International Internet Routing and Individual Rights: Network Sovereignty and Infraethics in the Infosphere

Elliott Williams

30 April 2016

Throughout history, space has been conceptualized as physical. However, new technologies shape and redefine how a space is experienced. Consider, for example, a train connecting two cities, or the electronic faregate in the station. Both dramatically influence a user's perception of and their ability to interact within a given environment. In the present "hyperhistorical" society, where interconnected technologies "become the necessary condition for development, innovation, and welfare,"[1] ICTs (information and communication technologies) are the driving force behind this new space, a space increasingly less geocentric. Floridi calls this new society the *infosphere*, juxtaposed against the biosphere, "a concept that can also be used as synonymous with reality, once we interpret the latter informationally."[2]

The Internet epitomizes this disruption. Without physically altering geographic space, it *transduces* it, creating new location-agnostic communities, markets, and cultures. This shift calls for a new definition of space, one that focuses less on the location and more on the *activity* that a space facilitates. To draw from Manuel Castell: "Space is the expression of society. Since our societies are undergoing structural transformation, it is a reasonable hypothesis to suggest that new spatial forms and processes are currently emerging."[3]

Because Internet infrastructure is itself morally agnostic, routing information from agent to agent, local nation-states lose their saliency as individuals are easily connected to people and organizations outside its borders. We see examples of how agents in the infosphere can use this new "information flow" to their advantage. However, issues of *sovereignty*—a governing's agency's "supreme authority within a territory"[4]—emerge as government and non-government actors vie for control. Individual actors and non-state organizations have unprecedented control over information flow, fro private companies owning and regulating public forums of communication,[5] to search engines being required to categorize which kinds of information should be public and private.[6] To the end that modern democratic states use their sovereignty to protect citizens' fundamental rights,[7] the loss in sovereign influence poses a disadvantage to individual rights. In particular, the presence of this threat calls for recognition of *network sovereignty*, the ability for an agent to "distinguish the boundaries of a network and then exercise a sovereign will or control within and at those boundaries"[8].

[1] Floridi, *The Fourth Revolution*, 31.
[2] Ibid.
[3] Castells, "The Space of Flows."
[4] Philpott, "Sovereignty."
[5] Zuckermann, "New Media, New Civics? My Bellwether Lecture at the Oxford Internet Institute."
[6] Floridi et al., "Advisory Council to Google on the Right to Be Forgotten."
[7] Philpott, "Sovereignty," see "circumscription of sovereign state".
[8] Clement and Obar, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance."

Unlike life in societies organized under individual nation-states, life in the infosphere creates a moral context where no one agent bears full responsibility for the ethical treatment of another. Thus, multiple entities are responsible—must "do their part"—in creating a ethical situation for an agent at a higher level of abstraction. Namely, to ensure protection of privacy and other fundamental rights, a better *infraethics* must be created: a technical "framework of implicit expectations, attitudes, and practices that can facilitate and promote morally good decisions and actions."[9]

International Internet routing is impinging on individual privacy protections and state sovereignty, creating an ethical situation distributed among different causal agents: technical, political, and legal systems are all in play. A proper response calls for recognition of network sovereignty, realizing that the communication infrastructure itself holds moral responsibility to protect individuals. Further, current Internet technologies can be augmented to create a better infraethics, laying the technical groundwork for a system that supports the development of a more ethical infosphere.

Technologies

The Internet is made up of geographically and nationally independent networks, each subordinate to the state and organization it is a part of. Networks vary in size and public accessibility, and are controlled by various organizations: governments, universities, and public internet service providers (ISPs) operate independent networks of computers. A network, known as an *autonomous system* (AS), typically has hundreds to many thousands of agents (called *hosts*) interconnected with each other via devices called *routers*.[10]

To send messages from one host to another, a route is determined between the source host and the destination, and the message is split up into *packets*. Each packet is passed from router to router until it reaches a router that can deliver the packet to the destination. Similar to how a package in the postal service moves from city to city en route to its destination, packets "hop" from router to router via a process called *datagram forwarding*.[11]

What makes the Internet unique is how ASes discover and communicate with each other. Inter-autonomous system communication is what enables the illusion of being able to directly communicate with any Internet-connected computer in the world. ASes discover each other through the *Border Gateway Protocol*, an "inter-Autonomous System routing protocol" which "exchange[s] network reachability information with other BGP systems…sufficient for constructing a graph of AS connectivity."[12] ASes dynamically learn about each others' existence and connectivity, and can use that knowledge to send information between nodes by finding a path from one AS to another.

The key observation here is that networks within the Internet discover each other automatically and send messages to each other algorithmically. There is no regard for where a message comes from or is going, and there is no overarching delivery system aware of the conditions and particulars of the data being transmitted; any internet is merely a system of interconnections between networks, with no single entity "owning" or "controlling" the space, thus the Internet is politically, geographically, and morally ambiguous.

[9] Floridi, *The Ethics of Information*, 272.
[10] Comer, *Computer Networks and Internets*, 342.
[11] Ibid., 387.
[12] Rekhter, Li, and Hares, "RFC 4271."

Network Sovereignty

Networks, hosts, and other components of the Internet are independently "governed" by multiple agencies. Unlike the Internet they make up, they exist in a specific geographical space. Statutory laws regulate how Internet services are accessed in a particular state, and provide authorization for statal systems of control such as surveillance or censorship. Non-state governing bodies, such as the Internet Engineering Task Force (IETF), design rules and protocols by which the Internet operates (e.g. BGP), which influence how other agents participate the space. Computer code itself, such as the BGP path-finding algorithm, systems of encryption, or the TCP/IP stack that Internet agents use to send and receive data, plays an infrastructural role in limiting what the space can be used for. Castells says that technical infrastructure

> "defines the new space, very much like railways defined 'economic regions' and 'national markets' in the industrial economy; or the boundary-specific, institutional rules of citizenry (and their technologically advanced armies) defined 'cities' in the merchant origins of capitalism and democracy. This technological infrastructure is itself the expression of the network of flows whose architecture and content is determined by the powers that be in our world.[13]"

The issue is that the Internet, as-is, cannot protect an agent's privacy. Privacy, under Floridi's ethics, is a necessary component of personal identity in a hyperhistorical society, and is necessitated "by considering each person as constituted by his or her information, and hence by understanding a breach of one's informational privacy as a form of aggression towards one's personal identity[14]". Thus, the system an individual exists in *must* have infrastructure in place to protect their civil right to privacy: "Any society (even a utopian one) in which no informational privacy is possible is one in which no self-constituting process can take place, no personal identity can be developed and maintained, and hence no welfare can be achieved, social welfare being only the sum of the individuals' involved."[15]

In an Internet shaped and governed by non-state agents, a person's statal legal protections are insufficient to protecting their right to privacy. For instance, as observed by the *IXmaps Project* at the University of Toronto, a significant amount of Canadian Internet traffic is routed through the United States. Even Canadian-to-Canadian communicated often travels abroad: due to the US's formative role in Internet infrastructure, much of the highly-efficient infrastructure exists within US borders. Using a method of recording Internet pathways called *traceroute*, IXmaps determined that roughly 25% of Canadian-to-Canadian traffic passes through routers and switches in the US.

This is of particular concern due to suspected NSA surveillance of Internet communications. Project researchers Obar and Clement point to revelations from Snowden, Klein and others that suggest that NSA is engaged in bulk collection of Internet traffic at various top-tier "choke points" in the Internet backbone.[16] This paper does not intend to comment on the ethical implications of dragnet surveillance; however, what is important to recognize is that *Canadians do not have rights as protected citizens under US law*. While their data are passing through US networks, regardless of whether they *intended* to communicate with a US entity or not, they are foreigners subject to near-zero protections, outside of the legal jurisdiction of Canada. As Obar and Clement note:

> ...the IXmaps research makes visible a widespread phenomenon we call 'boomerang routing' whereby Canadian-to-Canadian internet transmissions are routinely routed through the United

[13] Castells, "The Space of Flows."
[14] Floridi, *The Fourth Revolution*, 119.
[15] Ibid., 119.
[16] Clement and Obar, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance," 15.

> States. Canadian originated transmissions that travel to a Canadian destination, but via a U.S. switching centre or U.S. carrier, are subject to U.S. law — including the USA Patriot Act and FISAA. As a result, Canadian-to-Canadian internet transmissions that boomerang expose Canadian communications to potential U.S. surveillance activities – a violation of Canadian network sovereignty.[17]

In proposing ways to regain this network sovereignty, Obar and Clement propose legislative and technical solutions. They call for a strengthening of Canadian privacy laws, namely the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which would result in greater transparency, accountability, and enforcement powers behind the law, which was created to provide baseline data protections to Canadian citizens when sharing information with private companies. Obar and Clement suggest that such a strengthening of the law "should be implemented with a focus on data collection and management practices, including routing behaviours[18]". Their technical solution is to "repatriate internet traffic by building more Canadian Internet exchange points", namely, to solve the boomerang routing problem by building domestic networks that will be selected by BGP and other Internet routing protocols. They quote the president of the Canadian Internet Registration Authority Byron Holland, who remarked that "by building a robust Canadian Internet infrastructure, including a nation-wide fabric of IXPs [Internet exchange points], we can ensure more Canadian traffic stays in Canada, and is therefore only subject to Canadian law.[19]".

A similar example of the network sovereignty problem has appeared in Germany, and, to an extent, in the rest of the EU. German Chancellor Merkel and French President Hollande met in 2014 to discuss ways to "maintain a high level of data protection" in regards to knowledge of NSA surveillance of EU countries over international networks. This came after Deutsche Telekom, one of the major internet service providers in Germany, announced plans to begin work on a 'national internet' that would ensure any domestic data sent on it remained in Germany.[20] The technical details of their plan are vague, but such a system could be implemented by imposing constraints on BGP and other inter-Autonomous System routing protocols: If all German ASes know who the other German ASes are, they can be configured to only keep sensitive information within the internetwork of German providers.

Distributed Morality and Infraethics

Both aforementioned scenarios present ethical situations in which multiple agents are at work. The various technical, bureaucratic, and statal governing agents mentioned at the start of this section form what Floridi calls a *Distributed Morality* (DM), a moral situation in which actions from various agents, each made independently without necessary moral worth, work together to trigger a moral action at a higher level of abstraction. He describes DM with an example where Alice only knows that 'the car is in the garage or Carol has it' while Bob only knows that 'the car is not in the garage.'[21] Here neither agent knows that Carol has the car, but the *supra-agent* 'Alob' does. Floridi's continues: "The question about 'distributed morality' is this: can 'big' morally loaded actions (in this case, Alob's actions) be caused by many, 'small', morally neutral or morally negligible interactions (in our example, Alice's and Bob's actions)? I hold the answer to be yes."[22]

In the network sovereignty cases, we can identify a few different agents at work:

[17] Obar and Clement, "Internet Surveillance and Boomerang Routing," 3.
[18] Ibid., 7.
[19] Ibid., 8.
[20] Dohmen and Traufetter, "Spy-Proofing."
[21] Floridi, *The Ethics of Information*, 262.
[22] Ibid., 262.

- (A) Nations (e.g. Canada, Germany) establishing laws governing how their citizens' data be treated, providing legal grounding for an individuals' fundamental rights, and possessing enforcement powers within their sovereign territory
- (B) Internet service providers and other operators of Autonomous Systems, complying with the laws of the country they physically reside in, and behaving according to agreed-upon Internet protocols
- (C) Routers, autonomously and algorithmically sending messages from one host in the Internet to another, and determining the optimal way to route data across multiple networks

Similar to Floridi's example, these agents pose no immoral intention with their actions. But when paired with a fourth agent (D), a nation that conflicts with other agents' intentions in the way it handles data (e.g. the United States), agents B and C become complicit in facilitating an immoral action, and A is unable to effectively influence the situation. The key here is that this change happens with the introduction of a new agent, not with a change in intention of any preexisting agents. For Floridi, in such a system, "we cannot rely on a system of moral evaluations based on intentionality or motive-related analysis[...]we need to evaluate actions not from a sender but from a receiver perspective: actions [...]are assessed on the basis of their impact on the environment and its inhabitants."[23]

In discussing how to influence a distributed moral situation, Floridi suggests that in addition to improving ethical systems of incentives and disincentives, and redesigning the way in which people interact with technological and moral 'aggregators', he calls for infrastructural change: "it seems that part of the solution will also depend on the development of social and technological infrastructures[...] that will foster the right sort of distributed morality."[24] He goes on to call for a new *infraethics*: the development of "environments that can facilitate ethical choices, actions, or process."[25] Infraethics are the 'pipes' by which ethical actions can be carried; the 'meta-technologies' that can facilitate the development of moral technologies. For Floridi, "an infraethics is not morally good in itself, but it is what is most likely to yield moral goodness if properly designed and combined with the right moral values."[26]

Code

Infraethics provides a model which suggests that by changing underlying *technologies* in the Internet, the infosphere can be made a more ethical space. It follows that a solution to the network sovereignty problem ought to explore ways to infraethically strengthen the Internet. Unfortunately, "the problem is how to design the right sort of infraethics":[27] Using the Internet as a infraethics-forming meta-technology requires understanding how to regulate and transform the Internet as a technology.

In analyzing the development and nature of the Internet, various individuals point to *software* as the infosphere's native regulatory mechanism—that changing the rules on agent C in our system is the best way to influence the DM. This follows the thinking of Dodge and Kitchin in their discussion of software code as it relates to space, referring to communication via the Internet as "a transduction wherein the relational problem cannot be solved without code. Here, code dominates the transduction of space to the extent that the transduction is dependent on code."[28] Selinger and Hartzog[29] similarly refer to efforts

[23] Ibid., 265.
[24] Ibid., 271.
[25] Floridi, *The Fourth Revolution*, 190.
[26] Ibid., 190.
[27] Ibid., 190.
[28] Kitchin and Dodge, "Code and the Transduction of Space," 172.
[29] "Obscurity and Privacy."

by policymaker and companies to create so-called "privacy-by-design" technologies [p. 16]. Speaking to the regulatory power of software, Lessig[30] invokes the phrase 'code is law':

> In real space, we recognize how laws regulate——through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different "code" regulates——how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's "law." "Lex Informatica," as Joel Reidenberg first put it, or better, "code is law."

Returning to some of the technical specifications of Internet routing in the above sections, various technologies have been proposed to change the way the Internet can work, helping solve the network sovereignty problem. Computer scientists at Princeton developed a routing protocol called *MIRO* (Multi-path Interdomain ROuting),[31] which extends BGP to provide a routing framework that grants individual ASes more flexibility in how packets are routed between them. BGP provides no mechanism for an AS to disseminate alternative pathways, which "limits each router to using a single route[...]which may not satisfy the diverse requirements of end users."[32] In response, MIRO allows an AS to discover multiple routes to a destination on the Internet, and select a pathway of its choosing, allowing (among other things) for an AS to "choose paths that satisfy their special needs, for example: avoiding a specific AS for security or performance reasons". This kind of technology may be similar to what Deutsche Telekom hinted at in the creation of their 'national internet'. What's significant about it is that it doesn't reduce an agent's ability to be hostile—the protocol could be spoofed and manipulated by enemy Internet entities—but it provides for an infraethics, by serving as a technology that, if implemented, would allow other routing technologies to make ethical routing decisions. One can envision the major Canadian ISPs (perhaps compelled by the Canadian government) using a protocol like MIRO to give users the choice of keeping sensitive data domestic.

An *a posteriori* method of controlling Internet pathways similarly allows users to avoid hostile ASes. A team of researchers at the University of Maryland created *Alibi routing*: software that can runs independently of routing protocols which proves that a given Internet packet never entered a designated geographic regions. The technique involves sending packets through a trusted router called an 'alibi': "a relay that is so distant from the forbidden region that transiting both would induce noticeably high delays."[33] By calculating the time it would take information traveling at fiber-optic speeds (about 2/3 the speed of light) to reach the alibi *and also* reach the forbidden region, an upper boundary can be established for 'safe' transmissions. If a packet was delivered through the alibi to the destination sufficiently below that upper bound, then it would be impossible for the data to have entered the forbidden region—the time would be insufficient for the packets to have traveled there. Utilizing "the fact that, while an attacker can lie about having greater latency to a victim, it cannot lie about having lower latency than it really has", and that "information cannot travel faster than the speed of light", they conclude that "these standard apparent impossibilities are sufficient for allowing many source-destination pairs to provably avoid various countries."[34]

One fundamental limitation of the technology "is that it places the onus on users to determine where in the world their attackers are. As such, we expect Alibi Routing to be used mostly for avoiding large, very powerful adversaries."[35] This suits Alibi routing perfectly for being a technical solution for furthering gains in network sovereignty. An Internet where such a technology is widely used would serve as a

[30] *Code and Other Laws of Cyberspace*.
[31] Xu and Rexford, *MIRO*.
[32] Ibid., 36:1.
[33] Levin et al., "Alibi Routing," 613.
[34] Ibid., 614.
[35] Ibid., 614.

meta-technology, providing a means for ICTs to better ensure their users' privacy. Such a technology then becomes part of an infraethics which allows for moral actions at a higher level of abstraction in the infosphere.

Floridi, in describing privacy within his ethics, remarks that "At each of these three stages [data generation, storage, and management], solutions to the problem of protecting privacy can be not only self-regulatory and legislative but also technological."[36] Creation and adoption of these technologies, along with policy and institutional change, will provide the incentives, disincentives, and 'moral enablers' that make up a Distributed Morality.[37] The ethical potential of Internet-based ICTs exists; the infrastructural and regulatory means have yet to be fully developed. Reidenberg[38] summarizes this well, remarking that

> "Despite the popular perception, the global information infrastructure ("GI") is not a lawless place. Rather, it poses a fundamental challenge for effective leadership and governance. Laws, regulations, and standards can, do, and will affect infrastructure development and the behavior of GII participants. Rules and rule-making do exist. However, the identities of the rulemakers and the instruments used to establish rules will not conform to classic patterns of regulation" [p. 1].

It is with this inspiration that the work to produce an infraethical infosphere continues.

References

Castells, Manuel. "The Space of Flows." In *The Rise of the Network Society*, 407–59. Wiley-Blackwell, 2010. doi:10.1002/9781444319514.ch6.

Clement, Andrew, and Jonathan A. Obar. "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Response to Privacy and Network Sovereignty Challenges." In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, by Michael Geist, 350. University of Ottawa Press / Les Presses de l'Université d'Ottawa, 2015. http://www.oapen.org/record/569531.

Comer, Douglas E. *Computer Networks and Internets*. Prentice Hall Press, 2008.

Dohmen, Frank, and Gerald Traufetter. "Spy-Proofing: Deutsche Telekom Pushes for All-German Internet." *Der Spiegel*. http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spyi
html.

Floridi, Luciano. *The Ethics of Information*. OUP Oxford, 2013.

———. *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality*. Oxford University Press, 2014.

Floridi, Luciano, Sylvie Kauffman, Lidia Kolucka-Zuk, Frank La Rue, Sabine Leutheusser-Schnarrenberger, José-Luis Piñar, Peggy Valcke, and Jimmy Wales. "Advisory Council to Google on the Right to Be Forgotten," 2015. https://www.google.com/advisorycouncil/.

Kitchin, Rob, and Martin Dodge. "Code and the Transduction of Space." *Annals of the Association of*

[36] Floridi, *The Fourth Revolution*, 113.
[37] Floridi, *The Ethics of Information*, 269.
[38] "Governing Networks and Rule-Making in Cyberspace."

American Geographers 95, no. 1 (2005): 162–80.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. Vol. 3. Basic books New York, 1999.

Levin, Dave, Youndo Lee, Luke Valenta, Zhihao Li, Victoria Lai, Cristian Lumezanu, Neil Spring, and Bobby Bhattacharjee. "Alibi Routing." In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 611–24. ACM, 2015.

Obar, Jonathan A, and Andrew Clement. "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty." In *TEM 2013: Proceedings of the Technology & Emerging Media Track-Annual Conference of the Canadian Communication Association (Victoria)*, 2012.

Philpott, Dan. "Sovereignty." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Summer 2014., 2014. http://plato.stanford.edu/archives/sum2014/entries/sovereignty/.

Reidenberg, Joel R. "Governing Networks and Rule-Making in Cyberspace." *Emory LJ* 45 (1996): 911.

Rekhter, Y, T Li, and S Hares. "RFC 4271." *Internet Engineering Task Force, Http://www.rfc-Editor.org/rfc/rfc4271.txt* 6 (2014).

Selinger, Evan, and Woodrow Hartzog. "Obscurity and Privacy," 2014.

Xu, Wen, and Jennifer Rexford. *MIRO: Multi-Path Interdomain Routing*. Vol. 36. 4. ACM, 2006.

Zuckermann, Ethan. "New Media, New Civics? My Bellwether Lecture at the Oxford Internet Institute," 2013. http://goo.gl/wJMFHG.