REPORT

Index policy paper: Is the EU heading in the right direction on digital freedom?

20 Jun 2013
BY BRIAN PELLOT

The internet's rapid spread has opened up a wide range of debates, nationally and internationally, around freedom of expression online. Many governments, not only in authoritarian regimes, are considering or taking some actions that restrict rather than promote digital freedom. Recent revelations and allegations around the US National Security Agency's mass surveillance programmes show the deeply worrying extent to which freedom of expression is being undermined and compromised globally.

In this paper, we look at where the EU is situated in these pressing debates – analysing some of the core issues and policies relating to digital freedom in both the EU's external and internal policies. While in principle the EU supports freedom of expression, it has often put more emphasis on digital competitiveness and has been slow to prioritise and protect digital freedom. Individual member states have emphasised digital freedom to varying degrees, but pronouncements in favour of keeping the internet open and free at the international level are too often undermined by more restrictive policies at home, from digital surveillance to filters and takedown requests. Human rights including freedom of expression are as crucial online as they are offline. The EU acknowledges this and has started identifying ways to better safeguard freedoms online. One significant development on this front is the EU's work on forthcoming freedom of expression guidelines, but the EU still lacks a coherent overarching strategy and set of principles for promoting and defending freedom of expression and human rights more generally in the digital world – both within and beyond the EU.

Globally, we are seeing increasing debate – amongst both state and non-state actors – about whether or not and how to regulate freedom of expression online. In the next two to three years, these debates are likely to lead to crucial decisions including whether or not to establish top-down control of the internet – something EU member states and the US currently oppose in favour of a more diverse and bottom-up multistakeholder approach. With China and Russia pushing for greater government control, these debates are acquiring a strong geopolitical dimension.

Rapid shifts in technology have also raised new questions around how takedown requests, filters, surveillance, cybersecurity, privacy, net neutrality, copyright, offence, and basic access issues impact on digital freedom. The EU is developing policies and directives on some of these issues but not always in ways that protect human rights and freedom of expression, nor in ways that ensure a coherent, consistent approach to digital freedom. A strategic approach is vital, both to guide the EU through areas where different interests may conflict, and to ensure the EU has strong and compelling external strategies and positions promoting digital freedom internationally. Without a unified strategy, the EU risks failing to defend freedom of expression online and may even undermine it.

In this paper, we first look at the EU's positioning in external debates and policies. We then consider how its internal policies complement or conflict with external positions.

Section One: The EU's role in the global digital freedom debate and its external policies

The EU's external policies on a range of digital issues are increasingly important for global freedom of expression, but too often these policies are ad hoc and inconsistent. External initiatives including the EU's No-Disconnect Strategy, forthcoming freedom of expression guidelines and export controls on surveillance technologies have been generally positive but have not led to the development or adoption of a unified digital freedom framework. The European Parliament's proposed digital freedom strategy for EU foreign policy is a step in the right direction, but leaders in the Commission and elsewhere within the EU need to take these issues seriously if the Union is to contribute to safeguarding digital freedoms on the global stage. This section explores where the EU stands on the most important global digital freedom debates and how effective its external policies are at safeguarding freedom of expression online.

The global internet governance debate

Who should control the internet is an emerging and critical fault line in geopolitics. The internet governance debate came to a head at the Dubai World Conference on International Telecommunications (WCIT) summit at the end of 2012. This meeting brought together 193 member states of the International Telecommunication Union (ITU) in part to decide whether or not and how the ITU should regulate the internet. On one side of the divide, Russia, China and Iran lobbied for greater government control of the net. Most influential emerging democratic powers (India the notable exception) overwhelmingly aligned with this top-down approach for a range of reasons. On the other side, EU member states and the US argued the internet should remain governed by an open and collaborative multi-stakeholder approach. The EU's influence in advancing this more positive position for online freedom of expression at the ITU is partly limited by the fact that only individual states can vote.

The European Commission, as a non-voting WCIT observer, did produce a common position for member states that opposed any new treaty on internet governance under the UN's auspices. This position called on states to support only technology neutral proposals and to oppose any attempts to make ITU recommendations binding. The position also supported privacy and data protection, network robustness, and pro-competitive measures for telecommunications traffic but made no mention of free expression. This absence is worrying, given that privacy and data protection do not always align with free speech and that the position's commercial point on traffic could be interpreted to negate net neutrality. To effectively promote digital rights, this common position should have explicitly acknowledged freedom of expression as a human right the ITU need respect.

Because ITU member states negotiated behind closed doors, media and civil society were largely shut out of the treaty drafting process. Sources with some knowledge of the negotiations reported division among EU member states in the initial discussions. Ultimately, all 27 EU member states and another 28 countries including the US abstained from signing the final treaty amid a range of concerns. 89 states including China and Iran but also the emerging democratic powers of Brazil, Turkey, Indonesia and Mexico signed on to the new treaty. The fact that states with massive populations and rising influence in their regions are leaning towards more top-down control of the internet should be of significant concern for the EU and member states who sit on the other side of the debate.

Lacking a coherent strategy

The EU has yet to establish a coherent strategic approach either internally or externally on digital freedom, but the European Parliament and the European Commission have started to address some key issues such a strategy should include. The forthcoming EU freedom of expression guidelines and strategies around global network resilience mentioned below are crucial and positive developments, but a broader, more joined up strategy will be necessary for the EU to positively and effectively influence internet governance and related issues and to encourage international partners and EU member states to fully commit to digital freedoms at home and internationally.

“A Compact on the Internet”

Two years ago, the Commission looked set to develop a coherent strategic approach to digital freedom. The Commissioner for internet-related policies Neelie Kroes put forward what she called a “Compact on the Internet” listing seven “internet essentials” to preserve the net’s social and economic benefits. Although not perfect, this compact at least attempted to address some of the most important digital freedom issues, but it was never developed into a standalone strategy and is no longer a live part of EU policy discussions.

The seven issues Kroes’s compact addressed are: civic responsibility, one internet, multistakeholder, pro-democracy, architecture, confidence of users, transparent government. While most of these principles are crucial and positive, others either do not go far enough, miss the broader picture or open the door to potentially troubling regulation and legislation.

If “civic responsibility” implies civility and respect, as it seems to do in Kroes’s description, EU policy should not be used to set such boundaries for speech. “One internet” that ensures unity and avoids fragmentation is essential, but this point should have gone one step further to include net neutrality i.e. the principle that access to information should not be made faster or slowed down for commercial or political purposes.

Kroes’s compact was never developed into a comprehensive initiative, but some of its key points have been addressed in recent EU polices. The European Parliament has proposed a comprehensive digital freedom strategy, but there has been no similar initiative so far from the Commission or European Council.

EP Report on a Digital Freedom Strategy in EU Foreign Policy

The European Parliament has recognised that safeguarding digital freedom will require a more unified and comprehensive strategy than the current mix of ad hoc principles and initiatives allow. In December, a majority of Parliament endorsed the EU digital freedom proposal put forward by Dutch MEP Marietje Schaake. The comprehensive report covers human rights and development, trade, and internet governance and addresses some of the greatest threats facing digital freedom of expression.

The report calls for the EU to recognise digital freedoms as fundamental rights and as “indispensable prerequisites for enjoying universal human rights”. The strategy also promotes net neutrality and multi-stakeholder internet governance, both crucial for free expression online, and stresses that digital freedoms should be mainstreamed in all EU external actions and annually reviewed.

Although these broad principles are positive, specific points in the EP strategy do need further consideration. One point stresses that for a country to receive EU aid for implementing technological infrastructure it must safeguard digital freedoms. Given that some EU member states restrict digital freedoms at home, this conditionality provision is perhaps too heavy handed. If the EU is to help bridge the digital divide, as this strategy intends, its approach on this needs to be proportionate. The strategy also calls for a ban on the export of EU-made “repressive technologies and services” to authoritarian regimes. Although such policies often bring positive results, some EU and US export bans in the past have inadvertently harmed the safety and free expression of activists, meaning that any such ban should be proportionate and followed up with regular impact assessments. Despite these reservations, the report is a welcome start and could be the foundation for a strategic EU approach to global digital freedom.

EU external initiatives on digital freedom

As its common position at WCIT demonstrated, the EU has the capacity to positively shape clear freedom of expression policies and priorities on international digital freedom issues. Several initiatives including the new European Endowment for Democracy, the European Instrument for Democracy and Human Rights and other EU bodies aim to enhance rights and freedoms including digital freedom abroad. The most significant efforts on this front are the No-Disconnect Strategy, which aims to support activists and ensure network resilience during political crises, and the new freedom of expression guidelines due by the end of 2013. These and other initiatives

outlined below represent positive advances for EU digital freedom policies, even if their actual effects have yet to be seen or their successes have so far been mixed.

No-Disconnect Strategy

The EU's first major attempt to address digital rights in its external work was the No-Disconnect Strategy in late 2011. This strategy began as the EU's digital human rights response to the Arab Spring, but its scope rapidly expanded beyond its southern neighbourhood. No-Disconnect aims to provide activists, political dissidents, bloggers, journalists and citizens the tools and support they need to exercise their rights under authoritarian regimes and to prevent governments from inappropriately monitoring citizens or crippling communications networks, as happened in recent years during protests in Egypt and Syria.
No-Disconnect's first year was spent conducting research to deliver on its objectives, meaning it has produced few tangible outcomes to-date. One promising project in the works aims to map network disruptions and offline legal and political developments affecting internet access around the world. A workshop was help in November 2012 to discuss this European Capability for Situational Awareness project.

Given No-Disconnect's small budget (under 5 million Euros), civil society's expectations for its scope and what it can achieve should be measured. NDS is not an overarching EU digital freedom strategy and was never intended to be. It has neither the capacity needed to function quickly nor the remit to adequately address all challenges currently facing digital freedom of expression. It is, however, the EU's first initiative of its kind to systematically address key threats to freedom of expression online and provides an important network and funding pool for organisations working on digital freedoms.

Freedom of Expression Guidelines

As part of its 2012 Action Plan on Human Rights and Democracy, the EU is working on new guidelines for online and offline freedom of expression due by the end of 2013. These guidelines, similar in format to previous EU guidelines on torture, the death penalty and religious freedom, could provide the basis for more active external policies and perhaps encourage a more strategic approach to digital freedom. The guidelines are expected to come into play when carrying out human rights impact assessments and in determining conditionality on trade and aid with non-EU states. Freedom of expression is on the agenda at each of the EU's more than 30 human rights dialogues with non-member states each year, meaning these guidelines could also help to enhance this process.

Member states met in early May to discuss an outline of the guidelines. It is expected that a version of this outline will be posted online in June for comment and consultation, but the first full draft – which is expected to be ready in July – will not be openly published. As these guidelines will be a Common Foreign and Security Policy document, there will be no full and open consultation for civil society to comment on the draft. This is unfortunate and somewhat ironic given the guidelines' focus on free expression. The Council should open this process to wider debate and discussion.
Key principles that must be included in the digital freedom part of these guidelines are clear. Safeguarding freedom of expression online requires a multi-stakeholder approach to internet governance. Only a bottom-up approach that protects the voices of netizens and civil society can preserve a free and open net. Any limits made on speech must be approved by a court order. Only limitations that are prescribed by law, serve a legitimate aim and are necessary in a democratic society can be lawfully imposed. In these exceptional circumstances, restrictions should be limited, transparent and proportionate, and takedown requests should be backed by a court order. Mass surveillance and the unnecessary storage of digital communications also breach fundamental human rights and should be addressed in the guidelines, along with basic access issues and net neutrality.

Although externally facing, the freedom of expression guidelines may also be useful in indirectly establishing benchmarks for internal EU policies. If such policies contradict the EU's external guidelines, the latter will have little relevance or impact.

Curbing the ‘digital arms’ trade

A more concrete move by the EU to promote digital freedom of expression abroad has been the recent establishment of export controls to Syria and Iran. Self-regulation and corporate social responsibility often do not go far enough to adequately address this issue. These regulations, drafted in January 2012, are meant to limit the flow of surveillance equipment made in the EU to these states, both of which have used such technologies to suppress their citizens’ fundamental rights.

European Parliament agreed to proposals requiring the Commission to maintain an updated list of restricted technologies and affected states in late 2012. Meant to curb the “digital arms trade”, these measures are important steps for maintaining the EU’s human rights credibility and promoting freedom of expression abroad. Although generally seen as positive, some restrictions have inadvertently prevented activists from downloading tools that enhance their security. The EP Report on digital freedom strategy calls for wider bans, but as mentioned above, these can sometimes infringe on freedom of expression and lead to unintended consequences, meaning such bans should be proportionate and subject to regular impact assessments.

Conclusion on external EU policies

Debates around internet governance, takedown requests, surveillance, censorship and other digital issues are intensifying on the global stage. Initiatives like the No-Disconnect Strategy and upcoming freedom of expression guidelines should help the EU to define its key priorities on digital freedom of expression and increase its effectiveness in promoting these principles abroad. Recently announced plans for a Global Internet Policy Observatory – a collaborative online platform to monitor new internet policies and technological developments around the world – mark another step in the right direction. Yet a more comprehensive, coherent, and strategic approach is still needed if the EU is to play a positive role in setting the global agenda and influencing decisions on digital freedom. Kroes’s compact on the internet never turned into a full-blown initiative, but the EP’s proposed digital freedom strategy for EU foreign policy shows how a comprehensive strategy could be developed. Any digital freedom strategy should also address crucial internal issues – including domestic member state policies and EU-level concerns around cyber security, surveillance, privacy and other issues explored below – if it is to be relevant and effective.

Section Two: Digital freedom and regulations within the EU

Across EU member states and the EU as a whole, external policies that promote a free and open internet are often at odds with internal policies and actions that restrict digital freedoms at home. In this section, we first look at some of the key issues in individual member states and then assess some of the most important new internal EU digital policies, especially those on data protection and cyber security, that are having an impact on freedom of expression. Attempts to promote corporate social responsibility around digital rights issues and to establish more clarity on takedown requests and intermediary liability are also underway, but establishing credible human rights guidelines for businesses is difficult when member states and the EU do not always lead with best practice. In the absence of a coherent strategy, member state policies permitting excessive surveillance and filters are negatively affecting digital freedoms.

EU member state policies and digital freedom

Sweden, the UK and the Netherlands are some of the more active EU member states promoting digital freedom abroad, but restrictive domestic policies within these states often contradict their positive external stances.

The World Wide Web Foundation places Sweden at the top of its 2012 Index of internet growth, utility and impact, with the UK, Finland, Norway and Ireland also in the top 10. Freedom House ranks Estonia as number one on its 2012 Freedom on the Net index, and all EU member states in the ranking are at the “free” end of the scale. These indices represent a snapshot of the EU’s

digital freedom situation but do not imply these states fully respect digital rights. Member states consistently fail to uphold their freedom of expression obligations online and offline, showing that even these “best” member states have their flaws.

Sweden is one of the strongest proponents of global digital freedom. The annual Stockholm Internet Forum organized by the Ministry for Foreign Affairs brings together government, civil society and business representatives to discuss the social and economic benefits of a free and open internet. The Swedish government focuses heavily on freedom of expression in its cyber security strategy and has backed civil society’s Declaration of Internet Rights, which calls for a free and open internet. Its internal policies are better than many other states but do raise some serious concerns.

Given the chilling effects surveillance can have on freedom of expression, Sweden’s most troubling digital laws are those that allow the government to monitor online communications. The Law on Signals Intelligence in Defence Operations authorizes the Swedish intelligence agency to intercept, without any warrant or court order, all telephone and Internet traffic that take place within Sweden’s borders. A 2012 data retention directive requires service providers to store data about online communications, and a 2008 law allows the government to monitor the actual content of international communications with court permission. These policies set bad precedents for other countries looking to implement their own digital initiatives.

The UK also leads calls for digital freedom abroad while some government officials continue to push for restrictive policies at home. In 2011 the UK hosted the first annual Conference on Cyberspace in London (followed by Budapest in 2012 and headed for Seoul in October 2013). At the 2011 summit, Foreign Secretary William Hague proposed principles for governing behaviour in cyberspace that include universal access, openness and freedom. These principles are positive, but others calling for tolerance and respect online and collective action to address cyber crime could potentially lead to further restrictions on freedom of expression.

The British government recently dropped support for a ‘Snooper’s Charter’ that would have included sweeping data collection and retention proposals that amount to population-wide surveillance. A House of Commons MPs’ scrutiny committee strongly criticised these proposals. Plans to put forward less extensive online surveillance laws were announced in May. The UK has seen a growing number of social media prosecutions in recent years, often for speech that is merely offensive. The Director of Public Prosecutions recently issued new guidelines aiming to clarify and limit how prosecutors deal with online offence, but laws that allow the criminalisation of “grossly offensive” speech are still on the statute book.

The Netherlands is another example where positive external rhetoric on digital freedoms does not always align with initiatives at home. The Dutch foreign ministry launched the Freedom Online Coalition in 2011 to work with other countries towards advancing digital freedom. The 18 states that have joined the coalition agree to work with civil society and the private sector to better respect and promote our rights online. Domestically, the Netherlands recently passed legislation to safeguard net neutrality, but a push in the Dutch parliament to grant police greater surveillance powers shows that not all domestic developments have been positive for digital freedom in the Netherlands.

When these and other EU member states promote digital rights abroad but restrict some of those same rights at home, they undermine their credibility on the global stage and give states with repressive policies an excuse to postpone reforms or to enact even worse policies.
The next sections will explore how internal EU initiatives on cyber security and crime, privacy and data protection, copyright and takedown requests, and corporate responsibility are supporting or restricting freedom of expression online.

Cyber security and crime

Globally, there is growing concern about cyber attacks and the potential threats they pose for commerce and communication. Several new EU policies on network resilience and cyber security aim to address both the financial and free speech effects of cyber crime. Cyber security is closely tied to privacy and data protection, as security breaches can expose users to some of the same

threats. Security is also a basic access issue – when communications networks are compromised or cut off, so is digital expression. Despite some overlap, cyber security and freedom of expression considerations are not always aligned. Initiatives that protect the privacy and security of individuals often promote freedom of expression online, whereas those that allow governments to monitor and interfere with online communications can do the opposite.

The EU's new strategy on cyber security, agreed February 2013, directly addresses how cyber attacks and network disruptions threaten fundamental rights, including freedom of expression and privacy. The Commission states that cyber security is predominantly the responsibility of member states but hopes this strategy will help to address EU threats in a more joined up manner. This approach means increased government surveillance across member states, which is likely to have detrimental effects on individual privacy and freedom of expression despite the strategy explicitly stating that "increased global connectivity should not be accompanied by censorship or mass surveillance". This principle must be upheld if freedom of expression is to be preserved and promoted across the EU and beyond its borders, meaning any new surveillance policy's reach should be limited and proportionate. The EU should also address revelations that external government surveillance efforts like the US National Security Agency's Prism programme are undermining EU citizens' rights to privacy and free expression.

The strategy aims to raise awareness of cyber security threats, provide a framework for member states and international actors to combat these threats, and reduce cyber crime through the effective implementation of new legislation. Overall, the document is more a summary of threats to be tackled than an actual strategy, but it should guide the Commission's actions in the coming years.

A directive on network and information security announced in the new strategy and currently being considered by Council and Parliament aims to collate information on major cyber security incidents across the EU. This pooling of information could help coordinate rapid responses to cyber attacks but also risks negatively impacting on free expression if personal data is included in surveillance efforts.

The cyber security strategy is not the EU's only recent attempt to address cyber crime. In January 2013, the EU and Europol opened a cyber crime centre in The Hague to try to reduce illegal online activity in Europe. The centre's efforts currently focus on online fraud, child sexual exploitation, and threats to critical infrastructure. Cyber crime prevention efforts that focus on content, such as child pornography or copyrighted materials, can lead to unintended and overly broad censorship triggered by automated filters that block perfectly legal content. Any efforts to curb the flow of online content should be limited and must be carefully monitored to ensure that legal content is not restricted.

One cyber security proposal that caused considerable concern in 2012 was the EU's Clean IT project, which aimed to fight terrorist content and activity online. Leaked draft proposals endorsed making the act of linking to terrorist content illegal and included several other recommendations that European Digital Rights (an NGO network) described as "absurd", including proposals that governments should be permitted to circumvent notice and takedown procedures, that real name laws preventing anonymity online should be implemented, and that any laws preventing employers from filtering or monitoring their employees' internet usage should be abandoned. These provisions, which seriously conflict with freedom of expression principles, were dropped when the final report was published in January. Many EU insiders say the project will not be followed up on due to lack of consensus around the definition of what actually constitutes terrorist content or activity.
These EU cyber security initiatives present real threats to freedom of expression. Safe and secure networks are vital for digital communications and economies, but the means used to maintain networks should not compromise fundamental rights. These security proposals should be limited and respect privacy as both a fundamental right and an integral aspect of freedom of expression. The prime emphasis should be on security for the individual user.

Privacy and Data Protection Regulations

The EU is currently debating data protection reforms that would strengthen existing privacy principles set out in 1995 and harmonise individual member states' laws. Privacy and freedom of expression are often complementary rights, increasingly so online where conversations can be chilled when people know they are being monitored or recorded. But these rights sometimes conflict over issues of public interest and when the notion of a "right to be forgotten", not currently recognised under international law, is interpreted too broadly. Individual EU member states approach privacy from very different legal and cultural traditions. These differences and concerted corporate and government lobbying efforts have led to much conflict over the prospect of a unified binding policy on EU data protection.

The revised EU General Data Protection Regulation, which is likely to be voted on in July, aims to give users greater control of their personal data and hold companies more accountable for their use of it. Many companies that rely on user data for profit oppose the plan, whereas some privacy advocates argue it does not go far enough. In April, a coalition of European digital rights groups launched a campaign called Naked Citizens to warn that new proposals, largely influenced by corporate lobbying efforts, could reduce users' privacy rights. In June, it emerged that US officials successfully lobbied for a clause to be dropped from the new data protection regulation that would have limited requests for EU citizens' communications records under the US National Security Agency's controversial Prism programme.

Privacy and freedom of expression often diverge over the deletion of data. The proposed regulation's right to be forgotten would primarily allow users to remove content they provided to social networks in the past. This limited right is not expected to require search engines to stop linking to articles, nor would it require news outlets to remove articles users found offensive from their sites. The British government and several others have criticised the proposal for having the potential to create unrealistic expectations for users and practical difficulties for companies. The Center for Democracy and Technology called these difficulties "unreasonable burdens" that could chill expression by leading to fewer online platforms for unrestricted speech. These concerns, while perhaps too strongly expressed, should be taken into consideration at the EU level. In the data protection debate, freedom of expression should not be compromised to enact stricter privacy policies.

Takedown requests and intellectual property rights

European laws are vague in defining what constitutes valid and legitimate takedown requests. This ambiguity results in legal uncertainty for both companies and users. In June 2012, the EU announced a public consultation to clarify how "notice-and-action" i.e. takedown procedures affect freedom of expression and other issues. The consultation received many responses, and the Internal Market and Services Directorate General (DG MARKT) is apparently drafting a new policy on notice and action. It is anticipated that this directive or communication will specify that takedown requests must meet certain criteria and be substantiated with evidence while also clarifying how "expeditiously" intermediaries must act to avoid liability. A policy that clarifies companies' legal responsibilities when presented with takedown requests should limit the problem of over-compliance and its detrimental effects for freedom of expression without extending liability beyond what is appropriate or necessary given their roles as platforms and networks.

Intellectual property rights have become the source of much debate and tension at international trade negotiations in recent years. In July 2012, the European Parliament rejected the Anti-Counterfeiting Trade Agreement (ACTA), which threatened basic digital freedoms including access and net neutrality, amid substantial and sustained pressure from civil society and everyday netizens. This activism alerted many politicians to new, influential constituencies that strongly favour digital freedom of expression.

ACTA's defeat has not ended debate around intellectual property rights. Copyright removal requests from corporations and government requests for the removal of otherwise illegal or offensive content are steadily on the rise. A good benchmark to track this trend is the Google Transparency Report. Although EU countries are nowhere near the worst offenders (Brazil, the US, India, Russia and Turkey) in terms of takedown requests, Germany, France, Austria, Italy, the UK

and Spain all requested that more than 100 items be removed from Google's services between July and December 2012. In May 2013, the British Recorded Music Industry led the list of copyright owner takedown requests, specifying more than 3.2 million URLs be removed from Google's search index. The sheer volume of such requests can overwhelm web companies and internet service provides, causing those afraid of stiff penalties to over-comply and remove URLs that do not link to illegal content.

Under the 2000 e-commerce directive, internet companies can be held legally liable if they fail to expeditiously remove content when they have "actual knowledge" that it is illegal. In a recent letter to the Commission, European Digital Rights highlighted the fact that individual member states interpret this "actual knowledge" clause differently, leading to uncertainty and over-compliance. Other EU projects encouraging internet companies to self-regulate content through their terms of service compound this problem and constitute a chill on freedom of expression.

Corporate social responsibility and freedom of expression

Major web companies increasingly provide the platforms and set the rules for our digital communications but are not held to the same openness, transparency and accountability standards as are states when they regulate our public spaces. This privatisation of censorship is a growing cause for concern. One partial way to tackle it is for companies to commit clearly to implementing and respecting basic human rights. In a bid to increase corporate responsibility on this front, the EU is drafting CSR guidelines and principles around freedom of expression and privacy for information and communication technologies companies.

These guidelines, which were subject to an open consultation with companies and civil society groups in early 2013, aim to unpack how the UN's approach to business and human rights can apply to the technology sector. Even though EU companies are their primary target, the guidelines, due to be published this summer, could act as a model for best practice globally. Although generally positive and useful, the draft guidelines do not adequately address the types of human rights risks small companies are likely to face. Balancing competing rights concerns, such as privacy and freedom of expression, can be daunting for small businesses and often lead to them over-complying with laws that restrict free speech. Closer attention should also be paid to explicitly protecting the privacy and anonymity of end-users. Although ICT companies should consult relevant stakeholders as human rights issues arise, they should not assume that governments necessarily prioritise human rights over other concerns and policies, such as monitoring citizens' communications data. The guidelines should also encourage companies to issue regular transparency reports, but disclosing information about requests they receive should not mean publicly disclosing information that can be used to identify individual users. These guidelines represent a positive example of the EU proactively identifying and working to address emerging freedom of expression and human rights challenges. Incorporating these suggestions should make them more effective.

Conclusion on Internal EU policies

Just as digital policies in individual member states like Sweden, the UK and the Netherlands are mixed (with external policies mostly promoting digital freedom and internal ones sometimes compromising it), internal EU initiatives have both troubling and promising implications for freedom of expression. The EU is paying more attention to digital freedoms and privacy in its work on cyber security, data protection, copyright and takedown requests, and corporate responsibility, but these internal initiatives too often inappropriately restrict online freedom of expression. Security proposals set out in the EU's cyber security strategy should be limited so as not infringe on privacy. At the same time, stricter privacy policies set out in the Data Protection Regulation should not infringe on freedom of expression. Companies also need clarity on their legal responsibilities when faced with takedown requests and guidance on how best to commit to basic human rights standards. Overlap and inconsistencies between the EU's own policies and those of its member states show that an internally and externally coherent digital freedom strategy is needed to effectively safeguard free speech rights online.

Conclusion

The EU has been somewhat slow to prioritise digital rights, placing more emphasis on digital competitiveness. It is now trying to maximise its impact on these issues by developing positions and policies that more effectively promote digital freedom. Too often, however, relatively positive external initiatives are being undermined by repressive or contradictory internal policies at the EU and member state levels. The EU's positioning at WCIT, the freedom of expression guidelines and the No-Disconnect strategy should help the EU strengthen its external polices around promoting digital freedom, challenging top-down internet governance models, supporting the multi-stakeholder approach, protecting human rights defenders in their use of the internet and social media, minimising surveillance, and limiting takedown requests, filters and others forms of censorship. But for the EU to have a strong and coherent impact at the global level, it now needs to develop a clear and comprehensive digital freedom strategy.

Such a strategy should be based on full respect for human rights online, in particular freedom of expression and privacy, in both internal and external policies. A comprehensive digital freedom strategy would help ensure coherent EU policies and priorities on freedom of expression and further strengthen the EU's influence on crucial debates around global internet governance and digital freedom. These global debates are well underway and will continue to evolve over the new two years of ITU negotiations and beyond. For the EU to effectively promote fundamental rights, it needs to address these most crucial digital challenges of our time with a comprehensive internal and external digital freedom strategy.

Brian Pellot is the digital policy advisor at Index on Censorship