

## Export controls and licensing

US and EU sanctions against repressive regimes such as Iran and Syria already include specific bans on the export of technologies and services that could aid in human rights violations. However, these will not prevent monitoring and censorship tools being acquired and built into the infrastructure of repressive regimes that are yet to reach this stage.

Many of these tools are "dual use", with legitimate network management and security purposes. Some are required for law enforcement purposes by democratic states. There are extensive international controls on the export of other "dual use" technologies with civil and military applications. However, many of the technologies we discuss can already be used to enable widespread repression, without that use being "military".

Technology companies have legitimate concerns that export controls limit access to potentially significant markets, and impose bureaucratic constraints on legitimate sales that may be ineffective against bad actors. A further danger is that controls block the provision of tools to democracy activists. This can happen through broad controls such as those applied by the US against Iran and Syria. But even when relaxed, the complexity of the controls and the harsh penalties for making a mistake still discourage many companies from allowing the use of their products by anyone in these countries.

Some software and telecommunications products require frequent updating by the vendor, or can be remotely disabled. Where such restrictions can be shown to be effective, the need for export controls on that equipment as a preventative measure is reduced, since usage controls can be put in place at any time.

## Recommendations

On the basis of our analyses and building on the UN Guiding Principles and GNI Principles and Implementation Guidelines, we propose the following possible steps that can be taken to prevent or mitigate human rights violations perpetrated or facilitated by the use of globally networked digital technologies.

### Companies

Companies should exchange information on legal systems and experiences in specific jurisdictions with other companies, governments and non-governmental organisations (NGOs). Before entering a market, companies should assess whether the domestic legal

systems and practices conform to international human rights and rule of law requirements. If authorities in the country are involved in human rights abuses, and if the technologies a company is considering selling there could contribute to such repression, it should carefully plan how it can make its technology available in a form that minimises the risk of abuse.

Companies should ensure they have a clear understanding of lawful procedures under which subscriber data can be requested, material blocked, and connections terminated. Where possible they should agree on specific points of contact for government requests, and mechanisms to check the authorisation of requests. Companies should share and collectively publish aggregate statistics about the use of these procedures, and challenge ambiguous demands in the higher courts.

Companies should use "Privacy by Design" principles to reduce the processing and storage of personal data no longer required for a legitimate business purpose, which could later be subject to compelled disclosure. In countries with deficient laws, this may include storing personal data outside the control of that jurisdiction. Companies' terms and conditions should specify that user data will only be provided to government agencies upon receipt of a legally binding request. Companies should insist that Mutual Legal Assistance (MLA) arrangements are the only appropriate means of cross-border data access.

If host country authorities demand *ad hoc* access to data in circumstances that suggest a potential violation of international human rights law, the company should challenge the demand before the courts of the host country, and resist attempts at access pending full judicial review of the demand. If the host country demands direct access to company data, through the insertion of opaque "black box" interception or access devices, the company should fundamentally consider its provision of the product to the country: such effectively unlimited and uncontrollable access is fundamentally contrary to basic principles of the rule of law, unless accompanied by a very strong control and oversight regime.

## Governments

States should be willing to engage in dispute resolution measures to resolve conflicts over human rights compliance in the use of products sold and supported by companies from their country.

States should insist that demands for access to data held on their territory should be made only through the applicable Mutual Legal Assistance arrangements, and that extraterritorial demands for access to data on a server in their jurisdiction would otherwise constitute a violation of sovereignty. They should consider backing up such action in domestic law, and in inter-governmental arrangements and treaties. They should also consider applying civil legal liability to companies that fail to perform due diligence checks or to take measures to prevent, mitigate or end abuse of products for the perpetration of large-scale or serious human rights violations.

States should consider including tools that have primary or significant potential uses for human rights violations in "dual use" export control regimes, requiring suppliers to undertake extensive due diligence on end-users before export to or support, maintenance or training for specific repressive regimes. The maintenance of a list of controlled items and targeted states would require frequent multi-stakeholder discussion between states, technology companies, and human rights groups and academics with expertise in the use of these tools for human rights violations.

Tools useful for political activism should be more clearly excluded from export controls and sanctions. At a minimum, broad general licences, allowing the export of software and support as well as information, are easier to understand and comply with than a requirement for individual licensing procedures. Information security tool controls could be immediately scrapped.

Meaningful statistics and information should be published to allow the public to see how, how often, and in what kind of circumstances blocking technologies are used, and how personal data and communications of private citizens are being shared between Internet intermediaries and governments.

## Inter-Governmental Organisations

Global and regional inter-governmental organisations (IGOs) should review MLA arrangements, to address the currently unresolved complex legal issues that arise under them. Such a review should also address the need to introduce speedy access to personal data under MLAs, subject to appropriate safeguards. Further research is needed into measures that can increase the responsiveness of MLA requests while protecting human rights and public policy objectives, and into conflict of laws issues that are currently arising.

IGOs should make clear that states may provide incentives to companies that act in accordance with these recommendations, and may impose disincentives on companies that act blatantly contrary to those recommendations. US and European calls for restrictions on Internet freedom of expression to be classified as barriers to trade should be given speedy consideration by the World Trade Organisation.

## Non-Governmental Organisations

Human rights NGOs can play an important role in educating companies about relevant international standards, in training company staff on dealing with human rights concerns in countries in which they operate, and in the conduct of human rights impact assessments.

NGOs should support efforts to create stronger international law frameworks for the protection of human rights in relation to the sale and support of human rights sensitive products by companies. They should develop and campaign for stronger human rights law standards on how governments demand content removal /blocking and sharing of user data, given that specific governmental actions often have global implications.

NGOs should do more to raise public awareness about the roles and responsibilities of ICT companies in protecting people against human rights abuses, and how to make informed decisions as consumers and users when choosing between ICT products and services. They can also do more to educate people about how to protect themselves against human rights abuses when using ICTs in their daily lives as well as during political crises.

## Investors

Socially responsible investors should expect companies to commit to appropriate human rights standards that meet three essential tests. Standards should have operational utility, addressing issues in a concrete, practical way. They should be developed and implemented in a multi-stakeholder process with NGOs, academic experts and other stakeholders. And they should require accountability through public reporting, even if certain details are held back in some extremely sensitive situations