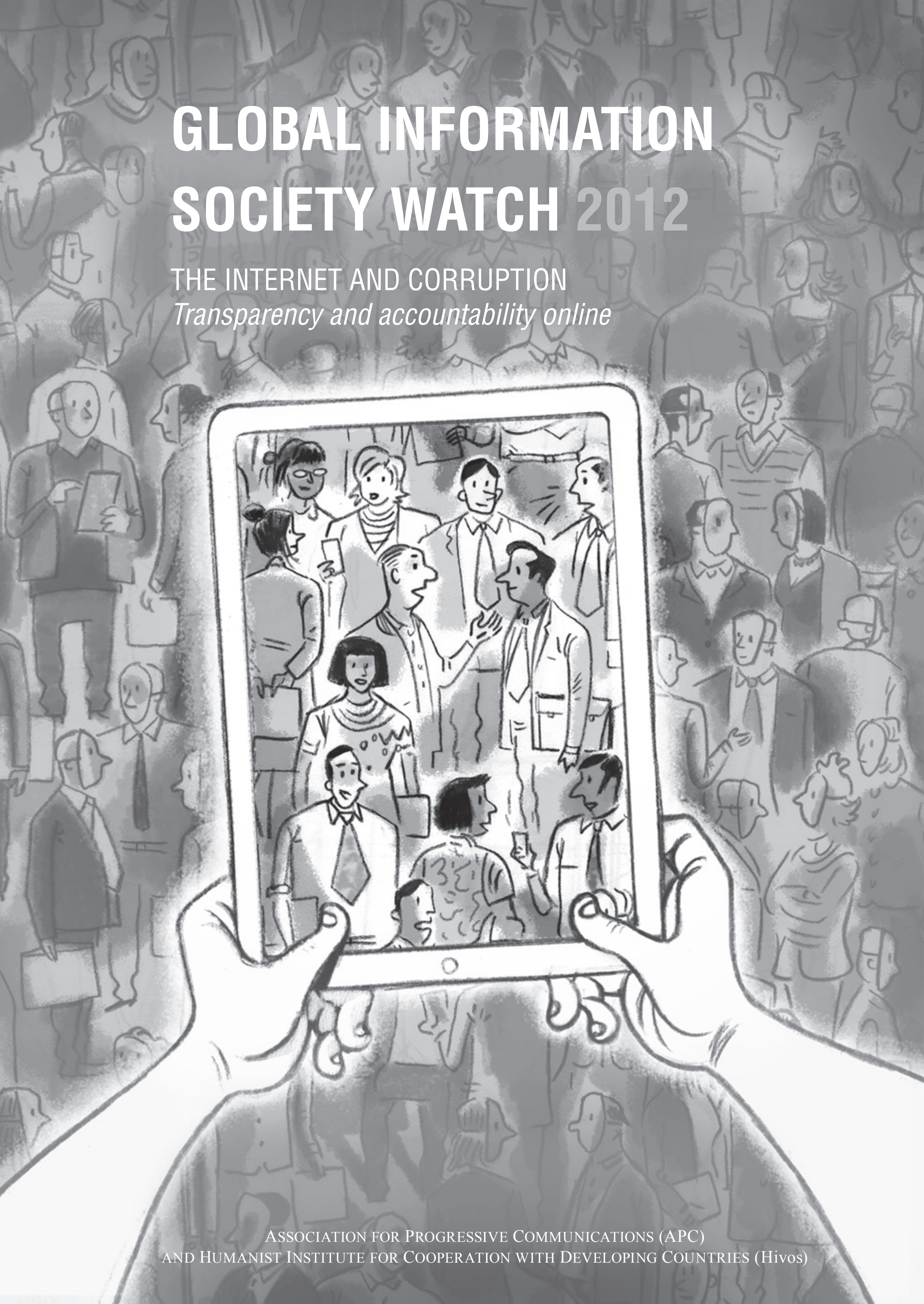
GLOBAL INFORMATION SOCIETY WATCH 2012

THE INTERNET AND CORRUPTION

Transparency and accountability online



Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch

2012

APC

Hivos
people unlimited

Global Information Society Watch 2012

Steering committee

Anriette Esterhuysen (APC)
Loe Schout (Hivos)

Coordinating committee

Karen Banks (APC)
Monique Doppert (Hivos)
Valeria Betancourt (APC)

Project coordinator

Valeria Betancourt

Editor

Alan Finlay

Assistant editor

Lori Nordstrom

Publication production

Mallory Knodel

Proofreading

Valerie Dee
Lori Nordstrom

Graphic design

Monocromo
info@monocromo.com.uy
Phone: +598 2 400 1685

Cover illustration

Matías Bervejillo

Financial support provided by

Humanist Institute for Cooperation with Developing Countries (Hivos)
Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch
Published by APC and Hivos
2012

ISSN: 2225-4625
ISBN: 978-92-95096-85-1
APC-201301-CIPP-R-EN-DIGITAL-176

In search of transparency: From “using” to “shaping” technology

Arne Hintz and Stefania Milan
Cardiff University and The Citizen Lab,
University of Toronto
www.cardiff.ac.uk/jomec and citizenlab.org

In an age in which power equals “the possession, assimilation and retailing of information as a basic commodity of daily life,”[1] transparency has become a luxury and is no longer a given. Cyberspace is populated by an ever-growing number of invisible barriers making knowledge sharing and circulation difficult, such as strict copyright enforcement and content-based discrimination. Digital technologies, however, can contribute to increase transparency and fight corruption. They can amplify and facilitate grassroots mobilisation, and allow an unprecedented outreach and scaling up of protest. Numerous initiatives that work towards creating and expanding transparency happen in the realm of technological activism or at the level of policy activism. Here we want to point to three of them: Anonymous, WikiLeaks and the Icelandic Modern Media Initiative (IMMI) represent different ways – yet with shared characteristics – in which digital technologies can help leverage the grassroots demands for transparency. They demonstrate how technology can be used, but also how it needs to be shaped and developed in order to enhance social and political change. They emerge at the intersection between content and infrastructure concerns, and they therefore demonstrate the need to combine transparency as a political goal with transparency of the technological infrastructure that serves to advance this demand. In what follows we illustrate these three instances of internet-enabled and internet-focused mobilisation, and we explore, in particular, how they address, implicitly and explicitly, a changing environment for online communication.

Net challenges and opportunities

During its short history as a public communication platform, the internet has enabled people to spread information further and wider than before, and to bypass the traditional gatekeepers such as mass media, infrastructure providers and the state. In this way it has constituted a crucial tool for civil society campaigners and social movements, with recent examples including the widely debated role of technology in the “Arab Spring”. However, as its uses have progressed, so have the attempts by both public and private actors to control and restrict what was previously seen as borderless, “free” and uncontrollable cyberspace. The filtering of web content has become a common practice across the globe, and states in both the East and West now restrict (and persecute) the dissemination of content deemed illegal or illegitimate.[2] Intermediaries such as internet service providers (ISPs) and search engines are increasingly enlisted by governments to control and restrict access to content, effectively becoming proxy censors. Access to infrastructure and online services has been shut down, particularly in times of political turmoil (for example in Egypt in January 2011), and the “three strikes” laws in France and elsewhere restrict people’s internet access if they violate intellectual property law by downloading copyrighted content. The controversies on net neutrality – initiated in the US and increasingly spreading to other jurisdictions – have highlighted the role of network providers as potential gatekeepers who may discriminate against some content, for example dissident or non-profit content. Access to critical resources such as funding increasingly takes place online through companies such as PayPal: their decision to withdraw services or limit access can cripple a media organisation, as happened with WikiLeaks. Finally, with the ubiquity of electronic communication, the “capacity of the state to gather and process information about its citizens and about the resources and activities within its space is growing by orders of magnitude.”[3] We are witnessing a trend toward systematic and

[1] Sterling, B. (1993) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Bantam, New York.

[2] According to the OpenNet Initiative, 47% of the world's internet users experience online censorship, with 31% of all internet users living in countries that engage in "substantial" or "pervasive" censorship. OpenNet Initiative (2012) Global Internet Filtering in 2012 at a Glance, blog post, 3 April. opennet.net/blog/2012/04/global-internet-filtering-2012-glance

[3] Braman, S. (2006) *Change of State: Information, Policy, and Power*, MIT Press, Cambridge, p. 314.

ongoing surveillance of all online data, and the erosion of judicial oversight and established notions of due process. Recent examples include the EU Data Retention Directive, "lawful access" legislation in Canada, and the Cyber Intelligence Sharing and Protection Act (CISPA) in the US.[4] Internet companies are gathering significant amounts of user data and are increasingly forced to hand over data to governments. For example, Google received 5,950 requests by the US government for the disclosure of user data in the first six months of 2011 alone, a number which was up 70% from 2010.

The previously free and open environment for citizens' online communication is rapidly transforming into a restricted and controlled space, and internet activists have had to take these changes into account. Efforts to use the internet for advancing social change are therefore complemented by, and intertwined with, activism that addresses the platform itself by opening new technological avenues for information exchange, looking for and exploiting unrestricted spaces, and advocating policies that allow for free communication. Net activism, in this respect, encompasses web-based collective action that both addresses the openness and accessibility of network infrastructure and exploits the latter's technical and ontological features for political or social change. Examples include electronic disturbance tactics and hacktivism, self-organisation and autonomous creation of infrastructure, software and hardware hacking, and online leaking. In the following sections, we will briefly introduce and discuss three current initiatives whose goals combine infrastructure and political change.

Mobilising for transparency: Anonymous, WikiLeaks and IMMI

One of the most prominent examples of net activism in recent years has been the loose network "Anonymous". Its self-identified members have engaged in disruptive activities using electronic civil disobedience techniques such as distributed denial of service (DDoS) attacks, and they have mobilised to increase transparency and circumvent information blackouts on the web. They have taken action against companies, governments, and individuals that, in their view, restrict access to information both on- and offline. Earlier actions included campaigns against the Church of Scientology, accused of censoring information as well as its members' opinions, and against the International Federation of the Phonographic Industry for its pro-copyright battles and its prosecution of the free sharing of cultural goods. During the Egypt internet blackout in 2011, Anonymous used a variety of technological means to facilitate information exchange between Egypt and the rest of the world, providing citizens with alternative communication infrastructure. Efforts to uncover secret information have included Operation HBGary, named after a security firm whose CEO, Aaron Barr, had announced he had identified the network's most active members and threatened to hand them over to the FBI. Anon activists hacked Barr's Twitter account, downloaded some 70,000 emails and documents and published them online, uncovering proposals by the company to the US Chamber of Commerce to discredit WikiLeaks, and thereby providing useful information on secret collaborations between state agencies and security firms.

Having originated in online chat rooms that focused on (largely politically incorrect) pranks, the network has maintained an orientation to the "lulz" – a neologism that derives from LOL ("laughing out loud") and indicates the fun associated with pranks. Its particular approach to the defence of free expression has been marked by irony and disruption. Unsurprisingly, the authorities in several countries, most prominently the US and the UK, have not been willing to see the fun of DDoS attacks and internet break-ins and have rigorously persecuted Anonymous. Despite its sometimes illegal and often deliberately annoying approach, we maintain that several of the network's actions and revelations have, in fact, increased transparency and have shed light on interesting secrets.

A similarly prominent but more formal initiative against information secrecy has been WikiLeaks. Founded in 2006 as an online platform for whistleblowers and for publishing information censored by public authorities and private companies, WikiLeaks' goal has been to harness the speed, interactivity and global reach of the internet in order to provide a fast and secure mechanism to anonymously submit information, and to make that information accessible to a global audience. Partly through its own website and partly with the help of media partners, WikiLeaks revealed extensive corruption in countries such as Kenya; illegal toxic waste dumping by British company Trafigura in Côte d'Ivoire (which the British media was legally barred from reporting); corrupt practices of the finance industry in countries like Iceland; information on Guantanamo Bay prisoners (the so-called "Guantanamo Files") and on the digital surveillance industry

[4] See, for example, Berners-Lee, T. (2012) Analysis: "Cybersecurity" bill endangers privacy rights, *ars technica*, 18 April. arstechnica.com/tech-policy/news/2012/04/analysis-cybersecurity-bill-endangers-privacy-rights.ars

("Spyfiles"); and many other disclosures of information previously hidden from the public eye. In 2010, WikiLeaks made even bigger waves by publishing the Afghan and Iraq War Logs, almost 500,000 documents and field reports that provided an unprecedented and comprehensive account of the two wars and revealed thousands of unreported deaths, including many US Army killings of civilians; and by publishing select US diplomatic cables, taken from a pool of over 250,000 documents, in what became known as "Cablegate". The dispatches offered a broad perspective on international diplomacy, revealing backroom deals amongst governments, US spy practices on UN officials, cover-ups of military air strikes, and numerous cases of government corruption, for example in Middle Eastern and North African countries where the revelations fuelled the growing anger amongst populations with their national elites. In the wake of Cablegate, WikiLeaks operations became increasingly hampered by government investigations of its staff (particularly of founder and editor-in-chief Julian Assange), and extralegal economic blockades that have choked WikiLeaks' access to financial resources. WikiLeaks has seen an onslaught of attacks from both public and private actors, sustained attempts to shut down its operations, and even calls for Assange's assassination.

WikiLeaks has demonstrated the persistence of both governmental and private sector secrecy, as well as the inability of traditional mass media to uncover all publicly relevant information and to inform the citizenry comprehensively. As a member of the "networked fourth estate",[5] its cyber activism has utilised the possibilities of the internet to increase the transparency of our political and economic environment, even though it has chosen the more passive route of providing an upload and publishing function, rather than Anonymous' approach of aggressively seeking and exposing information on perceived wrongdoings. Its core goals have focused on content provision – releases of information that is relevant for public knowledge – but technological as well as legal skills have been at the heart of the project and fundamental for its success. Using decentralised server networks and placing servers in countries with beneficial laws that prevent or reduce the risk of censorship and surveillance, WikiLeaks embodies the intrinsic connection of content and infrastructure.

WikiLeaks' practice of exploiting favourable legislation leads us to the third and final example of internet-related activism: the Icelandic Modern Media Initiative (IMMI). Although very different from the hacktivism of Anonymous and the alternative publishing platform of WikiLeaks, it nevertheless combines concerns with content and infrastructure in online environments. IMMI emerged in the context of the financial collapse of the Icelandic economy in late 2008 and was set up to change the development model of the country from a safe haven for banks and financial services, based on secrecy and the suppression of information, to a transparency haven and a favourable environment for media and investigative journalism. Local social and media activists, supported by international civil society organisations, created a bundle of legal and regulatory proposals to "protect and strengthen modern freedom of expression."[6] At its core is the concern to prevent the suppression of content by both public and private actors. IMMI has initiated the development of a new Freedom of Information Act to enhance access for journalists and the public to government-held information; proposed measures to limit the use of libel laws, prior restraint, and strategic lawsuits to block legitimate information; initiated a new law on source protection, making it illegal for media organisations to expose the identity of sources for articles or books if the source or the author requests anonymity; and developed policy proposals on whistleblower and intermediary protection.[7] Most of its suggestions are informed by, if not borrowed from, existing laws and regulations in other countries. If implemented, this package would provide a legal environment able to protect national and international publishers from content (and other) restrictions. All information originating from, routed through or published in Iceland would be governed by the new set of laws and would therefore be very difficult to suppress. In this sense, the content-focused proposals of IMMI are intrinsically bound to the infrastructure through which content is transmitted: blogs, websites and all kinds of online publications would fall under Icelandic jurisdiction if they use Icelandic infrastructure, even if the publishing organisation does not physically relocate to the country but merely posts content on web serv-

[5] Benkler, Y. (2011) A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate, working draft. www.benkler.org/Benkler_Wikileaks_current.pdf

[6] See immi.is/Icelandic_Modern_Media_Initiative. WikiLeaks was instrumental in starting the initiative by proposing the idea of a transparency haven, providing knowledge on relevant laws in other countries, and developing some of the thematic cornerstones together with local and international experts.

[7] IMMI (2012) IMMI Status Report, 9 April. immi.is/images/8/8c/2012-04-15_IMMI_status_report.pdf

ers hosted there.[8] Consequently, IMMI has added infrastructure-related concerns to its agenda, particularly proposals on safeguarding net neutrality, and it has engaged with debates on the European Data Retention Directive and, more broadly, online surveillance.

From "using" to "shaping"

Ideas of openness and transparency were at the centre of early internet development and internet policy. The supposedly borderless network with its new publishing opportunities for everyone who had access to it nourished hopes of a new age in which normal citizens could bypass traditional information gatekeepers. Numerous examples demonstrate the power of using online publishing and communication for political action and social change, from activist Facebook groups to blogger networks such as Global Voices, and certainly including Anonymous' actions and the revelations facilitated by WikiLeaks. Thanks to these initiatives, we know more about the world, and it is more likely that corruption is moved from the shadows of secrecy to the sunlight of public knowledge.

However, as online communication is increasingly restricted, surveilled and controlled, the "free network" can no longer be taken for granted. For social movements, this means that "using" the net may no longer be sufficient but rather has to be complemented by "developing", "shaping" and "changing" the net infrastructure and its regulatory and legal framework. Just as the net can be a tool for transparency, its own transparency needs to be safeguarded and expanded. This is, of course, not entirely new. Grassroots tech groups such as riseup.net have, for a long time, engaged in providing secure and free technical infrastructure for civil society groups and social movements, campaigns on net neutrality have become very prominent in many countries, and the network of civil society-based internet service providers, the Association for Progressive Communications (APC), is a major force in global internet governance. However, current forms of cyber activism display an even closer connection between content and infrastructure. Based on thorough technical skills and understanding, they couple a focus on exposing relevant information with a commitment to shape and expand the free spaces of online communication in the face of increasing restrictions. Boundaries between different strategies and practices become blurred as the hacktivism of Anonymous creates new information channels, the media approach of WikiLeaks is shaped by infrastructure and informs a policy initiative such as IMMI, and IMMI engages in the compilation of policy components towards new legal "code", a practice which could be described as "policy hacking". The practices of the three distinct initiatives described here tell us something about new and sometimes unlikely places where current mobilisations for transparency can be found, as well as the need to combine technical strategies, content-related approaches and policy understanding. ■

[8] Bollier, D. (2010) A New Global Landmark for Free Speech, 16 June. www.bollier.org/new-global-landmark-free-speech