The Unlawful Freedom of Communication

Oxford Internet Institute
September 2010

Michael Markwick
markwick@sfu.ca
School of Communication
SIMON FRASER UNIVERSITY

Abstract

Is the Internet a *polis* or is it a camp? From the desperate revolution by Twitter on the streets of Tehran to Obama's web 2.0 electoral triumph, the communication devices in our hands today and the exponentially more powerful devices to come promise a new era of political mobilization. These devices will allow us to know our own minds and act as a body politic in breathtaking ways. Against this temptation to triumphalism stands the transnational project of wiring these same devices for ubiquitous, unblinking state surveillance.

This paper examines the agenda of the Government of Canada, in lock step with its international partners, to convert all personal communications technologies into a latent, ubiquitous surveillance system. *The Unlawful Freedom of Communication* shows how Canada's "lawful access" agenda advances the rise of the surveillance regime in the United States, the United Kingdom and the European Union, and is part of a contest—web 2.0 against "Stasi 2.0"—that will decide whether the digital revolution's promise of a new birth of freedom may in fact be stillborn.

The paper provides a concise treatment of an edited volume the author is developing for UBC Press. It applies Giorgio Agamben's biopolitics and Jacques Derrida's deconstruction to determine, on a close reading of the "securitization" of the Internet, what Politics and Policy are making of the practice of democratic citizenship.

To govern the Internet is to govern people. As we entwine communication technologies with every aspect of our lives, and advocate universal access to these technologies against the "digital divide" as a necessary condition for human flourishing, we expand the power of Internet governance to govern us. The communication devices in our hands today, and the exponentially more powerful tools to come, may play as epochal a role in our development as persons as the home itself—integral to the formation of one's identity, powerful sites for the relationships that give substance to personality and meaning to life. These devices— from the faltering spark of the revolution by Twitter on the streets of Tehran to Obama's web 2.0 electoral triumph, from the discontent of many behind the Great Firewall of China to Wikileaks and the war in Afghanistan—may bring a quantum change in our ability to interrogate and contend with the power of the state, to bring the genius of peaceful democratic scrutiny against sovereign power's monopoly over violence. Even as they may allow all of this, the communication devices that make the Internet ubiquitous also allow sovereign power to embed itself in our lives in the name of our emancipation from perils of every kind. They allow sovereign power a capability that has proven elusive throughout its history, the ability to identify, observe and control the subject from the inside out. Where Giorgio Agamben uses the term "sovereign power" to mean governance as a whole (Agamben 1998), I believe there is much to be gained in using it specifically to scrutinize the role of Internet governance in the expansion of the "security regime" (Young 2003)—the rise of the executive branch over the other branches of government in the aftermath of 9/11. To borrow from Agamben, the intimacy of twenty-first century communication technology allows sovereign power to name us as bare life, perfecting its project of the total administration of life. I argue that

markwick@sfu.ca

this is the biopolitical effect of Internet governance as revealed in Canada's "lawful access" agenda. In "lawful access" governance of the Internet shows itself to be inseparable from the security regime as such; it is an exercise of sovereign power that seals the difference between the Internet as a *polis* and the Internet as a camp. Recognizing the freedom of human communication afforded by the Internet, the security regime makes this freedom unlawful.

It is a well established rule in Canadian constitutional law that one's ability to safeguard "a biographical core of personal information […] from dissemination to the state" is integral to the protection of "dignity, integrity and autonomy"; this is a defining feature of a free and democratic society. (R. v. Plant 1993 3 S.C.R.) In the first part of this paper I will map the Canadian government's agenda for the "modernization" of "lawful access", with a view to exploring the tension between this constitutional rule and the future of Internet governance in Canada. "Lawful access", as contemplated by the executive branch and its official opposition, would bring to Canada measures that are already entrenched in Great Britain, the United States and Australia, allowing Canadian ratification of Europe's Convention on Cybercrime. In mapping this agenda, my specific concern is that "lawful access" will convert Canada's civilian communication system, principally the Internet as it is now and as it evolves, into a latent and ubiquitous surveillance system. It would require the private telecommunications sector to ensure all of its devices and systems are engineered for surveillance, and compel the sector to collaborate covertly with trade, police and intelligence officers; it would reduce the standards for judicial oversight and, in crucial areas, eliminate judicial oversight altogether; it would facilitate the collaboration

between Canadian and foreign officials even as the executive branch's "maintenance of foreign confidences" is shielded from democratic and judicial scrutiny (Charkaoui v. Canada (Citizenship and Immigration), 2007b); it would have a wide range of application, from non-criminal matters to serious offences-in-the-making of terrorism and other forms of organized crime. The government seeks this expansion of powers without adducing why it is demonstrably necessary and proportionate to any risks to Canadians presented by the Internet.

Fundamentally, the protection afforded by the *Canadian Charter of Rights and Freedoms* against unreasonable search and seizure is an attempt to establish a firewall—by turns liberal and contingent in the hands of the Supreme Court of Canada—between the human person and sovereign power. My purpose in the second part of the paper is to unpack the idea of sovereign power as it applies to the project of Internet governance in "lawful access". Specifically, I believe Agamben's bleak assessment of our biopolitical situation with respect to the powers of the state should provoke a re-assessment of our ideas of privacy rights and democratic deliberation. The Internet is not neutral in its impact on our capacity and appetite for democracy; its impact on our political culture is in no sense virtual. At the risk of being demoralizing, I will propose vivisection and vivification as two forms of sovereign power that are shaping the architecture of the Internet in Canada with respect to the possibilities of privacy and democracy. The exercise of these powers articulates governance of the Internet as a "state of exception", the constitutional abrogation of fundamental freedoms.

It is of course little consolation to anyone living in a camp to state the obvious, that they are stripped of personhood and reduced to bare life. The point, to use Marx's riposte to Feuerbach, is not interpret the world but to change it. I will conclude the paper with a look at how Alain Badiou and Jacques Derrida might get us there. To what extent, if any, can governance of the Internet support the practice of politics as "a truth procedure"; to what extent can the lives we lead online open a path to the "democracy to come"?

Lawful Access

In the strictest sense, the phrase "lawful access" evokes one of the oldest principles of Canada's constitutional order, a heritage signified powerfully this year when Elizabeth, the Queen of Canada, laid a stone from Runnymede as the cornerstone for the Canadian Museum of Human Rights. Her gesture, seven hundred and ninety-five years out from King John's signing of the *Magna Carta*, articulated on Canadian soil that the sovereign is not above the law.[1] This is elementary civics, but the salient clause of that document bears repeating:

> No free man shall be seized or imprisoned, or stripped of his rights or possessions, or outlawed or exiled, or deprived of his standing in any other way, nor will we proceed with force against him, or send others to do so, except by the lawful judgement of his equals or by the law of the land. To no one will we sell, to no one deny or delay right or justice. (1215)

[1] The Queen's timing was apposite. Weeks before her arrival, the Supreme Court—after what appears to have been something like a pointed internal debate—found no constitutional protection for the confidentiality of journalistic sources. (2010b. "R. v. National Post, 2010 SCC 16." In CanLII: Supreme Court of Canada.) Months earlier, the Court censured minority Prime Minister Stephen Harper for violating the rights to liberty and security of the person of Omar Khadr while, at the same time, confirming his power to leave unchallenged Khadr's interrogation and detention by U.S. authorities in Guantanamo Bay. (2010a. "Canada (Prime Minister) v. Khadr, 2010 SCC 3." In CanLII: Supreme Court of Canada.)

The sovereign's access to the person, rights, standing and possessions of a "free man" must be lawful. This feudal provision might not have been intended to be an immutable constitutional principle, but it has become a point of demarcation between a free, democratic society and despotism. This suggests an historical moment that is quite different from Agamben's understanding of our current biopolitical condition. He defines the "state of exception" as a constituent feature of sovereign power—the ability of the sovereign, at its sole discretion, to decide when the law should apply and when it should be suspended. (Agamben 2005) It describes the sovereign's unique prerogative lawfully to suspend the rule of law. I believe something different was at work at Runnymede. The *Magna Carta* enshrined the right of the barons, "with the support of the community of the land", to use whatever means necessary against the Crown if it failed to redress within forty days a duly constituted grievance. The barons could suspend their oath of loyalty to the sovereign, their consent to be governed, if they found themselves subject to an unlawful condition. In this way, the state of exception worked *against* sovereign power, albeit for an elite cadre of the nobility; this state of exception prevented the actions or words of the sovereign from being law in its own right, acting as an absolute limit point to the scope of the Crown's power.

King John's Runnymede is a far distance from twenty-first century Canada, because there is little possibility now of a state of exception that might work against sovereign power. The imaginary of Canada today, as advanced by the governing Conservatives and the Liberal government-in-waiting, is of a nation that must prevent the Internet from becoming an existential threat in the hands of terrorists and gangsters. In order to ensure

the constitution, from the *Magna Carta* to the Canadian *Charter*, is not "a suicide pact", the norm of "lawful access" can no longer point to an absolute limitation on sovereign power; it must point to the opposite. Especially in matters where national security is concerned, the consent of the governed must give way to the muscle necessary to ensure the security of our bodies, our capital and infrastructure—our way of life—against people who mean us harm. This line of reasoning has something of an Orwellian effect on the phrase "lawful access". Instead of signifying a restraint or absolute limit, it describes the expediency of sovereign power, the processes and measures that hardwire the state of exception into Internet governance; it is the new normal, the best approximation we can have—given the gravity of the dangers we face—of a free and democratic society. It establishes as a condition for our survival that our communication devices along with the private industries that design, support and sell them to us must be, from now on, integrated seamlessly in a system that makes state surveillance intrinsic to the Internet.

The security regime generally has had little difficulty in ensuring the rapid passage of anti-terrorism legislation. Pointing to the United States, Iris Marion Young suggests this is because the aftermath of 9/11 induced not simply a state of submissiveness amongst her compatriots but a predisposition to honour, respect and adore the security regime and its use of "masculinist power" to ensure their safety against "bad men". (Young 2003) Canadian hearts also glowed with patriotic fervour, but any adoration of masculinist power here would have to be studied in the context of our racial and religious diversity. Indeed the experience of uncertainty and otherness in minority communities, the strategy of political campaigners to secure the votes of these communities in a fractious political

climate, and the challenge of calling public attention to the state's spooky powers of surveillance may have caused the governing parties to treat "lawful access" with a degree of caginess. Add to this the tectonic shift the country's party system, and it becomes clear that Young's idea of the security regime is better understood not as monolithic authority but as a dynamic, continual negotiation and consolidation of the powers of the executive branch. To date, both Liberal and Conservative governments have seen their "lawful access" bills die on the Order Paper; the former in 2006, when Paul Martin's government collapsed in the bathos of political scandal, and the latter in 2009 when the present Prime Minister forced the prorogation of Parliament in order to avoid a vote of non-confidence. Despite the bitterness of their rivalry, and notwithstanding signs of dissent on the matter within their respective caucuses, both the government and the official opposition remain determined to see "lawful access" carry into law.

The government and its officials make out their case for "lawful access" by drawing on Canadians' legitimate concerns about preventing the use of the Internet for sexual predation on children and minors. British Columbia's aboriginal communities are particularly vulnerable to this form of *in situ* sex slavery, because of the ready accessibility of web-enabled cameras and high-speed Internet access in many reservations. Indeed the argument for "lawful access" as a policing tool predates the argument from anti-terrorism; the nation's police chiefs have advocated these measures since 1995. However, from James Bond to television's Jack Bauer, the prospect of detecting a cabal of terrorists and preventing a devastating attack—passenger airliners converted into mammoth cruise missiles at the point of a utility knife, a dirty bomb lodged in a shipping container on a

Vancouver dockyard—remains powerfully seductive in our culture of fear. In all of this, the government never advances evidence to show how the scale of change envisioned in "lawful access", the conversion of the private telecommunications sector and its systems into the machinery of state surveillance, is in any way a proportionate and effective answer to the threats we face. It offers instead the tropism of the first class letter.

By the book, in order for there to be a reasonable expectation of privacy a person must be able to control access to the site in question. Be it a home, a hotel room or a locker in a bus depot, the Supreme Court hinges much of the constitutional right to be free from unreasonable search and seizure on whether one has the ability to admit or exclude others. This is what the envelope does for a first class letter. It separates the content of the letter from the information necessary to convey it through the mail, and secures the content from the eyes that must read the envelope. The government bases its proposed new governance of the Internet in Canada on this paradigm, a clear delineation between the content of our communications and the "tracking data" and "traffic data" necessary to move them through cyberspace. The crucial assumption here is that the Internet will continue to allow for our personal communications what folded paper and paste did for the first class letter, that the technology will preserve our ability to admit or exclude others. This assumption cannot hold, since one of the core purposes of "lawful access" is to ensure the ongoing development of the Internet in Canada will always enable the agents of the state, and their foreign counterparts, to gain access to our communications without our knowledge or consent.

The purpose of the first class letter analogy is to make palatable the state of exception "lawful access" would bring to governance of the Internet. Where the Supreme Court has named protection of our ability to keep from the state the "biographical core of personal information" as a necessary condition for a free and democratic society, "lawful access" would abrogate this constitutional norm citing the exigencies of fighting everything from questionable trade practices (and perhaps copyright infringements) to biker gangs and Al Qaeda. Even so, the defining innovation of web 2.0, and a guiding principle for the new architectures of the Internet, is the power it gives us to make this biographical core a point of contact, dynamic and vital, with friends and collaborators anywhere on the surface of the planet. Where the first class letter allowed one to express a discrete aspect of one's personality to a limited audience a hemisphere away, perhaps to see this mote of personality preserved for a future reader, the Internet allows incomparably greater power for the intimacy and reach of personal communication. The envelope is the content. We live this "biographical core of personal information" dialogically, testing and growing our understanding about what it means to be oneself, what it means to be human, in the complexities of our core beliefs about life, our sexuality, our racial and cultural identity—the innermost aspects of personality lived with others, in a dynamic communion, online. The websites we visit, the photos, videos and tweets with share with each other, the places we frequent with an iPhone shunted into our social lives and the proximity of these devices to the smart phones of everyone else in the vicinity, the patterns discernable in whom we email and when, the files we upload to a computer cloud or download from a torrent are part of a constant aura of the biographical core of personal information that bleeds out into an Internet designed never to forget. Indeed,

long after the memory of an evening—be it a moment of sublime spiritual insight at a chapel or a mosque, or a somewhat less savoury experience in the booth of a nightclub—has faded, the digital imprint of any aspect of that moment that we have registered in some fashion online will remain afloat in a data stream, giving testimony to what kind of person we were likely to have been in that moment. This is precisely the kind of data—core biographical information—that "lawful access" would claim, as a state of exception from a free and democratic society.

In this state of exception, trade officials along with police and intelligence agents would have the power, without judicial supervision, to issue "preservation demands" to our telecommunications service providers. These demands will oblige the service providers to keep intact for up to twenty-one days all data—"data that can be processed by a computer"—concerning our online activities. (Valiquet 2009) Designated officers within these agencies, except in exigent circumstances when any officer would have the same powers, will have the authority to obtain without a warrant "basic" information about us from our service providers, including our names, IP addresses and, presumably, whether we tend to use any encryption devices. Canadian officers could effectively lend these broad powers to their foreign counterparts, acting for them within the borders of Canada.

The state of exception recasts the role of the judiciary, setting the standards of scrutiny so low that they amount to an administrative hurdle more than a judicial restraint on government agents. Basing their judgements on a (heretofore rare) "reasonable grounds to suspect" that an offence has or will be committed, rather than the more stringent and

common "reasonable grounds to believe", "lawful access" enables judges to accede to the requests of trade, police and intelligence officials for preservation orders, which would bind telecommunications providers for ninety days, and production orders. The difference between a production order and a warrant is that the party who possesses the information sought by the order must surrender it on demand; law enforcement officials would not have to enter the premises, search for the information and seize it themselves. Production orders would empower the officials to obtain historical data about online activities, including the date, time and duration, size of attachments, origin, destination and parties to a communication. (Valiquet 2009) The officials would require a warrant to track these communications in real time and obtain the content, except in exigent situations. "Lawful access" broadens Canada's wiretap laws, empowering law enforcement officials to obtain warrants for the remote activation of systems already in place in smart phones and many vehicles such as GPS navigation systems, cameras and microphones. Again, Canadian officials can lend these powers to foreign law enforcement and intelligence agencies, participating in their investigations by being their hands and feet on Canadian soil.

At the same time, the government proposes exempting private communications systems—where these are run solely for the use of the members of the same household or business—from compliance with "lawful access". The effect of this exemption would create a two-tiered Internet in Canada, granting organizations that have the means—ranging from oil companies to the Hell's Angels—licence to build surveillance-free systems.

Nothing in "lawful access" prevents a telecommunications service provider from voluntarily surrendering to law enforcement officials information within its control and access to its systems. Indeed, it seems entirely within the purview of the ministers responsible for regulating, subsidizing and taxing the telecommunications sector to provide incentives to foster closer, voluntary collaboration with law enforcement. There's something of a political economy at work in such arrangements, as shown in the relationships between Microsoft, Google and the Communist Party of China, and the pressures brought to bear on RIM by the United Arab Emirates, Saudi Arabia, Turkey and India to ensure Blackberry devices comply with domestic morals and surveillance standards; access to markets can be a powerful motivator for voluntary partnerships between the private telecommunications sector and the security regime.

At the same time, "lawful access" imposes on telecommunications providers a strict obligation of "confidentiality": under no circumstances can they share with their customers any information concerning the interest government officials have shown in their activities. The private sector thus becomes an instrument of sovereign power, lending its capital, expertise and infrastructure to the projects of the security regime and also, crucially, the relationships it cultivates with its subscribers. These relationships can be forms of devotion, with subcultures and whole generations branding themselves with their devices—iPads, iPhones and iMacs as icons of hip consumerism. In this way, Apple Computer gives the security regime a depth of reach Orwell could not have imagined for Big Brother, an array of continually fresh and ever more powerful devices that we embrace as tools for emancipation, an operating system for the existential work of

discerning and expressing identity. The telecommunications sector as a whole becomes something greater than the Ministry of Love. It internalizes the imperative of state surveillance, and creates beautiful devices that serve the security regime's biopolitical power of identification as effectively as they serve our needs as consumers.

The standards "lawful access" and its cognate initiatives in other jurisdiction bring to Internet governance make the biopolitical power of identification, the imperative of surveillance, a mandatory feature of telecommunications, the tipping point to web 3.0.

A Biographical Core of Personal Information

The surveillance capability of the security regime, especially when it is made intrinsic to the Internet, presents a challenge to the ways we understand democracy and privacy. The Supreme Court of Canada contemplates something similar when it affirms the constitutional right to be free from unreasonable search and seizure is grounded in both the norms of a free and democratic society and the primacy of human dignity. What is at issue here—a tension at least as old as the *Magna Carta*'s protection of the "standing" of the "free man"—is the integrity of personhood before the power of the state. Agamben argues that, in the biopolitics of our moment in history, sovereign power acts as both the origin and guarantor of our status as persons, and in this role always holds in reserve the power to reduce us to "bare life". (Agamben 1998) This leaves us with an inversion of the Aristotelian maxim that we are "born for citizenship"; we are all refugees. (Aristotle and Ross 1954) There is, he contends, no turning back from this condition, no possibility of return to the classical politics in which the state is constituted by the citizenry.

Assurances of constitutional rights and safeguards against the power of the state only serve to reinforce the state of exception—like a hapless gambler in Vegas, there's no beating the house. There are signs of the bleak truth of this in the security regime and its project of Internet governance, because under the gaze of the state—a gaze turned on us without our knowledge or consent, a gaze inextricable from our communication devices—we are neither persons nor citizens, we are bare life, digital organisms. Faced with this assessment of our situation, my aim in this section is to make something of a Kierkegaardian leap; I want to deconstruct sovereign power as applied to state surveillance because I cannot accept that our situation is ineluctable. Personhood endures even in a concentration camp. Analyzing the sovereign powers of vivisection and vivification will, I hope, suggest ways to think about the primacy of human dignity in Internet governance especially with respect to democracy and privacy.

Maher Arar's experience of the security regime is an iconic example of vivisection as a species of sovereign power. U.S. authorities detained Arar, a Canadian citizen of Syrian descent, one year after 9/11 as he made his way through New York City after vacationing in Tunis. In October 2001, officials in the RCMP's anti-terrorism team had advised their U.S. counterparts to place Arar and his wife, Monia Mazigh, on a border control "lookout" list, alleging without evidence of any kind that they were Islamic extremists with ties to Al Qaeda. (O'Connor 2006) They interrogated him, and instead of returning Arar to Canada they flew him to Jordan where they rendered him into the hands of Syrian officials. Senior officials of the Canadian Security Intelligence Service (CSIS) reported that this was to allow the Americans "to have their way with him." The Syrians placed

Arar in the hands of torturers in the notorious Far Falestin Prison. "We went into the basement," Arar recalls,

> and they opened the door, and I looked in. I could not believe what I saw. I asked how long I would be kept in this place. He did not answer, but put me in and closed the door. It was like a grave. It had no light. It was three feet wide. It was six feet deep. It was seven feet high. [...] I spent ten months, and ten days inside that grave. (Maher Arar quoted in Webb 2007)

Arar was one of four Canadians to be treated this way, all of them tortured to corroborate information the Syrians obtained from U.S. and Canadian authorities.[2] In one case, emblematic of all the rest, this meant "being treated to a stripping down to his underwear, pouring cold water over him, and intense beatings with what he described as a 'black electric cable roughly one inch thick.'" (Toope 2005)

Alain Badiou might find in the ordeal of Maher Arar, and in the commission of enquiry struck in the first month of Paul Martin's brief tenure as prime minister, an instance of politics as a "truth procedure". In the meticulous work of the enquiry's chair, Mr. Justice Dennis O'Conner, through one hundred and twenty seven days of public hearings and more days of *in camera* proceedings, the facts of Arar's vivisection confronted the "errant superpower" of the security regime. It gave shape to the otherwise unimaginable excess of the powers of the security regime over life as such, over human personality, to reveal how Arar—and by implication all of us—are "held hostage", to use Badiou's phrase and, in Agamben's, reduced to bare life. "The State", Badiou asserts,

[2] Responding to a recommendation of the Arar Commission, the government struck the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin under retired Supreme Court Justice Frank Iacobucci. This Inquiry has proved controversial, with Almalki, Abou-Elmaati and Nureddin complaining that it was held "in almost complete secrecy", excluding them, their lawyers, the public and the media from its proceedings.

> is in fact the measureless enslavement of the parts of the situation, an enslavement whose secret is precisely the errancy of superpower, its absence of measure. Freedom here consists in putting the State at a distance through the collective establishment of a measure for its excess. And if the excess if [sic] measured, it is because the collective can measure up to it. (Badiou 2005)

In his scathing and correct indictment of the RCMP and CSIS, O'Connor took the measure of the human impact of the broad surveillance powers of Canada's security regime; he set out in detail how the agencies performatively stripped Arar of his standing as a Canadian citizen, making it possible for U.S. authorities to entomb him for thirteen months in a fetid subterranean cell and subject him to the ministrations of Syrian torturers.

This process of meticulously laying bare something of the inner workings of Canada's anti-terrorism bureaucracy discomfited the executive branch, resulting in a relationship between the Commission and the government some observers describe as "confrontational and at times antagonistic". (Whitaker 2008) Stephen Harper assumed the role of prime minister, forming a minority government in 2006, just as O'Connor prepared to release the first volume of his findings, a comprehensive statement of the facts at issue in Arar. Continuing a challenge initiated by their Liberal predecessors, the Harper Conservatives brought an application to the Federal Court under the *Canada Evidence Act* to have approximately fifteen hundred words redacted from O'Connor's first report, arguing disclosure of this material would be "injurious to international relations, national defence, national security" and the "Canadian way of life". The Arar Commission prevailed, with the Federal Court ruling that the maintenance of foreign confidences and national security cannot be used as pretexts to shield the government from anything it might find "critical or embarrassing". (2007a)

Uncensored by court order, the O'Connor report reveals the RCMP, in seeking search warrants against Maher Arar, failed to disclose to the presiding judge that the information they presented to the court was obtained by means of torture, originating from a country with a deplorable human rights record. The Mounties also concealed information when they sought a warrant to tap Arar's phone lines. Paul Cavalluzzo, counsel to the Arar Commission, denounced this practice as an affront to judicial independence, especially since national security warrants—like the preservation orders, production orders and warrants contemplated in "lawful access"—are heard in a closed courtroom forcing judges to rely exclusively on the information adduced by the police and intelligence officials. (Tibbetts 2007) RCMP investigators, without a warrant and acknowledging they had no grounds for a warrant because Arar was not the subject of a criminal investigation, obtained a copies of his rental application and lease agreement in October, 2001. (O'Connor 2006) These documents listed Abdullah Almalki as an emergency contact; with this as their evidence the RCMP drew the FBI's attention to Arar, initiating the cascade of events that exposed him to the full brunt of powers, the "dark side", George Bush had granted his officials by executive order in waging the *war on terror*.

The expansion of surveillance powers as contemplated in "lawful access", and the conversion of our civilian communications infrastructure to make surveillance an intrinsic function of the Internet, must be seen through the lens of Maher Arar's vivisection. There is no mechanism in "lawful access" to allow anyone whose communications have been the subject of a preservation demand or a production order, or whose iPhone has been

activated as a tracking device, to be aware of this surveillance and to challenge it. Instead, "lawful access" would create an extra-judicial reporting mechanism, relegating scrutiny of the exercise of these powers to senior officials within the intelligence and police agencies, federal and provincial privacy commissioners, the Security Intelligence Review Committee and Cabinet. The perverse effect of O'Connor's work in the Arar Commission seems to have been to school the executive branch in how to insulate itself from the truth procedure of a dogged judge. This problem is difficult enough when Canadian authorities are the sole investigators, but it swells to a Kafkaesque obscenity when foreign agencies are involved. For this reason, "lawful access" is the antithesis of the "truth procedure" Badiou contemplates; it masks the surveillance powers of the state by making them inherent in our communication technologies even as it increases geometrically the magnitude of the security regime's "errant superpower".

I believe Arar's experience of the security regime should provoke a reconsideration of much of what we have come to understand about the right to privacy, and what this means for governance of the Internet. Arar throws into sharp relief the doctrine of the Supreme Court of Canada that privacy is about the protection of "a biographical core of personal information", because it shows how manifestly unequal we are to the challenge of protecting ourselves; the aim of "lawful access" is to remove our knowledge of and control over who has access to this core. The Court's doctrine, if it is to be meaningful against the imperatives of the *war on terror*, must find deeper roots in the values of human dignity and democracy it claims to advance. Canadians are well advised to pay close attention to the evolution of surveillance powers in Europe, and the rise of what many observers describe as

Stasi 2.0. For example, Arar corroborates Brown and Korff's concerns about the disproportionate nature of Internet surveillance, and how it contributes to a process of de-democratization in what they describe as the "European surveillance society". "The ever-closer relationship between the police and intelligence agencies," they observe

> undermines the fairness of trials against persons accused of being involved in organized crime or terrorism, in that courts increasingly allow effectively secret evidence and evidence from anonymous witnesses to form the basis of conviction. (Brown and Douwe 2009)

For this reason, I believe the preservation of privacy is best understood as a necessary condition for the practice of politics as a "truth procedure" because it speaks to our ability to form the collectivities necessary to expose sovereign power along with its claims to own and administer life as "bare life". Put another way, privacy is a necessary condition for what Aristotle described as "political friendships"; where the security regime would reduce privacy rights to the status of an administrative hurdle in the project of beating back the existential threat posed by terrorists and other gangs, we need an idea of privacy that is part of a richer understanding of the nature and purpose of our communal existence.

I want to turn now to the idea of vivification as a species of sovereign power. By "vivification" I mean the work of the superpower of the State to orient all relationships to itself, to make itself the measure and source of the right and the good, to make its reasons our reasons not by telling us what to think, as the old saw has it, but by telling us what to think about. Vivification describes the way sovereign power simulates as human community, the way it makes the camp appear to be a *polis*. It is the pressure to internalize the logic of surveillance, the impetus to self-censor and at the same time believe that the security regime has only "bad men" under surveillance whilst being grateful for

this protecting gaze. Stephen Harper, when he was leader of the Official Opposition, exemplified this in 2002, castigating the Liberal government for its attempts to secure the release of Maher Arar from Syria by conducting "high-level consultations to defend a suspected terrorist." (McGregor 2006) He would go on, as prime minister, to issue a letter of apology to Arar asserting that all of his suffering took place on the watch of the previous government. Vivification would, in this way, actively suppress the practice of politics as a truth procedure in the name of the better angels of our nature.

James Q. Whitman, in his useful genealogy of the concept of privacy in European and United States law, debunks the idea that only democracies can evince respect for the right to privacy. The European project of privacy rights is to "level up" or extend to the masses the protection of honour in the public square that was once enjoyed exclusively by the nobility. He contrasts France's grounding of privacy rights in respect to the concern in Germany for personhood and dignity. Against the view that the right to privacy in Germany found its legs, as it were, after WWII as a bulwark against a return to Nazism, Whitman asserts "some of the fundamental institutions of the continental law of dignity experienced significant development under the star of fascism." Understood as the law of "Inner Space", he argues the purpose of German privacy law is to allow one freely and self-responsibly to develop one's personality. Privacy, in this sense, was part of the right to free self-realization that the Nazis held was inherent in all Aryans. (Whitman 2004) The right to privacy and the idea of personality that sustained it became boundary or point of exclusion between the justified life of the Aryan elect and the waste life, the bare life, of

everyone else. It became a means of vivification. The state was the guarantor of this right against the grasping ranks of the media and other reprobate gossips.

This is a world apart, Whitman argues, from the idea of privacy in the United States. The locus of the republic's idea of privacy is not the public square but the home, dating back to the Bill of Rights and the curbs it imposed on the powers of the state. He observes this results in an idea of privacy as "a right that inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade." (Whitman 2004)

The idea of privacy as a zone of exclusion plays a powerful role in U.S. jurisprudence and political philosophy. John Rawls' conception of political liberalism, for example, is an immensely influential articulation of the idea that liberty necessarily requires the priority of the right over the good. In modern, pluralist societies, the state must refrain from imposing its own edicts about the nature and purpose of human life; it must instead establish the basic rules necessarily to allow each of us maximal scope in sorting these issues out for ourselves, to define and pursue our own, private life projects. (Rawls 2005) Nevertheless, this masks the fact that the state, as Michael Sandel and other critics have shown, is continually imposing its own understanding of the good as universally normative. (Sandel 1998) Sandel observes the result is an impoverished idea of pluralism because it assures those who are well adapted to the dominant idea of what constitutes a "reasonable comprehensive doctrine" greater latitude and social acceptance for their life plans. The limits of this form of tolerance are set out graphically in Munir Ahmad's

documentation of the ways an enraged public, "a rage shared by law", treated "Muslim-looking" minorities in the months following 9/11. (Ahmad 2004) The right to privacy in the United States, which began as a shield against the powers of the state and evolved into a putative anchor for social pluralism, is also a boundary or point of exclusion separating those who most easily conform to the American way of life from the alien other. In this way, the right to privacy in the United States became a form of vivification rather than a check on the power of the state.

Comparing the laws of privacy in France, Germany and the United States, Whitman argues it is wrong to believe there is one universal idea of what the right to privacy means. Helen Nissenbaum shares this view; she would replace the idea of a universal right to privacy and the public/private dichotomy with a conception of privacy as "contextual integrity". Nissenbaum observes that the sharing of information is a central part of our ability to form relationships, from our personal interactions to our dealings in the marketplace and the state. Instead of a universal standard of what would count as an invasion of privacy, she would instead rely on the norms prevalent in any given society because, barring powerful reasons for change, nothing should unsettle the status quo. Having based her thesis on cultural relativism, she concludes with what amounts to a meta-cultural (if not universal) test as to what would amount to a violation of privacy as contextual integrity:

> […] when violations of norms are widespread and systematic as in public surveillance, when strong incentives of self-interest are behind these violations, when the parties involved are of radically unequal power and wealth, then the violations take on political significance and call for a political response. (Nissenbaum 2004)

I believe these approaches are not well suited to the challenges presented by the security regime in its agenda for governance of the Internet. If politics is a truth procedure, and its aim is to identify the errant superpower of the State, then the truth it reveals cannot be valid just for one culture; it must, as Badiou asserts, be valid universally. It would be small comfort to say to Maher Arar that the impact of state surveillance on his life was troubling with respect to the values Canadians hold at this particular moment in our history. The fact of the injustice inflicted on Arar by police and intelligence surveillance ought to elicit universal condemnation.

Oscar Gandy, drawing on Ellul, observes that there is a tendency of technological systems to justify themselves, to make themselves seem indispensable long before we have weighed the benefits they bring and burdens they impose. This insight goes some way to explaining the disproportionate nature of "lawful access" with respect to the harms it is intended to prevent. In their joint declaration on "lawful access" in 2009, Canada's privacy commissioners observed that the federal government has not presented evidence to support its claims as to the necessity of making surveillance an intrinsic function of communications devices. Such a change would confer upon the state what Gandy describes as the power of identification, with its biopolitical premise that "the identity of any individual can be reduced, captured, or represented by measurable characteristics." He contrasts this with the way we form identity in the exercise of our agency as persons, entering into relationships with each other that shape who we are "beyond the gaze and influence of powerful others." (Gandy 2000) "Lawful access", in its project of making

state surveillance ubiquitous, turns this gaze relentlessly on us; this will change our identity as persons and as a political community.

Ursula Franklin captures the deep systemic nature of this gaze, as part of what she describes as the "real world of technology". With or without "lawful access", the nature of technology is conducive to what I describe as vivification where, in Franklin's words, "the fact that citizens are more stringently controlled and managed is often considered as normal and fundamentally beyond questioning, as a necessary feature of technological societies." (Franklin 1999) This shifts the locus of power, she says; it makes the State a superpower, a biopolitical force immeasurably more powerful than the lives it would orient to itself.

Conclusion

Answering the state of exception in Internet governance, as seen in "lawful access" and its project of making surveillance intrinsic to everything we do online and every communication device we graft into our lives, should provoke a return to core questions about the nature of democracy.

Aristotle's question of why one should live in a political community demands an answer larger than the sound byte nostrums of the security regime's talking points. The purpose of living in a political community is not the Hobbesian goal of preventing our slaughter in the dark, more challenging than avoiding the life "nasty, poor, brutish, solitary and short." The purpose of politics is friendship, to cultivate in ordering the material conditions of our

lives together the conditions necessary for the good life—the practice of virtue for its own sake. The truth procedure of politics must not only take the measure of the powers of the state and their impact on human dignity, it must do so in a way that deepens our political friendship. (Yack 2006)

Jacques Derrida would call this "hospitality", contrasting it to the idea of tolerance advocated by Habermas. Tolerance always holds in reserve the power of expulsion; it is a strategy for containing others. Hospitality for Derrida is a radical openness to the other, the willingness to find in the other a messianic challenge—authoritative, radical and unanticipated—to one's self-understanding and way of seeing the world. (Borradori et al. 2003) On this view, the challenge of Internet governance is to keep it open to the messianic arrival of the other, to build the Internet for reciprocal communication on a human scale, secreted from the corrupting gaze of the security regime. If we exorcised the Hobbesian spirit of "lawful access" and its associated projects worldwide, the Internet would become a threshold for the arrival of the democracy to come.

References

1215. "The Magna Carta." In Treasures in Full, ed. Claire Breay. London: The British Library.
1993. "R. v. Plant." In S.C.R.: S.C.C.
2007a. "Canada v. Canada (Comm. of Inquirt—Arar) [2008] 3 F.C.R." In 2007 FC 766 (CanLII): Federal Court.
2007b. "Charkaoui v. Canada (Citizenship and Immigration)." In 1 S.C.R.: Supreme Court of Canada.
2010a. "Canada (Prime Minister) v. Khadr, 2010 SCC 3." In CanLII: Supreme Court of Canada.
2010b. "R. v. National Post, 2010 SCC 16." In CanLII: Supreme Court of Canada.
Agamben, Giorgio. 1998. Homo sacer : sovereign power and bare life. Stanford, Calif.: Stanford University Press.
Agamben, Giorgio. 2005. State of exception. Chicago: University of Chicago Press.
Ahmad, Muneer. 2004. "A Rage Shared by Law: Post-September 11 Racial Violence as Crimes of Passion." California Law Review 92:1259.
Aristotle and W. D. Ross. 1954. The Nicomachean ethics of Aristotle. London: Oxford University Press.
Badiou, Alain. 2005. Metapolitics. London: Verso.
Borradori, Giovanna, Jacques Derrida and Jürgen Habermas. 2003. Philosophy in a time of terror : dialogues with Jürgen Habermas and Jacques Derrida. Chicago: University of Chicago Press.
Brown, Ian and Korff Douwe. 2009. "Terrorism and Proportionality of Internet Surveillance." European Journal of Criminology 6(2):119 - 134.
Franklin, Ursula M. 1999. The real world of technology. Rev. Edition. Toronto: Anansi.
Gandy, Oscar H. 2000. "Exploring Identity and Identification in Cyberspace." Notre Dame Journal of Law, Ethics & Public Policy 14.
McGregor, Glen. 2006. "Retract 'scurrilous accusations,' Harper, two of his key MPs told." In The Ottawa Citizen. Ottawa: Canwest.
Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." Washington Law Review 79:119.
O'Connor, Dennis. 2006. "Report of the Events Relating to Maher Arar: Factual Background, Volume I." Ottawa, ON, Canada: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.
Rawls, John. 2005. Political liberalism. Expanded Edition. New York: Columbia University Press.
Sandel, Michael J. 1998. Liberalism and the limits of justice. 2nd Edition. Cambridge, UK ; New York: Cambridge University Press.
Tibbetts, Janice. 2007. "Uncensored Arar report faults CSIS; "They can have their way with him"." In The Gazette. Montreal.
Toope, Stephen J. 2005. "Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar
Report of Professor Stephen J. Toope, Fact Finder." Ottawa: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar

Valiquet, Dominique. 2009. "Bill C-46: Investigative Powers for the 21st Century Act." ed. Library of Parliament. Ottawa: Library of Parliament.
Webb, Maureen. 2007. Illusions of security : global surveillance and democracy in the post-9/11 world. 1st Edition. San Francisco, USA: City Lights Books.
Whitaker, Reg. 2008. "Arar: The Affair, the Inquiry, the Aftermath." Montreal, QC, Canada: Institute for Research on Public Policy.
Whitman, James Q. 2004. "The Two Western Cultures of Privacy: Dignity Versus Liberty." The Yale Law Journal 113.
Yack, Bernard. 2006. "Rhetoric and Public Reasoning: An Aristotilean Understanding of Political Deliberation." Political Theory 34(4).
Young, Iris Marion. 2003. "Feminist Reactions to the Contemporary Security Regime." Hypatia 18(1):223-231.

markwick@sfu.ca