Policy Brief Examples

ID: HF10247
To: Government of South Africa
From: Section 27
Scenario: A
Date: March 8 2019
Word Count: 1742

South Africa's Internet Freedom Strategy: The time is now

Who is Section 27?

Section 27 is a public interest law centre which works in cooperation with many other public interest organisations to advance human rights and Constitutionalism in South Africa. Established in 2010, Section 27 seeks to develop the law in such a way that promotes, protects and advances the human rights of all South Africans.

Outlining the problem

In the wake of the acrimonious end to the World Conference on International Telecommunications (WCIT) summit in December 2012, with 55 member states refusing to sign the new International Telecommunications Union (ITU) regulations, battle-lines have been clearly drawn between proposers and detractors of a global authority on internet governance. This stale-mate just shows that the reality of even basic global norms for internet governance is a distant one. In the meantime, users' fundamental rights to privacy and freedom of expression are being infringed by *inter alia* increasing personal data requests from governments, intermediary liability legislation, firewalls and surveillance technologies. South Africa has a duty to its citizens to protect their fundamental, constitutionally entrenched rights and therefore needs to formulate a comprehensive internet freedom strategy and begin to implement it through promulgation of domestic legislation and review-mechanisms. Without such domestic action, the longer the United Nations takes to reach consensus on the issue of Global Internet Governance (if it ever does), the longer South Africans are exposed to violations of their rights to privacy and free-speech. The time to act is now.

The Debate: whether there should be a global, intergovernmental body solely responsible for internet regulation.

The Internet has revolutionised the way we communicate, interact, learn, conduct business and express ourselves. The world is now more interconnected than ever and dependency on the internet permeates every level of society. The Internet itself however is a double-edged sword which can be used to empower and emancipate citizens (Fontaine & Rogers, 2011) and, at the same time, can lead to serious threats to privacy, national security and intellectual property. In an attempt to harness the benefits of the Internet and curb its harms, there have been attempts to establish some kind of international regulation of the content of Internet. However, as was illustrated by the WCIT 2012, the inherent problem with the global position currently is that it is nothing more than dialogue and all attempts have failed to answer the fundamental question: whether there should be international regulation of the Internet's content.

An international regulatory body might seem like the appropriate solution to an "international" network like the internet; however it is problematic for the following reasons:

1) Jurisdiction issues are a perennial problem in establishing international treaties and agreements. Nations cannot be forced to be bound by a specific treaty and many nations would opt out of assenting to an International Regulatory Body that could work against their interests as an authoritarian regime (e.g. Iran) or their perspective on freedom of expression on the net (e.g. China). It takes many years for an international treaty to become a peremptory norm of *jus cogens* (and thus bind all states) so the success of an international regulatory body will be entirely dependent on nations volunteering to be bound by it and not all nations are willing to do this.
2) Agreements at International level rely on consensus, which is often very difficult and slow to achieve on all issues (especially important issues). This was illustrated by 55 states refusing to sign the new ITU which actually does not bind states anyway and has no leverage over resources or domain names (Wilson, 2013) Because agreements tend to develop very slowly, they allow harmful practices (such as data requests and surveillance) to continue in the interim when action is needed. Further, political considerations often influence how states reach
consensus – for example, it is feared that South Africa will side with Russia or China simply because of the economic ties we have to China (Patel, 2013)
3) Agreements are often over-compromised, under-representative and don't account for countries' individual realities and issues which might not fit with a one-size-fits- all international policy. The USA has considerable influence diplomatically and economically (because of ICANN and DNS) and is therefore able to skew
negotiations in such a way that might not be in the best interests of South Africa. A broad set of international norms rather than a specific set of rules relating to internet use allows nations to develop their own domestic law in accordance with the main issues facing their peoples with respect to internet use.
4) An International regulatory body is too far removed from the people affected by the body the most – internet users. Domestic legislation, on the other hand, has a greater chance of being more sensitive to people's wants and needs because citizens can directly influence what that legislation looks like and are more able to hold their governments to account for developing overly restrictive internet law. It is not possible for the average internet user to hold an international regulatory body to account if it acts contrary to their interests.

It is our view that international regulation of the internet is less desirable than each nation-state developing national legislation to regulate the Internet in accordance with broad international norms (very much like the United Nations Declaration of Human Rights sets a broad normative framework within which states must implement policies and legislation which protect, promote and realise such rights). Arguably, the resolution from the UN Human Rights Council affirming that online rights are the same as offline rights (Resolution L13) coupled with the ITU's role in ensuring that telecommunication technologies are safe and compatible is a sufficient global framework within which states can determine, individually, how content should be regulated. Any international attempt to regulate the content of the internet will be unsuccessful because consensus is so difficult to achieve.

It is in South Africa's best interests to support this perspective because it (a) allows government to protect South African internet users through domestic legislation immediately; (b) it shows that government is committed to fundamental rights enshrined in the Constitution; (c) it is the solution that maximises public participation and accountability therefore allowing for the "best-fit" for South Africa.

Policy Recommendations

In light of the above, the following domestic measures should be implemented:

1. *Updating and Promulgating Legislation*

South Africa needs to promulgate and/or update legislation that protects the fundamental rights of South African Internet Users against breaches by its own government, other governments, and international corporations.

The main points of such legislation should be an express rejection of monitoring or surveillance mechanisms; personal data of users handed over by intermediary platforms (e.g. Google, Twitter etc.) only according to a warrant from a court where exceptional circumstances exist; and clear and transparent processes for retrieving data and data take- down requests.

This legislation's starting point should be the protection of human rights and, unlike the proposed Communications Data Bill in the UK or the new Intermediary Liability legislation in India, should not give ISPs or web-hosts any reason to err on the side of caution and hand over private information of users without probable cause. The Law Reform Commission must be tasked with investigating developing South African law in this regard and make recommendations to the National Assembly, which, through its committees can draft legislation to this effect. This is a viable and frequently used option for developing the law (for example, it was used extensively for developing the Promotion of Administrative Justice Act). Further, Parliamentary committees are constitutionally mandated to consult the public and receive input from South Africans about the form and content of such legislation.

The focus of legislative reform should be on protecting South African Internet Users from unjustified infringements of their rights to privacy and freedom of expression. Even though the Google Transparency Report 2012 shows that defamation was the reason for take-down requests, it is only a matter of time before other, more sinister reasons are used. South Africa's defamation law is well developed enough to handle the existing cases and therefore this area of Internet Governance needs no further development legislatively.

2. *Review Mechanisms*

Review bodies must exist to investigate issues pertaining to (a) the promulgated legislation envisaged above; and (b) individual complaints about content or practices that violate rights or threaten national interests. Parliament can consider creating new institutions or, as suggested here, extending the scope of existing institutions such as the Human Rights Commission or the Film and Publications Board. These two institutions are created to protect human rights, ensure due-process is followed and regulate harmful content. The main purpose of the envisaged legislation (i.e. the protection of human rights) and the platform of the internet (as a public platform to communicate and receive information) both fall within the scope of these bodies and can be absorbed easily, effectively and inexpensively under either of them.

3. *Developing judicial precedent*

Having and developing strong judicial precedent with respect to Internet use is just as important as promulgating legislation. In fact, they go hand in hand because it is through these institutions (and the courts) that apply legislation and make it accessible, adaptable (where necessary) and workable.

These three policy considerations address the biggest risks Internet users face while the international community drags its feet in formulating a global policy to protect users. These considerations are in the best interests of policy makers because they can be tailored to the individual circumstances of South Africa as a developing

nation (global regulations cannot); they can be easily changed to fit advances in technology and new threats and difficulties; and importantly they restore legitimacy in the government (following heated criticism over the Protection of State Information Bill) in that government is acting, pre-emptively, in defence of the rights of South African internet users while the international community stalls.

Conclusion

Domestic regulations may not necessarily be mutually exclusive to broad international norms of internet governance, but while the latter runs the diplomatic gauntlet of compromise and negotiations, domestic regulations are the only way South Africa can protect the rights of its citizens at the moment. The South African government has a constitutional duty (under section 7(2) of the Constitution) to protect the rights of citizens. Further, the internet (in it's free, decentralised form) is a unique platform that empowers citizens, enhances civic agency and engagement and promotes participation.

This, in addition to fundamental rights to privacy and freedom of expression, deserves and requires protection by government immediately because it is under immediate threat.

References

Fontaine, R. & Rogers W. (2011) Internet Freedom: A Foreign Policy imperative in the Digital Age. Washington, DC. Centre for New American Security.

Google Transparency Report 2012 (2012). Retrieved on 01 March 2013 at http://www.google.com/transparencyreport/removals/government/ZA/

Patel, K. (2013). *Internet Governing Rights: World powers butt heads*. Retrieved on 01 March 2013 at http://www.dailymaverick.co.za/article/2012-12-05-internet-governing- rights-world-powers-butt-heads/

Resolution L13 (2012, July) *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. Retrieved on 01 March 2013 at http://ap.ohchr.org/documents/ sdpage_e.aspx?b=10&se=128&t=4

The Constitution of the Republic of South Africa, 1996.

Wilson, P. (2013). *Let's keep this dead horse alive so we can beat it some more*. Retrieved on 01 March 2013 at http://www.internetgovernance.org/2013/01/28/lets-keep-this-dead- horse-alive-so-we-can-beat-it-some-more/

ID: DE14567
To: Government of Latvia
From: Think Tank for the Latvian Nation
Scenario: B
Date: March 6 2019
Word Count: 1764

Government should take steps to discourage exports of communications technology

Background of the problem

It has come to our attention that Saur-N, a technology company based in Latvia, has entered into a contract with an authoritarian state X to which it is about to supply communications technology. Such technology can be used for different purposes. On the one hand, such technology would improve the efficiency of X's private sector business and can be used in instances of national insecurity when blocking digital content is necessary. On the other hand, it would also allow the state to exercise control over its citizens and intervene with their privacy by, for instance, tracking mobile phone signals, breaking into e-mail accounts or social network accounts.

This situation creates a serious problem for the government of Latvia and our society. The transfer of technology from Saur-N to X can create a situation where the communications technology that is sold is used to violate human rights of the citizens of X. This situation would substantially threaten Latvia's ability to ensure its international human rights obligations. Likewise, a damage can be done to Latvia's reputation abroad and negatively affect its diplomatic relations.

This contract has sparked a debate on how the government should react in this and similar cases. By means of the following analysis the aim of this policy brief is to show that it is in the interest of the government and our society to discourage the sale of communications technology by Saur-N.

Analysis of policy options

When comparing and analysing the different policy options, several issues emerge and should be considered by the government before deciding upon an appropriate response:

1. International human rights obligations

Firstly, the policy the government decides to pursue should ensure that Latvia fulfils its international human rights obligations. The current policies and legal framework lack a mechanism allowing Latvia to prevent human rights violations caused by the use of communications technology which is exported from Latvia.

Even though Latvia would not be per se responsible for human rights abuses resulting from the use of the exported technology by Saur-N, it can breach international human rights obligations by failing to take steps to prevent, investigate or punish the abuse done by private actors (UN Principles on Business and Human Rights, 2011). Such a situation would negatively affect Latvia's and its citizens' international reputation and therefore should be prevented from happening.

2. Relations between Latvia and state X

Secondly, it is in the interest of the Latvian government and the society that relations with state X remain peaceful. So far, both states have had a neutral relationship with each other. However, there is considerable risk of conflict. The Democratic Peace
Theory suggests that conflict is more likely to occur between democratic and authoritarian states since the different polity types lead to different foreign policy behaviours. In case of contention, which can result from inappropriate use of sold communications technology, outbreak of hostile conflict is more likely to occur (Russet, 1993). Since Latvia is a democratic state and state X is an authoritarian state, steps should be taken to prevent conflict from occurring and Latvia's policies should be carefully designed as to maintain neutral relations with state X.

3. Economic interests of the state

Thirdly, economic interests should be considered since the technology industry benefits the economy of Latvia on multiple scales - by creating employment opportunities, increasing tax revenue for the state and by contributing to state knowledge industry.

4. Specific use of communications technology by state X

Lastly, it should also be considered for which purposes state X will use the communications technology since such considerations go hand in hand with Latvia's international human rights obligations.

As was already pointed out, communications technology can be used in instances of national insecurity when blocking digital content is necessary. The advocates of Internet censorship argue that Internet needs a regulatory mechanism.
Accordingly, communications technology used for this purpose is justified since it allows the state to ensure security and to protect the well-being of its people. It is a common practice by many governments around the world, both democratic and authoritarian, to block online content that contains racist comments, which might create social unrest.

Since the number of users is increasing, content of the Internet becomes available to more and more people allowing information to spread quicker than ever before. Failing to block content that poses a danger to national security may have severe consequences. This is illustrated by the example of India where rumours were spread about two ethnic groups that supposedly were about to attack each other. Use of social media and mobile phones accelerated spreading of information and created a dangerous situation where violent protests took place in the streets of Mumbai and 300 000 Indians had to flee from their home. In this case, the Indian government took measures and blocked around 250 websites in the name of public security. Likewise, it required Google, Facebook and Twitter to close certain accounts and remove their content (Fisher, 2012). Arguably, in those kinds of scenarios failing to take these actions can have severe repercussions.

On the other hand, critics of Internet censorship argue that blocking any content on the Internet conflicts with democratic values such as freedom of speech.
Furthermore, communication technology has often been used to exercise control over state citizens and to intervene with their privacy. Research done by the University of Toronto (2013) revealed that so called Blue Coat Devices that are capable of filtering, censorship, and surveillance are used on public and government networks in countries that have a history of human rights abuses like Russia, China and many others.

"

Considering the fact that the authoritarian state X also has a history of detaining and intimidating people who have protested against the policies of the state it is important to ensure that the technology sold to state X is not used against its citizens and violates their basic human rights. This issue goes hand in hand with Latvia's international human rights obligations.

Proposed policy

On the basis of the analysis above it becomes clear that strategically and practically the most viable policy would include steps that best satisfy the combination of economic interests, human rights obligations and the goal to maintain good relations with state X. Therefore, the government of Latvia should pursue steps that discourage the sale of communications technology by Saur-N by limiting exports of such technology and implementing additional domestic legislative measures to prevent human rights violations.

Alternative options

Option 1: ban the sales of communications technology to state X

When considering alternative options, the easiest way to ensure that no human rights obligations occur due to the exported technology would be to simply ban the sale of communications technology to state X. However, such policy is least favourable when analysing its impact on the economy and relations with state X. A sales ban could potentially create pressure between Latvia and state X, especially since there is no proof that this communications technology will be used in a manner causing human rights abuses in state X. Furthermore, banning the sales of communications technology can lead to loss of income both for Saur-N and its employees as well as the Latvian state which receives tax payments from Saur-N. Since Latvia's economy is still recovering from economic crisis, stimulating production and exports should continue to be considered important by the government.

Option 2: maintain status quo

Furthermore, not pursuing any policy steps on this matter would be equally undesirable for Latvia given its international obligations. For instance, if human rights violations occur in state X due to the data that Saur-N has provided the authoritarian regime with and that are stored on servers in Latvia, Latvia can be held responsible for not having taken the necessary steps to prevent these abuses. Even though in terms of economic benefits this option would be the most feasible one, human rights obligations should be seen as equally important by the government of Latvia. Thus, action should be taken.

Recommendations

1. **Conclude Mutual Legal Assistance Treaty with the regime of state X before issuing an export license to Saur-N.**

A Mutual Legal Assistance Treaty should be concluded with state X before issuing export license to Saur-N. Having such a treaty will ensure that in order for state X to receive data that are held on Saur-N servers in Latvia its courts will need to officially request these data from Latvian courts. Such process ensures that procedural and substantive rights of all persons involved are protected, meaning that Latvian courts can evaluate whether the data will be

used for purposes that do not infringe with human rights and violate Latvia's international human rights obligations (Brown & Korff, 2011).

2. **Require Saur-N and similar companies to submit their corporate social responsibility strategy before issuing them an export license**

Requiring companies to develop their corporate social responsibility strategy increases the level of commitment and accountability the government can expect from the companies. Considering the concerns of human rights violations that could potentially result when communications technology is used, it is particularly important that the government requires from companies to address those risks by elaborating on how the company will try to reduce them or respond to them.

3. **Impose export tariff on all dual use communications technology**

An export licensing system is already in place; however, the barriers to export could be further increased to discourage technology companies from exporting dual use goods, which are defined as "items, which can be used for both civil and military purposes" (European Council, 2009, p. 3). As a result, the government of Latvia should impose an export tariff on all dual use communications technology software and hardware independently from its destination country. Export tariffs would make exports more expensive for the producers thereby discouraging them from exporting certain goods. Such a tariff would also give additional income to the state, which could be used to fund projects initiated by civil society aiming at promoting human rights in countries such as state X.

Concluding remarks

Overall, our analysis has shown that it is in the interest of the Latvian government and our society to discourage the sale of communications technology by Saur-N.
Implementation of the suggested recommendations would allow for the best combination of guarding our economic interests and international human rights obligations. Likewise, it would ensure that we maintain good relations with state X.
The combination of these measures would furthermore prevent Latvia's international reputation to be damaged and allow our diplomatic relations with other countries to remain good.

Bibliography

Brown, I. & Korff, D. (2011). Digital freedoms in International law. Retrieved from http://www.globalnetworkinitiative.org/files/GNI_2011_Annual_Report.pdf

European Council. (2009). Council Regulation (EC) No 428/2009. Retrieved from http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf

Fisher, M. (2012). When Is Government Web Censorship Justified? An Indian Horror Story. Retrieved from http://www.theatlantic.com/international/archive/2012/08/when-isgovernment-web-censorship-justified-an-indian-horror-story/261396/

Russet, B.M. (1993). Grasping the Democratic Peace: principles for a post-Cold War world. Princeton, NJ: Princeton University Press.

United Nations Principles on Business and Human Rights. (2011). Retrieved from http://www.business-humanrights.org/media/documents/ruggie/ruggieguiding-principles-21-mar-2011.pdf

University of Toronto. (2013). Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. Retrieved from https://citizenlab.org/wpcontent/uploads/2013/01/Planet-Blue-Coat.pdf