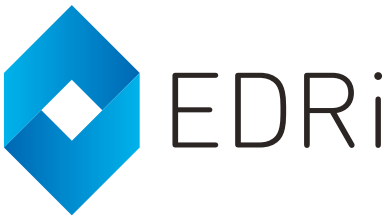

PROTECTING DIGITAL FREEDOM

Human Rights and privatised law enforcement

Abandoning rights - abandoning democracy - abandoning law

25 February 2014

European Digital Rights 20 Rue Belliard, 1040 Brussels www https://edri.org twitter @edri_org tel +32 (0) 2 274 25 70

"How can there be areas of lawlessness in areas of our society? How can one simultaneously claim that the economy is regulated but the internet is not? How can we accept that the rules that apply to society as a whole are not binding on the internet?"

- Nicolas Sarkozy

contents

OPEN SOCIETY FOUNDATIONS

Supported in part by a grant from the Open Society Foundations

With financial support from the Eu's Fundamental Rights and citizenship Programme.

Design by:

Marc Smits

info@smithwilson.eu

Introduction

The interplay between traditional principles of human rights in the offline world and the new threats and opportunities for human rights in the digital world is often counter-intuitive. We know that the internet is correctly celebrated for its success in expanding the enjoyment of fundamental freedoms online and offline. However, we are increasingly seeing digital technologies threatening those same freedoms, often in ways that are frequently unnoticed and unreported. We see these threats in overt restrictions such as the use of mobile phone location data to identify people involved in demonstrations, along with less obvious restrictions such as secret corporate and state surveillance and personality profiling.

A drive from governments, most influentially those in the United States and Europe, for private companies to impose arbitrary restrictions in order to achieve various political or public policy goals is leading to some basic human rights principles being undermined. These decisions have a global effect, due both to the normative effect of such policies and the fact that many online companies operate globally.

At the end of the 1990s, the US and EU focused their attention on ensuring an open online environment. They did this primarily by actively removing incentives for online intermediaries to interfere with, monitor or police online content (such as by limiting liability for online infringements in the US Digital Millennium Copyright Act (DMCA) and the EU's E-Commerce Directive). Fifteen or so years later, this approach is being replaced with measures to encourage and/or coerce intermediaries not just to police online content, but even to impose sanctions, such as the unilateral suspension of services.

The imposition of sanctions by intermediaries, outside the rule of law, undermines the presumption of innocence, the right to due process of law and, depending on the policing methods used, the right to privacy and freedom of communication. As a result, the internet increasingly seems more like a weapon that undermines rights rather than a tool to nurture them. As most of the global online companies are American, there is an obvious, although dangerous, temptation for the US administration to pursue a strategy

of having US law or public policy priorities imposed globally and "voluntarily" by US companies. The strategic motivations of the EU in supporting this approach are somewhat more difficult to explain.

This booklet will focus on a small number of key examples of how such policies are undermining democratic values and principles enshrined in human rights law. It will look primarily at measures that have an international effect. It will not address the numerous examples of national laws that push online regulation into the hands of online intermediaries. The most important of these are detailed in the report of the UN Special Rapporteur on freedom of expression and opinion[01]. While such local laws clearly are profoundly objectionable and undermine important civil, political and fundamental human rights, they are outside the scope of this analysis.

We start by looking at the positive democratic use of the internet for campaigning – looking at the fight against SOPA[02] and ACTA[03]. SOPA is the Stop Online Piracy Act, an American copyright protection proposal. ACTA is the Anti-Counterfeiting Trade Agreement, a plurilateral agreement on minimum standards for enforcement of so-called "intellectual property" rights. These campaigns provide a good example of the positive side of the internet and its facilitation of the enjoyment of human rights. Massive online campaigning led to real-world demonstrations involving hundreds of thousands of individuals and, ultimately, the prevailing of the popular will. We will then go on to look at how this democratic will was largely ignored and overturned by "voluntary" arrangements between policy-makers and the internet industry.

Finally, this document looks at some examples of how international bodies have developed policies on internet regulation which support, encourage and facilitate breaches of principles such as the right to due process, presumption of innocence, freedom of communication and assembly and privacy. The central focus of this paper will be the tension between the well-established principle that restrictions on civil and human rights must be based on law (vis. Articles 8 and 10 of the European Convention on Human Rights, Article 52 of the European Charter of Fundamental Rights, Article 19 of the International Convention on Civil and Political Rights, Article 11 of the African Charter of Human and Peoples' Rights, Article 16 of the American Convention on Human Rights, etc.) and lawless restrictions of these rights by private companies in the online space. Only states are bound by international law – so privatising the enforcement of such restrictions circumvents both international law and, as in the case of the United States, for example, domestic constitutions.

SOPA & ACTA

Democracy at work - democracy circumvented

SOPA (Stop Online Piracy Act) was a wide-ranging measure aimed at the protection of copyright, trademark and other rights and was initially introduced in 2011.[04] ACTA (Anti-Counterfeiting Trade Agreement) is a plurilateral "trade agreement", which aimed at establishing a "gold standard" for high levels of protection of copyright, trademark and other rights.[05] It was drafted over the course of several meetings, starting officially in 2008, with the final draft being completed in 2010.

The proposals for the "Stop Online Piracy Act" (SOPA) and the plurilateral "Anti-Counterfeiting Trade Agreement" (ACTA), the campaigns against them and subsequent policy developments, provide a good example of the positive change in the nature of online freedoms and the associated human rights. The campaigns demonstrate how the internet creates a new space for democratic discourse, campaigning, communication and can bring about real political change.

The campaigns

The campaigns against SOPA and ACTA shared information and awareness of the threats that they posed human rights and demonstrate how the internet creates new possibilities for exercising existing rights.

Detailed critiques of SOPA and ACTA were distributed online, via popular news websites such as Techdirt[06] and non-governmental organisations like the Electronic Frontier Foundation[07] and European Digital Rights[08]. Avaaz (a popular petition website) gathered over three million signatures in opposition to SOPA and Protect IP[09] and over two million signatures in opposition to ACTA[10]. Major international information-sharing and collaborative websites such as Reddit and Wikipedia carried out "blackouts" of their websites in protest and well over a hundred thousand people[11] braved freezing temperatures to demonstrate across Europe in early 2012.

The result of this explosion of democratic participation was that SOPA in the US Congress and ACTA in the European Parliament became politically "toxic". As a consequence, discussions on SOPA ended without agreement, while ACTA was overwhelmingly rejected by the European Parliament.

What made SOPA and ACTA different?

SOPA

In the field of copyright protection, citizens across the globe have long since become used to extreme proposals being made – and even adopted – with the direct or indirect aim of protecting copyright, to the detriment of freedom of communication, right to a fair trial, presumption of innocence and the right to privacy. For example, the EU's "Intellectual Property Rights Enforcement Directive"[12] (known as IPRED) provides easy access to internet users' personal data for copyright owners. This "right" has been used by law firms, in Germany and the UK in particular, to harvest IP addresses in peer-to-peer networks, in order to obtain data about individuals (at one stage 300,000 sets of personal data were being obtained per month in Germany[13]) from internet access providers. This information is then used to give the end-user "an offer they can't refuse" – either pay a comparatively low amount of money to be left in peace or seek to defend themselves in court, where the cost of losing would be far greater. This approach undermines freedom of communication, privacy and the presumption of innocence. The most famous proponent of this activity in the UK is the now defunct law firm ACS: Law, whose only registered solicitor was ultimately suspended by the Solicitors' Regulatory Authority for conduct unbefitting a solicitor, but only after over a million pounds was collected from individuals, in a process using methods described in one House of Lords debate as "blackmail". [14] [15]

Despite a plethora of such measures being proposed and enacted at international and national levels, reactions have sometimes been significant but have never been at the level of the opposition to SOPA/ACTA. It appears that the reason for this was that other measures did not touch the core functionality of the internet. While being negative in a human rights context, previous measures did not damage the internet itself. As a result, measures such as IPRED and the internet disconnection strategy in the HADOPI (a French law which created the sanction of disconnection of citizens from the internet) law were able to make it through the democratic decision-making process, even if they subsequently ran into difficulties.[16] As long as the core functionality of the internet – its openness – was untouched, the danger of such measures was perceived as limited.

However, SOPA was different from anything that had gone before. It took a big leap in severity, away from a rule-of-law and due-process based approach in dealing with alleged online infringements. For example, in section 104, it proposed that US companies would get full immunity for punitive actions against any online service, anywhere in the world, on condition that the action was based upon "reasonable belief," not of criminal behaviour but of "theft of U.S. property". It would not even be required for any specific law to be breached or for there to be an allegation of a law being breached. Law is not even mentioned in this attempt to make privatised law enforcement easier. Instead,

SOPA SEC. 104. IMMUNITY FOR TAKING VOLUNTARY ACTION AGAINST SITES DEDICATED TO THEFT OF U.S. PROPERTY.

"No cause of action shall lie in any Federal or State court or administrative agency against, no person may rely in any claim or cause of action against, and no liability for damages to any person shall be granted against, ***a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar*** for taking any action described in section 102(c)(2), section 103(d)(2), or section 103(b) with respect to an Internet site, or otherwise voluntarily blocking access to or ending financial affiliation with an Internet site, in the reasonable belief that (emphasis added)--

(1) the Internet site is a foreign infringing site or is an Internet site dedicated to theft of U.S. property; and

(2) the action is consistent with the entity's terms of service or other contractual rights."

there was a requirement for the activity to be included in the terms of service of the company undertaking the punitive action.

Any online activity relies on a whole range of online companies to function. An online shop in Costa Rica may accept payment via Paypal, an activist in Guatamala will rely on search engines like Microsoft's Bing to be discovered by interested citizens, a newspaper in Japan may fund itself using Google's advertising network. SOPA may be a US proposal, but its intended impact is unquestionably global.

This proposal neatly skirts around direct breach of US constitutional safeguards for protection of free speech (first amendment) and right to a fair trial (sixth amendment) by simply opening the door for private companies (who are not subject to the constitution) to impose the restrictions. By covering "domain name registries," even the Internet Corporation for Assigned Names and Numbers (ICANN) (the body that manages the "single authoritative root" for the global domain name system[17]) could be covered and liable to coercion to take punitive actions against any domain name user or registry, anywhere in the world (although it was not intended to include ICANN in the initial implementation of the Act).

It is remarkable to note that, at the same time as the US State Department website proudly proclaims that it "works to advance internet freedom as an aspect of the universal rights of freedom of expression and the free flow of information,"[18] the US proposal was that private companies could act as global police with impunity, to destroy online activity if they believed that US interests were being undermined. No court, no law, no accusation. Just "reasonable belief".

For a non-US online service, just one of these companies having a "reasonable belief" that they were "stealing" US property would be enough to remove their online presence or their income. Self-censorship and hoping that the system would not be abused – deliberately or accidentally - would be the only available tools for entities seeking to remain online.

The next question to ask is how likely it would be that such a system could be abused. The US, for example, already has a procedure for the "notice and takedown" of online content under the Digital Millenium Copyright Act (DMCA).[19] Under the DMCA, content can be removed from the internet automatically if a set of criteria are respected by the complainant, without judicial intervention.[20] According to a study carried out in 2006 by Jennifer Urban and Laura Quilter, 57% of notices sent to Google were sent by businesses that were apparently targeting competitors. The study found as many as 30% of the takedown requests presented "an obvious question for a court" (i.e. that were inappropriate for such a non-judicial framework).[21] The risks for human rights globally from SOPA are therefore very clear.

The dangers of expanding such a system to virtually every type of service provider in the chain of distribution for availability and legal certainty of online services are obvious. It would create an environment where intermediaries would only be liable for failure to act, but not for disproportionate, mistaken or unnecessary measures. As a result of the US DMCA, websites around the world are already being de-indexed by Google. The company often does not inform them that this has happened and, if it does, only does so in English. According to the Urban and Quilter study, 30% of DMCA takedown and de-indexing requests received by Google related to sites outside the USA.[22] Where is the democracy and legal certainty in a system where your revenue and the accessibility of your website can be seriously diminished or destroyed outside of a judicial framework, as a result of a foreign law,

Article 27.3, ACTA

"Each Party shall endeavour to promote cooperative efforts within the business community to effectively address trademark and copyright or related rights infringement while preserving legitimate competition and, consistent with that Party's law, preserving fundamental principles such as freedom of expression, fair process, and privacy."

" SOPA was different from anything that had gone before. It took a big leap in severity, away from rule-of-law and due process-based approach in dealing with online infringements. "

OECD Communiqué on Principles for Internet Policy-Making

"New and complementary approaches balanced to ensure effective protection of intellectual property should also be encouraged where necessary, and should also ensure protection of legitimate competition and ***fundamental principles*** *such as freedom of expression, access to lawful content and Internet services and technologies,* ***fair process****, and privacy. Sound Internet policy should encompass norms of responsibility that enable private sector voluntary co-operation for the protection of intellectual property. Appropriate measures include lawful steps to address and deter infringement, and accord full respect to user and stakeholder rights and* ***fair process***[25]*." [Emphasis added].*

based on a decision by a foreign company and where redress could only occur in a foreign country through foreign courts? Where is the principle of equality before the law in a situation where one would have to go to a foreign country, spend money on foreign lawyers in foreign courts?

ACTA

Because it is an international agreement, ACTA was a lot more subtle, even though the intention was obviously identical – "encouragement" for private companies to reach ad hoc agreements for ad hoc enforcement of copyright law.

Even more disturbing in a global context, Article 27.3, ACTA sought to establish a precedent in international law that due process of law – as required by every relevant international instrument[23] – would no longer be the norm. The reference to the "fundamental principle" of "fair process" is very significant. There is, quite simply, no fundamental principle of fair process in international law and it is difficult to imagine that the senior negotiators who drafted the text were unaware of this fact. The only available explanations for this wording being chosen is that it was a transparent attempt to either mislead people reading the text from a political perspective (it sounds like due process and fair trial, it sounds like a safeguard) or to give legal readers no option other than to interpret the text as a deliberate choice to downgrade (in an international legal instrument that was overtly intended to be normative), individuals' rights to due process of law.

ACTA's "fair process" appears to have its roots in the OECD "Communiqué on Principles for Internet Policy-Making", which was published in June 2011.[24] That text was quite explicit in its efforts to demand privatised enforcement by internet companies and the abandonment of due process of law. The identical wording ("fundamental principles" and "fair process") would suggest an impressive level of coordination between distinct initiatives (see box above).

Ultimately, a more balanced text, with less emphasis on privatised enforcement was published in December 2012, mainly as a result of energetic opposition to the June text by the Civil Society Information Society Advisory Council at the OECD.[26]

What happened after the democratic process killed the proposals?

When "voluntary measures" make democratic decisions irrelevant.

Opposition to, among other things, the privatised enforcement measures in SOPA and ACTA led to both of the proposals being dropped – SOPA was suspended while ACTA was rejected by a large majority in the European Parliament although is still, in theory, open for signature and ratification by countries outside the EU. So far (as of December 2013), only Japan has ratified the instrument. The internet's value for democratic discourse, its ability to facilitate the mobilisation of citizens in defence of their rights had triumphed over the proposals for the undermining of core democratic values of due process of law, freedom of communication, the right to privacy and freedom of association.

Through selective editing or editorial blindness the White House was reported in the press[27] as coming out against this approach as well when it issued a statement that it would "not support legislation that reduces freedom of expression, increases cybersecurity risk or undermines the dynamic, innovative global Internet."[28] In fact, the statement from which this quotation came also gave unequivocal support for the privatised enforcement measures, stating that "[w]e expect and encourage all private parties, including both content creators and internet platform providers working together, to adopt voluntary measures and best practices to reduce online piracy."[29] To put it another way – the democratic process prevented us from getting what we wanted, so now we will try by other means. As a statement of intent to circumvent the failure to adopt the measures through democratic means, the message could hardly have been clearer.

The next section of this paper we will look at developments with regard to privatised enforcement measures being taken by the types of companies listed by Section 104 of SOPA. It will specifically look at each type of intermediary mentioned in SOPA Section 104 ("service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar") to assess what happened after voluntary, ad hoc enforcement by these companies was not given democratic approval.

"Service provider"

Assuming that "service provider" means "internet access provider", it is noteworthy that a private surveillance and warning system was launched in the US only thirteen months after SOPA was suspended – the so-called "six strikes" agreement. Major internet access providers including AT&T, Cablevision, Comcast, Time Warner Cable and Verizon are participating in the system. The agreement was reached (but the policies not yet put in place) in July 2011. In short, the democratic rejection of SOPA had little impact on the original plans.

Under the system, peer-to-peer networks are analysed, IP addresses are harvested and "warnings" are sent to the users that the service providers believe were using the IP address at the time. The user is then contacted with warnings that they have been identified as committing illegal acts and provided with dubious information about the alleged risks that this activity generates. The punishments that follow several warnings vary service provider to service provider, but include bandwidth limitations ("throttling") and blocking of certain sites – all on the basis of "evidence" which is far from reliable.[30]

"Payment network provider"

In June 2011, the major credit card companies – American Express, Discover, MasterCard and Visa, as well as payment service PayPal – reached an agreement with the White House on blocking payments to (generally non-US) sites that have been accused of breaching US copyright. It is very difficult to find exact details of what was agreed in this deal, but some of the vigilante arbitrary actions taken in recent years by the payment providers show the dangers of this model for human rights. For example, the payment service providers were faced with a public relations challenge by the Wikileaks scandal. Even though Wikileaks had never (and still has never) been accused of breaking any law, the US Vice President, for example, publicly accused the organisation of being a "high-tech terrorist" organisation.[31] Subsequently, Visa, MasterCard and Paypal decided that it was in their best interests to unilaterally block payments to Wikileaks. There was no due process of law and no presumption of innocence. There was just swift, unilateral and arbitrary punishment, based on the flexibilities provided by the companies' terms of service. As a result, no individual, regardless of where they were in the world could use the most commonly used electronic payment services in order to make a donation to Wikileaks. The action was described in The Guardian as one of the "most sinister developments in recent years, and perhaps the most extreme example in a western democracy of extrajudicial actions aimed at stifling free speech."[32]

Even more arbitrary is the blocking of payments to providers of virtual private networks (VPNs) in Sweden. The online payment provider Payson has been told that such services are no longer allowed to receive payments through Visa and MasterCard.[33] Far from being illegal, the use of VPNs is actively promoted as a privacy enhancing technology by governments and European institutions. On a European Union level, the European Commission actively invests in the promotion of such technology. Even though the providers of VPN services are not accused of breaking any laws, even though the technologies are entirely legal, their use by private individuals is becoming increasingly difficult, due to voluntary law

enforcement measures by companies with power but no responsibility, imposed arbitrarily and without justification.

In another example, Paypal decided to impose censorship policies on one of its own clients. It told the ebook distributor Smashwords that it was not allowed to sell books that breached content guidelines set by Paypal – banning books on Smashwords that were legally available on, for example, Amazon.com. After a significant amount of public pressure, Paypal eventually backed down.[34] Whether a similar service outside the United States with a small customer base would be able to achieve the same result seems highly unlikely. Privacy, right to a fair trial, democracy, presumption of innocence can all be brushed aside, despite the constitutional protections for free speech in the USA.

"Internet advertising service, advertiser"

In July 2013, an agreement was reached between the White House and major online advertising companies including AOL, Google, Microsoft and Yahoo, whereby those companies promised to take voluntary punitive actions against online resources globally suspected of illegal activities, with a view to undermining their financial viability.

The agreement that was reached with the advertising companies not only implements the spirit of SOPA, but, in some cases, to implement the letter of the proposed law as well. For example, the penultimate paragraph of the complaint process of the Guidelines, (i.e. the procedure agreed by the advertising services) establishes that these "best practices" "should not, and cannot, be used in any way as the basis for any legal liability", which is exactly wording as in section 104 of SOPA.[35]

Ironically, at the same time as helping to broker this measure, whereby advertisers would take unilateral punitive action outside a legal framework, the White House IPR Enforcement "Csar", Victoria Espinel referred to the US administration's "broader Internet policy principles emphasizing privacy, free speech, competition, and due process" (emphasis added) in her 2013 Joint Strategic Plan.[36] Where is the free speech and due process in a system where a foreign advertising network can unilaterally remove your revenue and, potentially, put you out of business?

"Internet search engine"

Anyone who puts a website online needs potential visitors to be able to find their site. One of the most common ways that people find relevant websites is through search engines. As a result, if a search engine decides that users will should no longer be able to "find" your website, this will have a major impact on your human right to impart information and your potential visitors' right to receive that information. Google, the global leader in the search engine market had already implemented, prior to the drafting of SOPA, the non-judicial "notice and takedown" procedure in the DMCA on a global level. Interestingly, whereas Google will de-index sites for child protection or political reasons on a national level, based on national demands and laws, it only de-indexes globally on the basis of the US DMCA, for copyright enforcement purposes. This creates a dual online legal regime – anybody outside the USA needs to comply with their local laws and also

needs to comply with US law in order to avoid unilateral actions, based on foreign legislation, such as being de-indexed by Google.

"Domain name registry, or domain name registrar"

Even before SOPA was proposed, major US domain name registrars, such as GoDaddy.com, were deleting entire web domains without judicial order. GoDaddy.com confirmed this practice in testimony in the US Congress[37] The company explained that it does not just remove domains as a result of legal orders (i.e. in compliance with due process of law), but also on the basis of simple notifications from prosecutors. In just one example of its ad hoc actions against its own customers, the removal of jotform.com (which was reversed several days later) led to the two million web forms generated and hosted by the site breaking down – even though none of the 700,000 users of the site had even been (or has subsequently been) accused of anything and presumably only one had even been suspected of illicit behaviour.[38]

Two months after the suspension of SOPA, the single global (California-registered) authority that licences domain name registries, ICANN, published its "Thought Paper on Domain Seizures"[39] – which is essentially a "how-to" guide for registries (such as .com or .ie) to remove domains. The "thought paper" does not mention issues of due process or the vast and very well documented dangers of collateral damage that domain name revocation can produce – suspension of the mooo.com domain name, for example, led to approximately 84,000 perfectly legal websites being replaced with a notice that they were involved in child abuse offences.[40]

What does this mean for free speech globally – especially for individuals that have no link whatsoever with the United States? In one example of arbitrary and unpredictable policing, a British individual called Steve Marshall was living in Spain running a company providing tourism services to Cuba, aiming mainly at the Italian and French market. He had bought his domain names (such as www.cuba-hemingway.com and www.bonjourcuba.com) from an online company called eNom. Subsequently, the US Treasury placed Mr Marshall's company on a "watch list". eNom checked the Treasury list to see if any of its customers were on the list and, on discovering that Mr Marshall's services had been added to the list, unilaterally deleted all his domains. As the New York Times put it... "one wave of the watch list and free speech disappears".[41]

SOPA – rejected democratically, implemented voluntarily?

As we can see from the examples listed above, pretty much every type of service provider mentioned in SOPA Section 104 has now started undertaking the punitive measures envisaged, outside the rule of law, in the absence of due process of law, in the absence of assumption of innocence, circumventing constitutional protections and in the complete absence of any safeguards for human rights – not to protect society against terrorists or child abusers, but to protect the copyright of usually large and usually American corporations.

ACTA and "fair process"

After ACTA was killed by an overwhelming vote in the EU Parliament and after the OECD internet principles document was cleansed of the worst elements of its privatised enforcement drive,[42] there was reason for hope that the push for the illusion of corporate governance of our free speech rights through ill-defined "fair process" procedures would be killed as well. However, such assumptions have proven premature.

The Internet & Jurisdiction Project[43] has been seeking to address many of the jurisdictional problems that arise online. The project's 2012 Annual Report stresses the importance of due process, a point that is mentioned on pretty much every page of that document. In July 2013, the organisation organised a workshop in Paris, where the problem was suddenly phrased very differently. The meeting summary issued prior to the event, which was entitled "what cross-border frameworks to ensure interoperability and fair process" (emphasis added), described the problem at hand as follows:

"Tension is growing in the absence of appropriate frameworks to deal with the diversity of procedures put in place by states to enforce local laws, and cross-border platforms to implement their Terms of Service."

Instead of the previous reflections on the need for due process of law, the question now was "to explore how to multi-stakeholder frameworks can be developed to handle seizures, takedowns and Law Enforcement Agencies' access to private data." Instead of law, the question was how private companies' terms of service could be implemented. In January 2014, the Internet and Jurisdiction website was cleansed of its references to "fair process". However, the project leaders confirmed to EDRi that the change of vocabulary does not reflect any change of policy.

Seizures and takedowns are restrictions of freedom of communication, which can only be restricted on the basis of law, according inter alia to the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). Similarly, law enforcement agencies' access to private data is a restriction on the right to privacy and also must be based on law. It is difficult to find any other interpretation of the approach of the Internet and Jurisdiction Project, than that this is an effort to promote efforts to privatise the rule of law and replace laws with terms of service, in the same spirit as SOPA and ACTA. Coincidentally or otherwise, the Disney Corporation, one of SOPA's most energetic supporters, is one of the main funders of the Internet & Jurisdiction Project.

Digital decay of human rights law

New technologies used to undermine law and restrict rights

As mentioned above, it is an established principle of international law that restrictions on core democratic freedoms such as freedom of communication, speech and association, as well as the right to privacy, have to be based on law that is enacted in domestic legislation (or, at the very least, a procedure which is as predictable as a law). It is remarkable that the digital revolution, which has done so much to create new opportunities to exercise these freedoms, appears to have made policy-makers forget this previously unquestioned principle. At every level, we see examples of egregious breaches of this core safeguard, with an ever-growing avalanche of suggestions and demands to replace democratically agreed laws and predictable legal frameworks with ad hoc restrictions imposed by private companies, normally through their terms of service.

UN requesting breaches of UN law?

Access to personal data

The United Nations agency, the "United Nations Office on Drugs and Crime", published a report in October 2012 on "Use of the Internet for Terrorist Purposes."[44] This UN report also calls for the establishment of "informal relationships or understandings with ISPs (both domestic and foreign) that might hold data relevant for law enforcement purposes about procedures for making such data available for law enforcement investigations."[45] (emphasis added)

It hardly takes much legal expertise to see the obvious contradiction between this proposal and Article 17.1 of the United Nations International Covenant on Civil and Political Rights, which states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence." One is left with the impression that the UN report is nothing less

than a naked, unjustified and indefensible assault on decades-old, universally agreed human rights principles. Ironically, just two weeks before the report was published, UN Secretary General Ban Ki-Moon said "Where governments fail to live up to their obligations under international law, we have to remind them to do so." [46]

The report also comments positively on an "innovative tool" in the United Kingdom for authorities dealing with terrorism to issue takedown notices to have websites removed by internet companies.[47] The "innovative tool" is an agreement whereby online content is removed by internet companies on the basis of simple requests from (unspecified) relevant authorities. Unilateral, ad hoc non-judicial control of online speech apparently being too cumbersome for internet companies to administer, the report explains that the "authorities" do not, in practice, need to use their powers. Instead, they were generally able to negotiate takedown of questionable content, on the basis that it is contrary to the terms of service of the internet company in question. The fact that this practice is in quite obvious breach of Article 19.3 of the ICCPR (restrictions on freedom of communication must be "provided by law and necessary") appears to be of little concern to the United Nations agency that published the report.

This very lax attitude to the protection of personal data and privacy appears to be shared by the European Commission. In 2011, it produced an evaluation report[48] on the implementation of the Data Retention Directive[49]. That report explained that there are few cross-border accesses to data retained under the Directive because law enforcement authorities "prefer to request data from domestic operators, who may have stored the relevant data, rather than launching mutual legal assistance procedure which may be time consuming without any guarantee that access to data will be granted". In other words, EU member states are asking international telecommunications companies to provide access to data from other EU member states without going through agreed legal channels. The European Commission explicitly recognises that the circumstances of some these attempts to access personal data are such that obtaining the information may not be possible via legal means.

Even though the Commission launched – and threatened to launch – legal action against several EU Member States for failing to transpose the Directive into national law, it has taken no steps whatsoever to bring an end to this illegal breach of the fundamental rights of European citizens.[50] The Commissioner responsible, Cecilia Malmström, took a personal oath, together with all other Commissioners, on 3 May 2010 to "respect the Treaties and the Charter of Fundamental Rights of the European Union in the fulfillment of all my duties".

The Commission has explicitly acknowledged practices that are in breach of the Charter of Fundamental Rights, the Convention on Human Rights, the International Covenant on Civil and Political Rights, and the Commissioner responsible took a personal oath to uphold the charter. Despite this, the Commission has chosen to do nothing to bring an end to these practices.

Ad hoc private control of freedom of communication and freedom of assembly

Terms of service instead of laws. Terms of service instead of constitutions.

The use of the terms of service of private companies to replace law and due process is of law is a common theme of many lawmakers in recent years. This is particularly clear in some of the projects funded by the European Commission. For example, the "CEO Coalition to make the internet a better place for kids" was convened, chaired and funded by the European Commission. Its goals included the production of extra-legal procedures for the "effective takedown" of allegedly illegal content. In the course of the CEO Coalition meetings, which European Digital Rights attended, the European Commission made it very clear that it did not see a contradiction between convening, chairing and funding an initiative to use non-judicial methods to remove online content and its obligations under the EU Charter on Fundamental Rights to ensure that restrictions on freedom of communication be "provided for by law."[51] The Commission's view was that, as the measures would be applied "voluntarily" by private companies and not the Commission itself, its obligations were not activated.

This means that, as far as the European Commission is concerned, identical activities can be both illegal breaches of fundamental rights or legal measures that do not breach fundamental rights. If they are foreseen by law, then they are illegal, but if they are imposed "voluntarily" by internet companies, then they are legal. In the Sabam/Scarlet[52] and Sabam/Netlog[53] cases, the blocking and filtering measures under debate were deemed unlawful and the Court ruled that such policies could not be imposed by EU Member States or their courts on grounds that they would be in breach of the fundamental rights of citizens to freedom of communication and freedom to do business. In the CEO Coalition, the Commission took the view that the measures ruled by the Court to be unacceptable and illegal breaches of fundamental rights of citizens would be acceptable and legal if they were implemented outside the rule of law.

Both the "CEO Coalition" and a very similar project called "Clean IT" (also funded by the European Commission) worked to persuade companies to adapt their terms of service,

to permit maximum flexibility, allowing them to take ad hoc policing measures. A leaked draft of Clean IT's proposals suggested that terms of service "should not be very detailed", thereby maximising the potential for unilateral action on the part of the service provider.[54]

The European Commission took this bizarre logic to another level of incoherence in its draft Regulation COM(2013) 627. This explicitly proposed a right for internet access providers, in the absence of any specific safeguards, to interfere with online communications to prevent (undefined) or impede (undefined) serious crimes (undefined). This proposal is in quite direct and obvious breach of the European Commission's obligations to respect (and the Commissioners' personal oath to this effect) the European Charter of Fundamental Rights which states that restrictions must be "provided for by law" and must be "necessary and genuinely meet objectives of general interest".

"ISPs need to feel more responsible than they do today not just for the enforcement of the law, but also for the preservation of values."

- Robert Madelin

Director General of the European Commission Directorate General for Communications Networks, Content and Technology (DG Connect).

Some principles

The rules of the game?

Principles followed by governments to privatise law enforcement

1. Ignore competition concerns

Often, large businesses will see an opportunity to gain a competitive advantage by generously implementing measures ostensibly"for the good of society", while benefiting from an economy of scale and vertical integration. Smaller companies will then have the choice between bad publicity for failing to implement similar measures that the larger (and, therefore, better known) companies have implemented, or bearing the disproportionate cost of implementing the measures.

2. Never assess efficiency or possible counterproductive effects

Governments and business have efficient public relations departments that can "spin" so-called "voluntary" measures as being unquestionably good for society. As the media rarely investigate the details, there is little or no danger that a detailed analysis of whether the measure is actually helping or harming society will be undertaken.

3. Use child protection as the justification, wherever possible

It does not really matter what the ultimate aim is, whether from a business or policy perspective; if possible use child protection as the "reason" for the intervention. Once it has become normal to filter, block or carry out surveillance for ostensibly "child protection" purposes, it is much easier to spread the restriction to other policy areas.

4. Avoid using research or scientific data

"Why doesn't company x do more to protect children" is a great headline grabber. It is obviously better to do more than to do less. More than what? It does not really matter. When the objectives are political and the §impacts are not a priority, research will dilute the political message and political benefit.

5. Circumvent the democratic process

A democratic proposal will be subject to public scrutiny. It has proven comparatively easy to implement key provisions of ACTA and SOPA through "voluntary" measures. The democratic process created bad publicity and too much public attention.

Principles followed by governments to successfully persuade internet companies to accept devolved policing duties

1. Keep rules on intermediary liability as vague as possible

When liability provisions were first drafted around the year 2000, there were few blogs, there were few social media. The online services available have changed considerably, making it difficult to interpret the old rules in this new world. As long as companies are uncertain about their legal liability for possibly illegal content, they will play safe. Logically, they will prioritise measures that protect their own profits and market share. In early 2014, the European Commission has confirmed that it will reject its own internal analysis and not move forward with clarifying procedures for removal of potentially illegal material.

2. Cheap and ineffective is fine

Do not ask companies to implement expensive technologies for the exercise of devolved policing duties. The principle that internet companies can and should be policing online speech is more important than the effectiveness of this policing or any counterproductive effects that it may have.

3. Adopt laws to implement technologies that may not have been invented yet

Laws which call for the implementation of "agreed" (unspecified) standards, creates the possibility to implement measures in the future without needing to worry about either lawmakers or the public knowing what this is likely to mean in the future.

4. Use the press - "Somebody should do something about something bad"

We all agree that bad things are bad. The press can always be relied on to run a story that "[named big company – ideally one that is in the press getting bad publicity for other reasons] should do something" about something bad. Particularly if the technology is cheap, companies will capitulate very quickly rather than trying to explain the nuances of fighting whatever "bad" things they are supposed to police online.

5. Assure industry that there won't be mission creep

You won't be in power by the time they find out this is not true. In any case, with technology changing so quickly, you cannot really be held responsible for what you say now, because technology will have changed so much by the time you or your successors decide to expand the measure.

Principles to respect legality and effectiveness

At the Stockholm Internet Forum in 2013, EDRi held a brainstorming session with civil society and industry representatives from around the world. We discussed what elements might be necessary to establish the desirability, legality and effectiveness of voluntary measures taken by industry to achieve public policy objectives. This is the outcome of that meeting:

Criterion 1: Is the process internal or external to the intermediary?

Broadly speaking, the more the process is internal to the intermediary, the more likely it is that the measure will be effective. Internal motivations and implementation (solving something that is a direct problem for the intermediary through internal processes) are likely to lead to measures that achieve the public policy objective more efficiently than external motivations (such as avoidance of legislation) and external implementation (such as penalising customers or third parties for alleged infringements of law).

Criterion 2: Are there vested interests on the part of the intermediary?

Voluntary or mandatory interventions by intermediaries to achieve public policy objectives may be supported or initiated by companies as a way of achieving a competitive advantage. This can result in them taking punitive actions against competitors or by lobbying for measures which only incumbents (due to economies of scale) can easily implement. This can lead to unintended (economic and/or societal) consequences that are disproportionate to the public policy objective being pursued.

Criterion 3: How competitive is the market?

There are cases, online marketplaces for example, where the nature of the service and competitive environment may be adequate to ensure that voluntary interventions by the service provider would not result in any significant competitive or practical impact on the user whose activities are restricted. The real choices available to the subject of the measures in question are therefore of importance in assessing the value of a voluntary intervention.

Criterion 4: What is the (public) policy objective being pursued?

Is the intervention seeking to address the business or public relations concerns of the company (through a ban on content which is not illegal, for example) or to enforce a specific law? Interventions to implement a democratically agreed law clearly have more legitimacy than other measures.

Criterion 5: Whose law is being implemented?

Is the intermediary implementing (voluntarily or otherwise) a law that has been democratically approved in the country in question or (also) in countries outside the jurisdiction that adopted the law? This question is crucial for the democratic legitimacy of the activity.

Criterion 6: Are there regional variations of the impact of the measures?

Currently, certain social networks are given preferential treatment by mobile operators in some countries. As a result, the choices available to Internet users in those areas are significantly narrower, which changes the assessment of the proportionality of any measure. Voluntary interventions, especially to regulate activities which are not illegal, would be particularly inappropriate in such circumstances.

Criterion 7: What is the responsibility of the intermediary for its interventions and does the citizen have a right of redress?

Is there a practical legal way of making the company responsible for the impact of the measures it takes (particularly if voluntary) and is effective redress available for the user? If not, this creates a situation where

the intermediary has significant power but limited or no responsibility. It is clear that such situations should be avoided.

Criterion 8: What is the collateral damage for liability exceptions?

The "safe harbour" protections offered to Internet intermediaries have been crucial in the development of an open Internet, protecting free speech against arbitrary, defensive measures being taken by intermediaries. There is therefore a significant danger of voluntary measures being (mis)used to reduce liability protections.

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

- United Nations,

Universal Declaration of Human Rights

Conclusion

If we are going to abandon basic principles, should we have a conversation about it first?

How can it be that the digital world that has generated – and continues to generate – such opportunities for human rights can also be used as a tool for such destruction of human rights? The answer is populist reliance on private companies to regulate an environment that does not always lends itself easily to law and law enforcement. It is essential and urgent to stop the erosion of the rule of law, democracy, freedom of assembly, freedom of communication, privacy and legal certainty. As a society, we need to cherish the democratic potential of digital technologies and – even when this is difficult – prevent the silent digital decay of both online and offline rights that the we appear to have taken for granted.

We urgently need serious reflection on whether our societies still believe in principles that have been long established in human rights law and – if we do – concerted action to stop their continual decay. The International Covenant on Civil and Political Rights, in particular, has been ratified, or at least signed, by every UN Member State – yet the UN Office for Drugs and Crime urges those Member States to breach Article 17 and praises one Member State for breaching Article 19 of the UN Covenant on Civil and Political Rights. We cannot build a meaningful, credible, global structure for the defence of human rights in the digital era if we have no foundation – if we do not know what human rights we still believe in. We also need a clear understanding of the role of private companies in a complex, partially borderless "public space" that is owned by private companies, rather than sliding into an undemocratic world of corporate censorship.

Footnotes

01 All of these examples are detailed in Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, presented to the 17th Session of the United Nations Human Rights Council on 16 May, 2011 and available from http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (last accessed 27 September, 2013)

02 See http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act_iii

03 http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement

04 It formally still is, as the proposal was never formally withdrawn

05 It formally still is, as its signature by various countries still has legal meaning under international law

06 Mike Masnick, "The Definitive Post On Why Sopa and Protect IP Are Bad", Techdirt, 22 November 2011, available at http://www.techdirt.com/articles/20111122/04254316872/definitive-post-why-sopa-protect-ip-are-bad-bad-ideas.shtml (last retrieved 23 July 2013)

07 Maira Suton and Parker Higgins, "We Have Every Right to Be Furious About ACTA", 27 January 2012, available at https://www.eff.org/deeplinks/2012/01/we-have-every-right-be-furious-about-acta (last retrieved 23 July 2013)

08 A full list of EDRi's analysis documents regarding ACTA is available from http://www.edri.org/acta-archive (last retrieved 26 July 2013)

09 http://www.avaaz.org/en/save_the_internet/ (last retrieved 26 July 2013)

10 https://secure.avaaz.org/en/eu_save_the_internet/ (last retrieved 26 July 2013)

11 According to various references on the Wikipedia ACTA page - http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement (last retrieved on 23 July, 2013)

12 Directive on the Enforcement of Intellectual Property Rights (2004/48/EC). Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:EN:PDF (last retrieved 26 July 2013)

13 Mat Brian, "German ISPs hand over 300,000 accounts per month in fight against piracy", 1 June 2011. Available at http://thenextweb.com/eu/2011/06/01/german-isps-hand-over-300000-accounts-per-month-in-fight-against-piracy/ (last retrieved 30 June 2013)

14 For more information, see http://en.wikipedia.org/wiki/ACS:Law (last retrieved 23 July, 2013)

15 Hansard 26 January 2010, Columns 1309-1310. Available from http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100126-0003.htm (last retrieved 30 June 2013)

16 Siraj Datoo, "France drops controversial Hadopi law after spending millions", The Guardian, 9 July 2013

17 ICANN, "A single, authoritative root system for the DNS", 9 July 2001. See http://www.icann.org/en/about/unique-authoritative-root (last accessed 26 July 2013)

18 http://www.state.gov/e/eb/cip/netfreedom/index.htm (last retrieved 24 July, 2012)

19 Digital Millennium Copyright Act of 1998. For more information see http://www.copyright.gov/legislation/dmca.pdf for more informaton

20 Google's DMCA reporting form can be found at https://www.google.com/webmasters/tools/dmca-notice?hl=en&pid=0 (last retrieved 26 July 2013)

21 Jennifer Urban and Laura Quilter, '"Efficient process or chilling effects?" Takedown notices under section 512 of the Digital Millennium Copyright Act" 22 Santa Clara Computer & High Tech. L.J. 621 (2006). Available at http://digitalcommons.law.scu.edu/chtlj/vol22/iss4/1 (last retrieved 26 July 2013)

22 See also the summary of the study hosted at Chilling Effects http://static.chillingeffects.org/Urban-Quilter-512-summary.pdf (last retrieved 26 July 2013)

23 Articles 8 and 10 of the European Convention on Human Rights and Article 19 of the International Covenant on Civil and Political Rights, for example.

24 http://www.oecd.org/internet/innovation/48289796.pdf

25 Ibid, page 5

26 OECD Council Recommendation on Principles for Internet Policy Making, available from http://www.oecd.org/sti/ieconomy/49258588.pdf (last retrieved 31 July 2013)

27 Edward Wyat, "White House says it opposes parts of Two Antipiracy Bills", New York Times 14 January, 2012. http://www.nytimes.com/2012/01/15/us/white-house-says-it-opposes-parts-of-2-antipiracy-bills.html?_r=0 (last retrieved 26 July 2012)

28 The White House Blog, "Obama Administration Responds to We the People Petitions on SOPA and Online Piracy", 14 January 2012 http://www.whitehouse.gov/blog/2012/01/14/obama-administration-responds-we-people-petitions-sopa-and-online-piracy (last retrieved 26 July 2012)

29 Ibid

30 "Can you really be traced from your IP address?", PC Pro Magazine, 28 March 2011. Available at http://www.pcpro.co.uk/features/366349/can-you-really-be-traced-from-your-ip-address (last retrieved 31 July 2013)

31 "Biden makes the case for Assange as a high-tech terrorist", Huffington Post, 19 December 2010. Available at http://www.huffingtonpost.com/2010/12/19/joe-biden-wikileaks-assange-high-tech-terrorist_n_798838.html (last retrieved 26 July 2013)

32 James Ball, "The Bankers' blockade of Wikileaks must end", 24 October 2011. http://www.theguardian.com/commentisfree/2011/oct/24/bankers-wikileaks-free-speech (last accessed 30 July 2013) xxxiii Ernesto,

33 "MasterCard and Visa start banning VPN Providers", Torrentfreak, 3 July 2013

34 See https://www.smashwords.com/press/release/32

35 "Best Practice Guidelines for Ad Networks to Address Counterfeiting and Piracy". Available from http://2013ippractices.com/bestpracticesguidelinesforadnetworkstoaddresspiracyandcounterfeiting.html (last retrieved 26 July, 2013)

36 US Intellectual Property Enforcement Coordinator, "2013 Joint Strategic Plan on Intellectual Property Enforcement," June 2013 (last retrieved 26 July 2013)

37 Statement of Christine Jones before the United States Senate Committee on Judiciary on "Targeting Websites Dedicated to the Theft of American Intellectual Property", February 16, 2011. Available at http://www.judiciary.senate.gov/pdf/11-2-16%20Jones%20Testimony.pdf (last retrieved 24 July, 2013)

38 Nate Anderson, "Takedowns run amok" The strange Secret Service/Godaddy assault on Jotorm", February 16 2012. Available from http://arstechnica.com/tech-policy/2012/02/secret-service-asks-for-shutdown-of-legit-website-over-user-content-godaddy-complies/ (last retrieved 26 July 2013)

39 ICANN, "Guidance for Preparing Domain Name Orders, Seizures, Takedowns". Available from https://www.icann.org/en/about/staff/security/guidance-domain-seizures-07mar12-en.pdf (last retrieved 26 July 2013)

40 Mike Masnick, "ICE Finally Admits It Totally Screwed Up; Next Time, Perhaps It'll Try Due Process" 21 February, 2011. Available at http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml (last retrieved 24 July, 2013)

41 See http://www.nytimes.com/2008/03/04/us/04bar.html

42 "OECD Council Recommendation on Principles for Internet Policymaking", December 2011. Available from http://www.oecd.org/sti/ieconomy/49258588.pdf (last retrieved 26 July 2013)

43 See http://www.internetjurisdiction.net/

44 UNODC, "The use of the Internet for terrorist purposes", United Nations, New York, 2012. Available from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (last retrieved 25 July 2013)

45 Ibid, p 138

46 Ban Ki-Moon, "Keynote address to the World Forum on Democracy", 8 October 2012. Available from http://www.un.org/apps/news/infocus/sgspeeches/statments_full.asp?statID=1685#.UfDviaz4vjI (last retrieved 25 July 2013)

47 UNODC 2012, op cit, p 51

48 Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011)225 final. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF (last retrieved 25 July)

49 Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (last accessed 25 July 2013)

50 See, for example, European Commission, "Data Retention: Commission takes Germany to Court requesting that fines be imposed", 31 May 2012, available at http://europa.eu/rapid/press-release_IP-12-530_en.htm (last retrieved 30 July 2013)

51 Charter of Fundamental Rights of the European Union, 2000/C 364/01, available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf (last retrieved 25 July 2013)

52 Case C70/10

53 Case C360/10

54 Clean IT Project – Detailed Recommendations Document for best practices and permanent dialogue". Available at https://www.edri.org/files/cleanIT_sept2012.pdf (last retrieved 25 July 2013)