IRIE
International Review of Information Ethics Vol. 19 (07/2013)

Ulrik Franke:

On the cyber-reputation of governments

Abstract:

Government censorship has a long history, as do attempt to motivate it. This paper offers an analysis of the proposal that states should agree to cooperate ”in curbing the dissemination of information that […] undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment”. This position was adopted in 2011 by the People's Republic of China, Russia, Tajikistan, and Uzbekistan in a proposed *International code of conduct for information security*. The code of conduct can be understood as an attempt to protect the cyber-reputations of states and incumbent governments from the impact of compromising information. The article examines the code of conduct from the perspectives of utilitarianism and moral rights theories. Despite some interesting minor exceptions, it is concluded that neither normative theory can fully endorse the proposed code of conduct.

Agenda:

Author:

Dr. Ulrik Franke:

- Swedish Defence Research Agency (FOI), SE-164 90 Stockholm, Sweden
- ☎ + 46 - 8 – 5550 3504 , ✉ ulrik.franke@foi.se, 💻 www.foi.se

Introduction

Governments have long attempted to censor and curb unwanted information, but the advent of modern information and communication technology (ICT) has changed the playing field. Today, the amount of information available is larger, it spreads quicker, and physical distance matters less. The Wikileaks controversy and the role of ICT in the Arab spring are just a few examples of recent events that have caused a lot of debate.

This paper offers an analysis of the proposal that states should agree to cooperate ”in curbing the dissemination of information that […] undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment”. This position was adopted in 2011 by the People’s Republic of China, Russia, Tajikistan, and Uzbekistan in a letter to the United Nations secretary general, proposing an ”International code of conduct for information security” (Li et al., 2011).

The code of conduct can be understood as an attempt to protect the *cyber-reputations of states and incumbent governments* from the impact of compromising information. Political, economic and social stability is proposed as the good underpinning these restrictions on free speech online. This article examines this proposal from two normative perspectives: utilitarianism and moral rights theory.

How could such damaging information look in practice? Many scenarios are possible, but the recent case of Vladimir Pekhtin is poignant. Pekhtin was a member of the Russian Duma, chairing its Ethics committee. In February 2013, he resigned his position after opposition bloggers had made documents available that exposed his $1.3 million real estate in Florida. The documents were not leaked, but publicly available on the Miami-Dade County government website. In a final address, Pekhtin remarked that ”our opponents […] need to discredit the Parliament, the authorities, which are represented by every person sitting in this hall, and every one of us may turn out to be a target for them” (Barry, 2013).

The article unfolds by first briefly reviewing the code of conduct itself, then analysing it from the perspectives of utilitarianism and rights-based theories, respectively. The article ends with a few concluding remarks.

The code of conduct

The proposed *International code of conduct for information security* was submitted as an annex to a letter from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. It has the form of a potential General Assembly resolution. The purpose is said to be ”to identify the rights and responsibilities of States in information space […] so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people’s well-being” (Li et al., 2011).

Following a pre-amble, the actual code of conduct is composed of 11 articles (a-k), where the main thrust is in article b, where the signatories pledge ”Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies”.

However, the focus of this article is rather article c, the pledge ”To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment”.

If the code is ever signed into effect, it is not clear whether the signatories would comply with it. There is a large body of literature suggesting that democracies are more likely to comply with international agreements than are authoritarian regimes (cf. Simmons 1998 for a review). Given that all four originators are deemed ”not free” by Freedom House (2013), the initiative might be an attempt to limit the freedom of action for others (democracies) but retain it for oneself. At least one analysis claims that this is the ulterior motive behind Russian initiatives in the field of ”international information security” (Giles, 2011). While noting these concerns, this article does not take a stand on any hidden agendas or motives. Rather, the analysis proceeds by taking the proposal at face value, aiming to judge it fairly from the perspectives of the normative theories chosen. A more elaborate analysis of the code of conduct in the context of diplomatic initiatives related to so called cyberwarfare is given by Meyer (2012).

Utilitarianism

From any utilitarian perspective, the code of conduct is strangely *asymmetric*. Utilitarianism not only requires that information with *bad* consequences is *not* disseminated, but also that information with *good* consequences *is* disseminated. Thus, the preference for status quo (i.e. not undermining stability) is not a priori endorsed by utilitarianism. Rather, the utility of the status quo and the utility of any alternative state of affairs are to be assessed by the same normative standards, though there might be epistemic differences in their ease of evaluation. The analysis now unfolds by considering *act* and *rule* utilitarianism separately. This distinction is elaborated in many introductory textbooks on ethics, for example Tännsjö (2002).

Act utilitarianism

Act utilitarianism does not endorse signing *and complying* with any codes of conduct. Regardless of earlier agreements, the utilities of the alternatives at hand always remain the singular moral decision-criterion for the act utilitarian. In this spirit, however, act utilitarianism might endorse signing a code of conduct *without* (necessarily) complying afterwards. Instead the utility of the act would be brought about by affecting the future acts of others (since by hypothesis, future acts of the signatory itself are not affected). The analysis of signals and the effects on acts of others brings us very close to *rule utilitarianism*, which we will now analyze as the more plausible utilitarian candidate to warrant the code of conduct. The act utilitarian loophole of signing but not adhering will then be revisited.

Rule utilitarianism

The possible utility of upholding state reputations is two-fold: (i) *Symbolic* utility bestowed intrinsically by reputation, e.g. citizens’ utility of being proud of their government. (ii) Utility where reputation is *instrumental* to another good, e.g. citizens’ pride in their country driving work to improve the functioning of political, economic and social systems – or citizens’ pride in their country preventing revolutionary violence. The rule utilitarian, making rules for disseminating information, has to maximize the sum of both utilities.

Recent research on the subjective appreciation of poetry might help with the empirics of symbolic utility: individuals experience greater utility when reading a poem, if convinced that it was written by a highly regarded poet (Bar-Hillel et al., 2012). If the same is true for the aesthetic appreciation of flag waving and national anthems (live or on YouTube), then that is a utilitarian argument for curbing information that discredits states: individuals might experience greater utility if convinced that they live in the best of states, than if informed (or misled) to believe that they do not.

Nevertheless, instrumental utility is probably more important (in the sense that food, housing, health etc. are probably more important than the aesthetic appreciation of poetry – at least this holds psychologically true in many circumstances, cf. Maslow 1943). On the *negative* side, revolutionary upheavals are the greatest threat (and the chief concern of China et al.). The danger of pointless revolutionary violence was famously discussed by Burke, and made Hobbes embrace the absolute power of the sovereign. This is perhaps the strongest utilitarian reason for protecting the reputations of incumbent regimes. However, even if the consequences of revolutions are dire, it does not necessarily follow that the reputations of status quo should be preserved at all costs. As argued by Taleb & Blyth (2011) in the wake of the Arab spring, artificial suppression of volatility might merely postpone the inevitable:

> *"Such environments eventually experience massive blowups, catching everyone off-guard and undoing years of stability or, in some cases, ending up far worse than they were in their initial volatile state. Indeed, the longer it takes for the blowup to occur, the worse the resulting harm in both economic and political systems."*

This line of reasoning naturally leads to the *positive* side of variable reputations: they can serve as an error-correcting and efficiency-improving mechanism. Reputation systems on e-commerce websites enable sellers of high-quality goods to receive decent payments, while preventing fraudsters or sellers of or low-quality goods from profiteering on unsuspicious buyers (Resnick et al., 2000), defying Akerlof's infamous "market for lemons" (Akerlof, 1970). But such systems cannot work if reputations cannot be ruined. While incumbent governments are not E-bay peddlers, ICT-fostered transparency can plausibly reduce corruption (Bertot et al., 2010). If the reputation of an incumbent regime is allowed to deteriorate when that regime performs poorly, that can help avoid the brittle and dangerous state of affairs that so worries Taleb & Blyth. If seen from this perspective, it might be telling that the governments of China, ranked 80 in the Transparency International *Corruption Perceptions Index 2012*, Russia, ranked 133, Tajikistan, ranked 157, and Uzbekistan, ranked 170 (Transparency International, 2012), endorse a code of conduct that fosters less transparency.

Interestingly, recent political psychology research finds that the two categories of symbolic and instrumental utility are *psychologically* separate: "Exploratory factor analyses of the symbolic and instrumental items yielded two distinct and virtually orthogonal factors" (Schatz & Lavine, 2007). This means that information that decreases symbolic utility (e.g. by questioning and re-evaluating national myths, historical "truths" or great leaders) does not necessarily decrease the instrumental utility (e.g. the propensity of public sector clerks to fulfill their duties or of people to obey laws). However, some kinds of information that decreases symbolic utility (e.g. exposing corruption or identifying kleptocratic rulers) is a prerequisite for some increases in instrumental value (e.g. getting rid of corruption or ousting unfit office-holders). This is consistent with the observation of Ahlerup & Hansson (2011), who find that from an economic perspective (bearing in mind the importance placed on economic welfare by utilitarianism) the level of nationalism is higher than optimal in most countries, diminishing government effectiveness.

The position of rule utilitarianism can now be properly evaluated. Rule utilitarianism differs from act utilitarianism by considering not only the immediate, static, consequences of acts, but instead emphasizes incentives and dynamic consequences. Seen from this perspective, it seems that although agreements that protect the reputations of incumbent governments might avoid some short term damage (viz. revolutionary upheavals), this gain is far from certain, whereas the losses in the long run (viz. the incentives for corruption and kleptocracy) are virtually unavoidable. Rule utilitarians should select the dynamic error correction-mechanism of reputations that reflect merits, rather than the static status quo-preserving code of conduct. This conclusion becomes even more plausible since the instrumental utility is psychologically independent from the symbolic utility – the gains of error-corrections are to be had without loss of appreciation for flags and anthems.

Having examined some plausible consequences of the code of conduct, we can now return to the act utilitarian possibility of signing but not adhering. Following the analysis above, there is no indication that the utility of sign-not-comply would be greater than the (rule utilitarian) sign-and-comply, which on a balance is unlikely to be endorsed by rule utilitarianism. Thus, act utilitarianism as a foundation for the code of conduct can be ruled out on the same grounds.

Rights-based theories

Moral rights theory ascribes rights to individuals rather than incumbent governments, and does not care for political, economic or social stability – "liberty upsets patterns", as put by Nozick (1974). Thus, *prima facie*, it offers scarce support for protecting the reputations of states. On the contrary, the property rights of individual

Internet users, content providers such as Facebook or YouTube, and Internet service providers protect dissemination of information from state interference. This protection of free speech echoes the *Reporters without borders* condemnation of the code of conduct as ”a concept that in reality is aimed as [sic!] legitimizing censorship” (Reporters without borders, 2012). Ultimately, the right to self-ownership allows everyone to maintain whatever perception they like about others, including states, and attempts to protect one’s reputation must be non-coercive.

However, rights-based theories offer two interesting cases where the dissemination of information may be curbed. First, under a theory of *positive rights*, governments may legitimately provide basic ICT services to citizens, collapsing the distinction between state and service provider. Then, service provider property rights offer no protection against state interference. Second, the emphasis placed by rights-based theories on *voluntary contracts* opens a legitimate possibility for curbing any information dissemination that breaches terms of service. For example, the use of fake personas on social networks to influence opinions – so called *sock-puppetry* – typically constitutes such a breach. Programs for this kind of influence operations have been recently exposed both in the US (Fielding and Cobain, 2011) and in Russia (Barabanov et al. 2012). Such breaches of contract constitute rights violations, and rights-based theories sanction that the offended service provider ceases service and uses government institutions, e.g. police, to seek restitution. However, the wording in the code of conduct clearly warrants much more information curbing than can be plausibly claimed legitimate under the terms of service interpretation of rights-based theories. Thus, the code of conduct as a whole cannot reasonably be endorsed by moral rights theory.

Conclusion

Article b in the proposed *International code of conduct for information security* deals, in a sense, with the cyber reputations of states, or at least their incumbent governments. It makes a normative claim that political, economic and social stability are goods that warrant certain restrictions on free speech online; limiting what kind of information may be spread. States, it argues, ought to co-operate in curbing the dissemination of such harmful information.

Having examined these claims from the perspectives of utilitarianism and moral rights theories, it is concluded that neither normative theory can fully endorse the code of conduct. Though there are conceivable cases when states would be warranted to co-operate in curbing some information harmful to their reputations, these cases are clearly the exception, not the rule. This conclusion gains additional force from the fact that it is broadly supported by two normative theories oftentimes opposed to each other.

References

George A. Akerlof: The Market for "Lemons": Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics, *Vol. 84, No. 3, August, 1970, pp. 488-500*

Pelle Ahlerup & Gustav Hansson: Nationalism and government effectiveness, Journal of Comparative Economics*, Vol. 39, Issue 3, September 2011, pp. 431–451*

Ilya Barabanov, Ivan Safronov & Elena Chernenko: Razvedka botom [Intelligence Using a Bot]. Kommersant*, August 2012, http://www.kommersant.ru/doc/2009256, retrieved 7 November 2012*

Maya Bar-Hillel, Alon Maharshak, Avital Moshinsky & Ruth Nofech: A rose by any other name: A social-cognitive perspective on poets and poetry, Judgment and Decision Making*, Vol. 7, No. 2, March 2012, pp. 149-164*

Ellen Barry: Russian Lawmaker Quits After Real Estate Disclosure, New York Times*, February 21, 2013, http://www.nytimes.com/2013/02/21/world/europe/vladimir-pekhtin-resigns-from-russian-parliament.html, retrieved February 28, 2013*

John C. Bertot, Paul T. Jaeger & Justin M. Grimes: Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies, Government Information Quarterly*, Vol. 27, Issue 3, July 2010, pp. 264–271*

Nick Fielding & Ian Cobain: Revealed: US spy operation that manipulates social media., The Guardian, *March 2011. http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks, retrieved 18 January 2013*

Freedom House: Freedom in the World 2013*, 2013, http://www.freedomhouse.org/report/freedom-world/freedom-world-2013, retrieved 31 May 2013*

Keir Giles: "Information Troops" - A Russian Cyber Command?, 3rd International Conference on Cyber Conflict (ICCC), 2011*, pp. 45–60*

Abraham H Maslow: A theory of human motivation. Psychological Review*, Vol. 50 No. 4, 1943, pp. 370–96*

Li Baodong, Vitaly Churkin, Sirodjidin Aslov & Murad Askarov: Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359

Paul Meyer: Diplomatic Alternatives to Cyber-Warfare, The RUSI Journal*, Vol. 157, Issue 1, 2012, pp. 14-19*

Robert Nozick: Anarchy, State, and Utopia*, Basic Books, 1974*

Reporters without borders: Internet enemies report 2012*, March 2012, http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf, retrieved 31 May 2013*

Paul Resnick, Ko Kuwabara, Richard Zeckhauser & Eric Friedman: Reputation systems. Commun. ACM *Vol. 43, Issue 12, December 2000, pp. 45-48*

Robert T. Schatz & Howard Lavine: Waving the Flag: National Symbolism, Social Identity, and Political Engagement. Political Psychology*, Vol. 28, No. 3, 2007, pp. 329–355*

Beth A. Simmons: Compliance with International Agreements, Annual Review of Political Science*, Vol. 1, No. 1, June 1998, pp. 75-93*

Nassim Nicholas Taleb & Mark Blyth: The black swan of Cairo. Foreign Affairs*, Vol. 90(3), 2011, pp. 33–39*

Torbjörn Tännsjö: Understanding Ethics: An Introduction to Moral Theory*, Edinburgh University Press, 2002*

Transparency International: Corruption Perceptions Index 2012*, http://www.transparency.org/cpi2012/results, retrieved 18 January 2013*