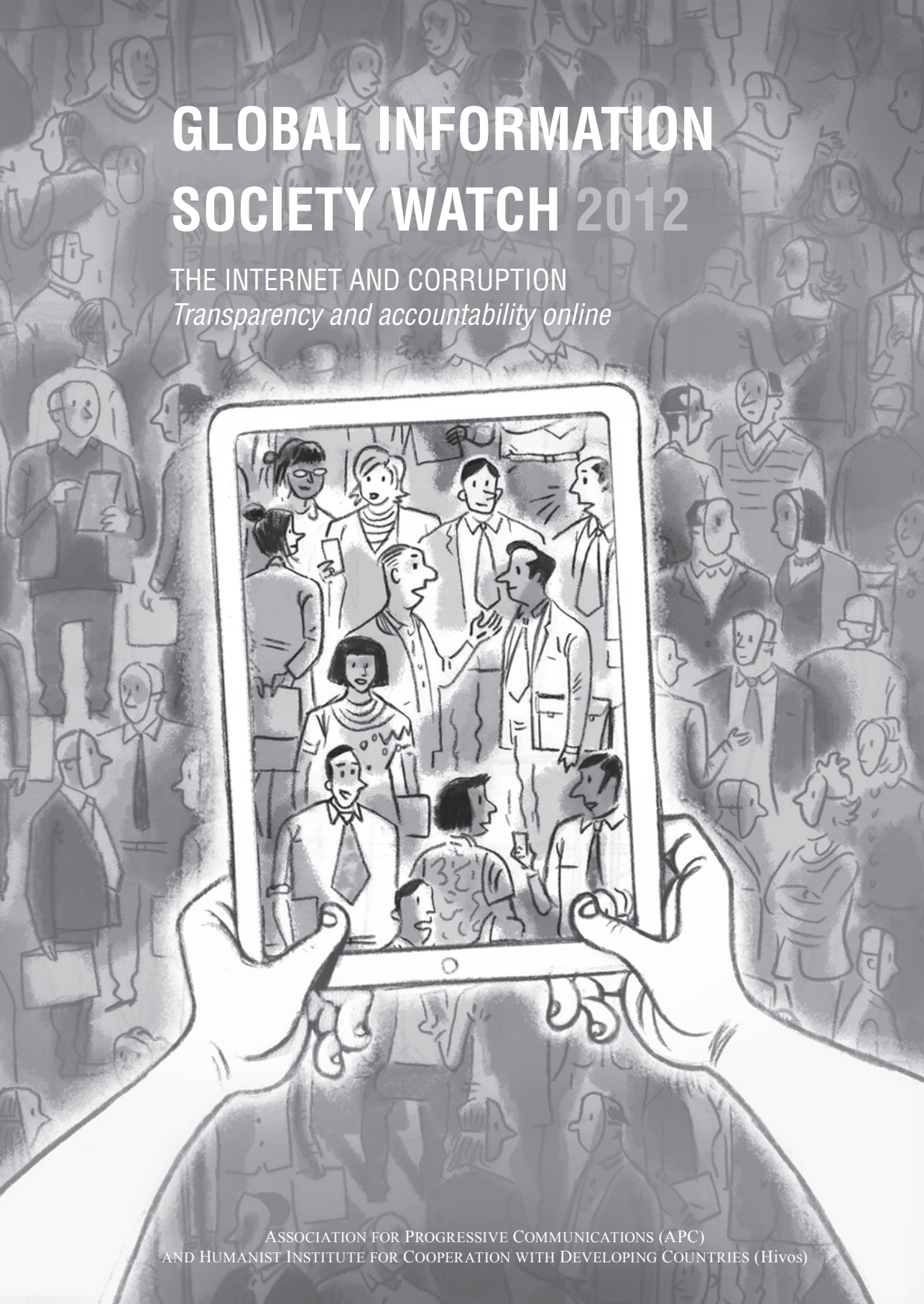
GLOBAL INFORMATION SOCIETY WATCH 2012

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

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

Secrecy, privacy and transparency: The balance between state responsibilities and human rights

Emma Draper
Privacy International
www.privacyinternational.org

Introduction

In 1929, Walter Benjamin wrote that "[t]o live in a glass house is a revolutionary virtue par excellence… Discretion concerning one's own existence, once an aristocratic virtue, has become more and more an affair of petit-bourgeois parvenus."[1] For Benjamin, and for many other Western Europeans, the 20th century was a time of "porosity, transparency, light and free air,"[2] conceptualised in direct opposition to the opaque and furtive 19th century. Yet he failed to predict that, while the average citizen would over the next 80 years come under increasing scrutiny from every angle, the operations of the state would remain comparatively impenetrable. Criticising the utopian ideal of the glass house in his 1986 work *The Art of the Novel*, Milan Kundera complained: "Though it represents a public thing, bureaucracy is anonymous, secret, coded, inscrutable, whereas private man is obliged to reveal his health, his finances, his family situation…"

Despite the fact that, as of January 2012, over 90 countries around the world had implemented freedom of information (FOI)/right to information (RTI) legislation[3] and many political parties around the world now campaign on platforms of openness and transparency, in many respects this situation persists today. There are three main reasons for this: a) FOI/RTI legislation is not applied sufficiently widely or consistently, both because certain bodies enjoy blanket exemption from it and because the laws themselves contain overly broad exceptions; b) when government-held data is published, it is often done so in such a way that it is extremely difficult for citizens to make sense of the information; and c) public officials frequently claim that revealing certain information would be a breach of their right to privacy when they are in fact attempting to conceal dishonesty and wrongdoing.

Narrow focus, narrow freedoms

The existence of FOI/RTI legislation is predicated on the idea that government transparency should be the norm and that state bodies will only shield their actions from view temporarily and when it is in the public interest to do so. The Information Commissioner's Office guidance to the UK Freedom of Information Act 2000 states: "Disclosure of information should be the default."[4] Yet some aspects of FOI/RTI legislation give public authorities far too much scope to restrict its application and remove whole sections of government from its scope. The US Freedom of Information Act (FOIA) 1966, for example, is one of the earliest and most influential examples of its kind, yet it only applies to the executive branch and independent departments and agencies and contains nine exemptions that have permitted many arbitrary denials of applications. There is also very little effective oversight of its operation and virtually no effective remedy available to citizens if agencies fail to meet their FOIA obligations.

Despite the Act's inherent problems, most US presidents historically encouraged interpretations in favour of citizen access – but this all changed with September 11 and the Bush administration's "War on Terror". In 2004, Phillip Doty complained that "[t]he current administration, unfortunately, using 9/11 and other supposed 'national security' concerns, has turned things upside down – the former presumption that government should make records available unless there is a compelling case otherwise has now become a presumption that records should remain hidden from public view unless there is a compelling case made for their publication."[5] Barack Obama campaigned on a platform of transparency, and on his first full day as

1 Benjamin, W. (2005) Surrealism: The Last Snapshot of the European Intelligentsia, in Jennings, M. et al. (eds.) *Selected Writings Volume 2, Part 1: 1927-1930*.

2 Quoted in Buck-Morss, S. (1991) *The Dialectics of Seeing: Walter Benjamin and the Arcades Project*.

3 right2info.org/access-to-information-laws/access-to-information-laws-overview-and-statutory#_ftnref7

4 www.ico.gov.uk/for_organisations/freedom_of_information/guide/act.aspx

5 Doty, P. (2004) *Government, Secrecy and Privacy: Dare we frame the fearful (a)symmetry?*

president claimed: "My Administration is committed to creating an unprecedented level of openness in Government."[6] Yet Obama's presidency has in fact been marked by increased resistance to FOIA requests at the agency level and in the courts,[7] an unprecedented crackdown on whistleblowers and leakers[8] and the disbursement of USD 10 billion on classifying official secrets. In January 2011, the Assistant Solicitor General told the Supreme Court that the administration "do[es] not embrace" the principle (well-established by decades of case law) that exceptions to FOIA should be "narrowly construed" because of the law's presumption in favour of transparency.[9]

In the UK, Privacy International's experience of making FOIA requests, particularly to the Metropolitan Police and other regional police forces, has been a disappointing one. Most of our requests have been met with point blank refusals in accordance with section 23(5) of the 2000 Act: the absolute exception for information directly or indirectly supplied by the security services or relating to the security services. The Information Commissioner's Office (ICO) guidance on section 23 states: "This exemption is not based on the content of the information or the likely effect of disclosure. It applies to all information supplied by or relating to one of these bodies, even if it does not relate to national security, or would not have a damaging effect if disclosed."[10] When drafting FOI/RTI laws, legislators should think carefully before including provisions that provide blanket protection for certain sections of government. Even bodies that deal with sensitive matters of national security should not be rendered entirely opaque and unaccountable, and including absolute exceptions of excessively broad scope allows public authorities to shield themselves from embarrassment under the banner of national security. Legislators should err on the side of transparency by making exceptions qualified rather than absolute whenever feasible, meaning that the public interest in maintaining the exemption must be weighed against the public interest in transparency.

Information overload

In her essay "The Fog of More", Sarah Leonard commented that "the display of lots of information online has itself come to symbolize transparent, healthy democracy." However, when governments focus their energies on simply publishing as much information as possible (what Leonard calls "the virtuous data dump"), the effect is ultimately counterproductive: the vast quantities of raw data are so daunting and difficult to parse that to the average citizen the operations of the state – far from being clarified – seem even more obscure.

The solution to this problem is twofold. Firstly, governments themselves could make more effort to publish information in intuitive formats, breaking data down by category or time period, ensuring that it is fully and effectively searchable by keyword, and publishing supplementary datasets to aid analysis. For example, in June 2010 the UK Treasury released several years' worth of COINS (Combined Online Information System) data through BitTorrent. COINS is the system the Treasury uses to keep track of spending across the public sector. Two months later, they published the first in a series of additional datasets utilising the raw data, in the expressed hope of "mak[ing] key parts of the COINS data accessible, manageable and comprehensible to the wider public, whilst maintaining a low level of aggregation."[11] However, the Treasury's guide to the COINS release acknowledged that, even with these additional datasets, "the files are large and the data held within the files complex. Using these files will require some degree of technical competence and expertise in handling and manipulating large volumes of data. It is likely that these data will be most easily used by organisations that have the relevant expertise, rather than by individuals. By having access to these data, institutions and experts will be able to process and present them in a way that is more accessible to the general public."

The Treasury was correct to assign the lion's share of analysis to external parties. The problem with leaving the responsibility for categorising, aggregating, dissecting and analysing data entirely in the hands of governments is that such activity tends to involve imposing subjective hierarchies, meaning that the data is filtered through certain perspectives and priorities. While this is still the case when "institutions and experts" are performing the task, there will at least be a range of different interests at play, a reduced interest in concealing government error or corruption, and thus less potential

6 www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment

7 www.politico.com/news/stories/0312/73606.html

8 www.politico.com/news/stories/0510/37721.html

9 www.freedominfo.org/2011/01/u-s-supreme-court-hears-corporate-privacy-case

10 www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/s23_security_bodies_v1_fop097.pdf

11 www.hm-treasury.gov.uk/psr_coins_data.htm

for compromising the principles of transparency. Government bodies should encourage as much civic participation in data analysis as possible by widely advertising the availability of raw data and by rewarding the most innovative and useful approaches. For example, the NYC BigApps project offered USD 50,000 in cash and other prizes to software developers for the best new apps utilising New York City open data to help local residents, visitors and businesses.[12]

So-called "civic hackers" like the ones that participated in the BigApps challenge often pick up the slack when the state fails to provide even the most rudimentary tools for understanding the information it disgorges. The website Indian Kanoon was born of its developer's frustration with the failings of the official Indian government judicial rulings website (www.judis.nic.in), which has extremely poor keyword search capabilities and does not order search results by relevance. As a result, the wealth of information it contains – over 1.5 million rulings – is rendered largely unusable. Sushant Sinha launched Indian Kanoon in January 2008. The website indexes judgements from the Supreme Court, the high courts and various tribunals and links them to the relevant statutes. Importantly, it provides all these tools free of charge.

Public access to, and understanding of, national law is crucial to any functioning democracy. As Sinha explained: "Even when laws empower citizens in a large number of ways, a significant fraction of the population is completely ignorant of their rights and privileges. As a result, common people are afraid of going to the police and rarely go to court to seek justice. People continue to live under the fear of unknown laws and a corrupt police."[13] Indian Kanoon is now helping to remedy that situation; it is used by approximately half-a-million unique users per month, widely promoted on Twitter and Facebook, and since March 2012 a mobile version has been available.

Privacy versus transparency?

The traditional expression of the relationship between privacy and transparency as a balancing act between the rights of the individual and the interests of the community is a false dichotomy that has led to a great deal of confusion in the operation of FOI/RTI laws. There is in fact a significant overlap in the contents of the two regimes, as former UK Information Commissioner Richard Thomas has noted: "Both involve the growing discipline of information rights – or rather the information duties and obligations on those who are holding either personal or official information. Both are heavily concerned with transparency and access. Both have a wide horizontal impact affecting virtually every aspect of public, commercial and private life."[14]

More broadly, both privacy and transparency are tools of public good essential for the proper functioning of a democratic society, and both are defences against abuses of power. Yet there are inevitably times when they come into conflict. For example, many records held by public bodies inevitably identify, or contain personal information about, their employees. It may well be in the public interest for there to be transparency about the salaries or salary brackets attached to certain roles, the level of seniority of officials responsible for making certain decisions, or which officials attended certain meetings with third parties. Public bodies also hold the kind of personal data many employers require of their employees, such as their home addresses, salary information, employment histories and photographs, and occasionally (though rarely), it may be in the public interest for some of this information to be revealed. Yet the right to information enshrined in domestic legislation cannot automatically trump the human right to privacy, or vice versa – one must always be weighed against the other.

Every national FOI/RTI law in the world has an exemption for personal privacy, and it is an extremely popular one; in the US the exemptions for personal privacy and law enforcement records concerning individuals have consistently been the two most frequently used exemptions, and in Canada, the privacy exemption was used in 31% of all refusals.[15] Given the vast, and increasing, amounts of information about citizens held by most governments, strong safeguards designed to prevent the unwarranted release of sensitive personal details are crucial. However, it is equally important that the right to privacy not be used as a "fig leaf" for the mistakes or misdeeds of public officials. For example, during the battle for the publication of the expenses of British members of parliament (MPs), it was repeatedly claimed that disclosing certain information (e.g. detailed breakdowns of claims for running second homes) would be an invasion of the MPs' privacy. When the courts finally ruled that such information ought to be disclosed, it became

12 2011.nycbigapps.com

13 www.technologyreview.com/tr35/profile.aspx?TRID=1049

14 Thomas, R. (2008) Freedom of Information and Privacy – the Regulatory Role of the Information Commissioner, paper presented at the Centre for Regulated Industries Occasional Lecture 21, National Liberal Club, London, UK, 9 January.

15 wbi.worldbank.org/wbi/Data/wbi/wbicms/files/drupal-acquia/wbi/Right%20to%20Information%20and%20Privacy.pdf

clear that many MPs had been abusing the system by wrongfully claiming thousands of pounds of taxpayers' money to cover bogus costs or extravagances far beyond the realm of acceptability.

Some cases may be considered less clear-cut. In 1998, the daughter of a Thai woman called Sumalee Limpaovart was denied entry to the elite, government-run Kasetsart Demonstration School. Limpaovart was told that her daughter had failed the entrance exam. She subsequently requested the test results for her daughter and the 120 successful applicants; the school refused, but she appealed to Thailand's Official Information Board for an order to force the school to release the information. While the appeal was in process, the school offered a compromise: an anonymised list of test results. To include the children's names, the school argued, would infringe their right to privacy. The list showed that a third of the students had also received a "failing" grade, but had nonetheless been given a place at the school. Limpaovart suspected that these students were *dek sen*, children from privileged families who used social connections or bribes to secure their offspring's entrance to the (publicly funded) school, but it took another year before the Board ordered the disclosure of students' names. It then became clear that many of them came from prominent political and business families. The Thai State Council ultimately ruled that the school's admissions policy violated the constitutional protection against economic and social discrimination, and schools across Thailand were ordered to reform their admissions procedures.

In this situation, the anonymised list of test results was not enough to reveal the corruption at the heart of Thailand's education system; exposing (and thus ending) this corruption required that the children's privacy be invaded and their names published. Yet unlike the MPs, the children were not responsible for the misdeeds of their parents and teachers. While the public good that flowed from this invasion was ultimately very significant, it was unclear beforehand that the publication of the children's names would benefit anyone except, possibly, Limpaovart's daughter. The balancing of the right to information and the right to privacy is perhaps one of the more challenging aspects of FOI/RTI legislation, and getting that balance wrong can have disastrous consequences.

In conclusion, it seems that there is still room for improvement in both the drafting and the application of FOI/RTI legislation. Candidates for public office tend to pay lip service to government transparency but show little genuine commitment to it once in power. Officials still see both national security and privacy as "get out of jail free" cards allowing them to dodge requests for embarrassing information. And many governments have yet to learn that disorganised outpourings of information actually undermine transparency. Yet for dozens of countries, particularly in the developing world, FOI/RTI laws are still relatively new, and enthusiasm around them is high. People are aware that, when used effectively by citizens and applied correctly by public officials, they can be a powerful tool for combating corruption and holding the powerful to account. By contrast, government transparency seems to be dwindling in the US, which has had a Freedom of Information Act for over half a century. It may be that the right to information, like a muscle, needs frequent and vigorous exercise in order to function as effectively as possible. Regular FOI/RTI requests remind governments that state transparency is the rule, not the exception to the rule, and that every citizen has the power to expose dishonest or abusive systems at his or her fingertips. And although the role of the internet in realising and strengthening this power is not always a straightforward one, information technologies can be extremely valuable tools for promoting transparency and empowering citizens. ■