

Code-Bodies and Algorithmic Voyeurism

Examining the impacts of encryption, rights of publicity, and code-specters

*By Christopher Parsons**

Version 1.3 :: April 10, 2009

* Doctoral student in the University of Victoria's political science department. Thanks to Arthur Kroker for his comments. Comments welcomed, and can be sent to Christopher@Christopher-Parsons.com

Table of Contents

Digital Principles and the Early Internet.....	2
Digital Voyeurism and Insect Colonies.....	3
Reasonable Publicity.....	5
Specters Around Kant.....	7
The (In)Visible Constituents of Being.....	7
Hyper-Phenomenology and Justice.....	8
Code-Bodies and Digital Bugs.....	9
What Haunts DPI?.....	10
Towards Resisting DPI Voyeurism.....	11
BIBLIOGRAPHY.....	14

David Lyon has argued that we live in a society dominated by voyeurism. Not only do the few watch the many (panoptic), but the many watch the few as well (synoptic). He maintains that our drive to watch in Western societies is substantiated by Lacanian psychoanalysis, a culture that is taught to enjoy watching through cinema, and a general immersion in voyeuristic practices (i.e. medical, security, and travel related examinations). By attending to agentic structures driving the voyeuristic gaze of surveillance, Lyon hopes that a normative ethic can be found to mediate what we would consider particular invasive penetrations of the body (Lyon 2007a). This drive to look at others passed from looking at ‘meat’ bodies to ‘code’ bodies long ago, but the caliber of examination is qualitatively different than in earlier eras of digital inspection.

The act of viewing establishes particular power relationships, where those who can see without being seen possess greater power because they avoid being visually penetrated. Unobserved, or opaque, surveillance techniques are more ‘powerful’ than observable or transparent techniques insofar as the former techniques renders bare the subject of analysis without presenting a body or process for the subject to fixate on (Hansen 2006: 11-13). In the latter case, techniques of voyeurism are manifest through visualizing processes that render the techniques’ agentic structures visible on the basis that, while the viewed subject is being acted upon (i.e. surveyed), they are given (some) recourse to exercise their own agency in relation to the particular surveillance assemblage. Their own agency is manifest insofar as they can respond to the assemblage and its driving motivations; when you see a camera in a public space, you can file information requests for its footage, assault the camera itself, hide yourself from its gaze as best possible, and so forth. When the technique of visualization is hidden, the individual is penetrated without a

reciprocal penetration being possible – you cannot hide from the assemblage because the locus of its gaze is hidden, its lines of penetration invisible.

In digital spaces, an arms race between agents supporting and opposing unobservable surveillance techniques has been unfolding for at least two decades. This paper will focus on the current ‘arms race’ involving surveillance techniques that render the digital subject bare to heuristic analyses, and the methods that have been developed and implemented to ‘harden’ otherwise soft digital ‘flesh’. I will argue that while contemporary surveillance counter-measures limit the ability of surveying parties to perform digital ‘body scans’, this has resulted in more broadly socially invasive (as opposed to an individually invasive) modes of surveillance. Drawing on both Kant and Derrida, I offer a critique of digitally mediated surveillance and suggest that there remain open-ended possibilities of resisting surveillance. Despite this optimistic note, the paper ends tentatively, suggesting that Kantian public right and Derridean specters alone are not necessarily sufficient to prevent the very ‘real’ rending of digital flesh, but may offer a path towards developing an ethic of voyeurism.

Digital Principles and the Early Internet

The Internet was born of war. ARPNET, the progenitor of the contemporary Internet, was a redundant networked communication system designed to facilitate military communications should a nuclear attack be launched against America. In 1982 ARPNET was opened to major educational institutions, and a decade later the earliest version of the Internet as we currently experience it was launched. While government monies fueled the development of the Internet, one can argue that governments were not fully cognizant of what they were paying for.¹

The government money that was being spent in developing the Internet was pouring into the pockets and research labs of academic and computer researchers who (*very generally speaking*) injected libertarian(-like) values into the very DNA, the underlying principles, that govern data transfer across digital networks:

1. **Openness:** any computer or network can join the universe of networks constituting ‘the Internet’.
2. **Minimalism:** few computers need to join the Internet for it to function.
3. **Neutrality:** data transfer protocols do not discriminate bandwidth allocations on the basis of applications generating and receiving data traffic. (Goldsmith and Wu: 2006: 23)

As a result of these principles, data packets that were transferred across the net were ‘naked’, insofar as data security or protection was not embedded into the basic

¹ This was, in part, demonstrated in 1998 when civilian researcher Jon Postel took control of the central Dynamic Name System (DNS) servers that resolve web addresses with Internet Protocol (IP) addresses. Had the American government fully recognized the potential damage that could be done by this seizure of control of the ‘net, one would imagine that it would have enacted measures to avoid such take-overs.

principles of the 'net. The Open System Interconnect (OSI) model (see Figure 1) divided data packets into seven separate layers, with routing information being held in layers 1-4 and packet contents being held in layers 5-7.

Network redundancy was possible because if a node of the network went offline then routers would simply find new pathways to push packets across. This principle of routing around damage led John Gilmore to state that, "The Internet interprets censorship as damage and routes around it." Where packets are prevented from moving through routing devices, typically because the device is configured to limit or stop particular packet transmissions, alternate pathways are discovered and exploited: information wants to be free, and the 'nets engineering principles are intended to guarantee that while information may be obscure, it cannot be censored.

In terms of 'digital bodies', this means that the code composing the binary-stuff that manifests as organs (underlying protocols that act as digital circulatory systems), orifices (applications on computers 'eat and 'excrete' data for 'meat' body perceptions), and meanings (the truths/values that are made manifest through the interaction of organs and orifices) is relatively free. The code-body can develop and move in digital spaces without fearing that virtual-roadblocks will or can stop its development.

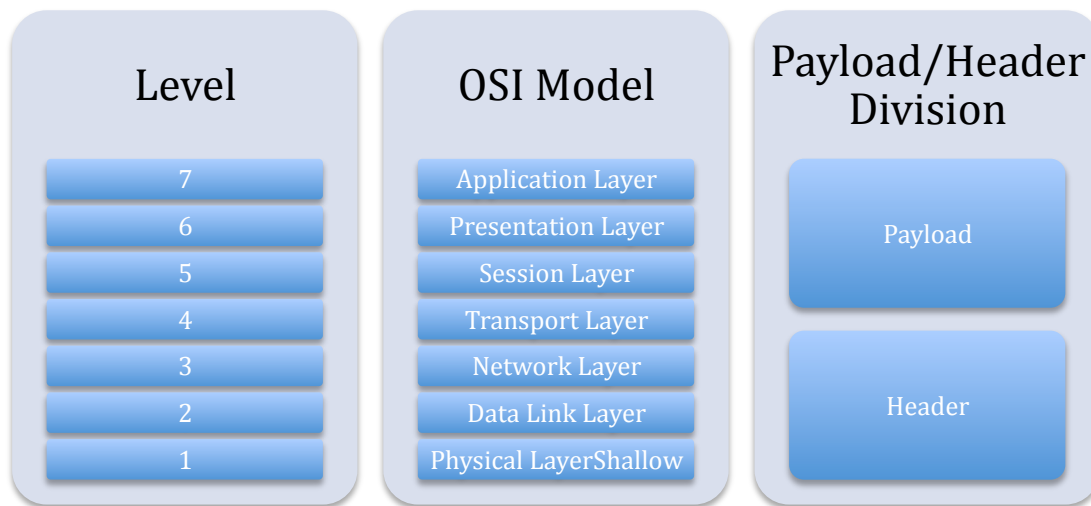


Figure 1: OSI Model

Digital Voyeurism and Encrypted Carapaces

Whereas in the Early Internet, code-bodies coursed through Internet gateways with little fear that their Being (i.e. payloads) would (or could) be examined, this has changed in recent years. With the development of technologies such as Deep Packet Inspection (DPI) that can examine layers 5-7 of packets, the digital body can be rendered fully visible. Organs can be mapped, and orifices identified and limited in their abilities to 'eat' and 'transmit' data packets, with the consequence that

meanings are be modified or censored.² Where insects develop bio-chemical shells to protect themselves from hostile environments, digital bodies have adapted to threats by shrouding themselves in encryption algorithms. This is demonstrated in the rising use of the Transport Layer Security (TLS) protocol by major commercial institutions to prevent eavesdropping, content tampering, and message forgery,³ as well as other protocols that are similarly aimed at preventing unauthorized voyeurs from perceiving anything more significant than packets' routing information. Just as we try to limit who knows our most intimate secrets in 'meat' space, we want to retain a similar degree of intimacy and privacy in the digital spaces that we inhabit.

In the effort to retain a semblance of personal privacy or, put another way, a modicum of control over who watches and records what we do and say, code-bodies have grown exoskeletons of encryption. These exoskeletons are constantly probed for weaknesses – new heuristics are developed to identify what encryption algorithms are being used, to determine what applications are generating data based on data transfer patterns, and ascertain packet contents based on their size and header characteristics (Parsons 2008) – and while our code-bodies may resist being penetrated, they unintentionally reveal the colonies that they are associated with. Once a packet is encrypted it is flagged by American intelligence services, which identifies the packet's point of origin and destination and stores this information in intelligence databases (Landau and Diffie 2008). As a result, in securing the *body*, the *community* becomes subject to intense military surveillance; securing one's personal privacy comes at the expense of the larger community that the code-body moves amongst. In this sense, voyeurism becomes *socially*, as opposed to just *individually*, invasive.

Data that is collected from these packet transfers can be correlated with surrounding information-sets; IP addresses can be traced to geographical locations and the names of Internet subscribers, patterns of digital movement can be used to develop composite identities (e.g. programs commonly used and bandwidth consumed, commonly accessed websites for behavioral tracking, etc.). This is affirmed by Diffie and Landau, when they write that “[t]raffic analysis reveals and organization's structure, its membership, and even the roles of its members” (Diffie and Landau 2008: 309). Bell Canada has implied that they classify consumers' digital bodies in a recent CRTC filing when they posit why wholesale customers consume a disproportionate amount of bandwidth:

² For a discussion of what censoring practices occur in Canada by major ISPs using DPI equipment see the section “Injecting Content with DPI – Rogers as a Case Model” in my Public Comments for CRTC Interrogatory PN 2008-19 (<http://tinyurl.com/d3arc5>).

³ The Pirate Bay, a large Bit Torrent Peer-to-Peer website, has recently announced that their contribution of the encryption wars is to provide easily accessible, easily used, Virtual Private Network (VPN) service for €5/month. This will fully encrypt all data traffic, and is meant to prevent media corporations from identifying whether individuals are transmitting or receiving data packets holding copy written data. Organs, orifices, and meanings are all 'shielded' from the gaze of security.

1. These consumers use HTTP for content sharing to greater extents (on average) than non-wholesale customers.
2. This consumer group is behaviorally disposed to consuming greater amounts of bandwidth, and are actively courted by retail wholesalers of Bell's broadband network ("The Companies' 2008⁴)

Just as physical surveillance technologies totally invaded the body⁵ and are deployed to map social movements,⁶ digital surveillance apparatuses can now similarly penetrate the code-body and map its relationships. Surveillance has become hyper-real, insofar as it has made the leap to digital spaces and normalized them according to the logics of 'meat' reality. A radical change in surveillance, however, has been the near-total replacement of human agency in the surveillance process. "[T]he watching gaze has long since ceased to be that of the artist or even the scientist, but belongs to the instruments of technological investigation, to the combined industrialization of perception and information" (Virilio 2005: 57). Confirming Lyon's later worries, this transition has been described as the endocolonization of the world that causes the world to become alien (Virilio 2005), one where all data is linked to particular identities (Solove 2008), where the commonly proposed solution is a heightened transparency of data flows instead of demanding that some of these flows themselves are terminated (Lyon 2007b: 181-2).

Given the seeming inability to prevent or stop the surveillance of our digital bodies, regardless of whether we develop code-carapaces or not, we might be inclined to throw up our hands and surrender to the Little Brothers surrounding us. Prior to abandoning all hope, let's turn to Kant and Derrida to both critique the current processes of securitization through surveillance, and to explore the conditions of perpetually evading surveillance of the code-body.

Reasonable Publicity

Kant approaches the world through his metaphysics, which he initially develops in the *Critique of Pure Reason*. In this text, he recognizes that time and space are pure *a priori* intuitions that are required for all other scientific endeavors. These intuitions require a subject, for;

...if we remove our own subject or even only the subjective constitution of the sense in general, then all constitution, all relations of objects in space and time, indeed space and time themselves would disappear, and as appearances they cannot exist in themselves, but only in us (Kant 1998: 185).

⁴ Only two of three of Bell's reasons are offered, because one was filed in confidence to the CRTC.

⁵ An example of 'total invasion' of the body would be the 'body scanners' that are being deployed in Western airports and are designed to see through one's clothes to give security examiners a view of the body underneath. The body is laid bare, subject to the voyeuristic gaze of security.

⁶ The New York/Manhattan security zone, as an example, aims to fully identify and track individuals that enter sensitive areas in Manhattan.

Reason orients individuals in the world insofar as this faculty lets them structure their experiences in, and critically engage with, the world. As subjects mature and develop this faculty, their freedom is 'extended' as they more completely understand the rational duties that they ought to perform in conformity with their moral obligations. Individuals are free because of their rational faculty and express their freedom whilst performing rationally universalizable actions.

Political environments facilitate the maturation of individuals by constituting republics that appropriately balance three *a priori* principles that emerge from Kant's moral theory:

1. The *freedom* of every member of society as a *human being*.
2. The *equality* of each with all the others as *subject*.
3. The *independence* of each member of a commonwealth as a citizen (Kant 2002: 74).

These principles are necessarily embedded in all nations' constitutions, and balance the public right (i.e. the capacity for action by individuals in civil society) through substantive instantiations in law. For law to be legitimate, insofar as all members of society can consent to being bound by it, it must accord with the transcendental and affirmative principle of public right. This principle demands that "[a]ll maxims which *require* publicity if they are not to fail in their purpose can be reconciled both with right and with politics" (Kant 2002: 130). Given that law must be publicly declared for citizens to follow it, legitimate laws must be made public; those that are hidden from the population are illegitimate and presumably upset the balance of public right by preventing individuals from appropriately modulating their civic freedom to accord with the freedom of all members of society. In short, hidden laws that prevent citizens from exercising their freedom, on the basis that a persistent concern that seemingly permitted actions might actually be illegal, cannot be reconciled with the harmonization of public right amongst the citizenry.

While Kant's discussion focuses on the state, given that his political writings emerge from the duties imposed through reason we can safely interpret his demands for publicity as imposing similar duties on private companies that operate key institutional infrastructures that citizens must interact with.⁷ It should be recognized that Kant's requirement for transparency is not intended to suggest that *citizens* necessarily be rendered fully transparent (though, arguably, an individual who performed their duty would be relatively transparent insofar as their actions would be predictable) – expectations placed on states and corporations diverge from those of citizens. On these bases, it would be both unreasonable (and thus

⁷ I intentionally condition the kind of private corporation as one that citizens *must* engage with, and thus differentiate them from corporations that citizens can *choose* to engage with. This means that, just as citizens *must* interact with the state (and thus must expect it to behave within the confines of reason) they *must* similarly interact with some private corporations. On the basis of this similarity, we should expect comparable logics to guide citizen-public and citizen-private institutional relationships.

illegitimate) for private corporations to deploy non-transparent surveillance apparatuses that:

1. Were not publicly announced.
2. Did not necessarily facilitate a just balancing of public right.

Consequently, the deployment of DPI devices, without a total explanation of why they are being used, what they do, and how they function would be in violation of Kant's requirement for state and state-like maxims to be made public. Code-bodies cannot be penetrated without good reason. Without publicly announcing that such penetrations will occur along with their full justification, the Kantian position must denounce their use as illegitimate.

Specters Around Kant

Kant theoretical structure presumes that the faculty of reason can capture freedom's total cognizable possibilities by working from the *a priori* concepts of space and time. Kantian time is linear and corresponds with the mechanization of time that aligns with the procession of time demanded by mechanical clocks. As such, there is a sequence of times that have past, and are to come, and each is necessarily experienced should a subject exist during a moment's particular temporal Being (as distinguished from a moment's Being-Past and Coming-to-Be). Further, space operates as a site to be filled, or experienced as an absence of filling. In either case, Kant's structure is problematized by the possibility of times that are always coming, and always simultaneously past, but can never be realized, as well as by spaces that are always filled, and never filled, where the *subject* is forever prevented from directly experiencing. While Kant can offer an account of the code-body, we must wonder how/if he addresses the code-soul.

Enter the Derridean specter.

The (In)Visible Constituents of Being

There are times, places, and objects that we sense as being somehow *different*; this differentness is not *frightening* so much as *uncanny*. In Turkle's words, the uncanny is that which "seems close, but "off," distorted enough to be creepy. [The uncanny] marks a complex boundary that both draws us in and repels..." (Turkle 2007: 8). For Derrida, specters are experienced as uncanny (Derrida 1994: 125); we only perceive them as frightening when they jeopardize cherished norms and hegemonic principles and, at these moments, transmute them from specters to ghosts. Let us unpack what the 'specter' is to exemplify why it challenges a Kantian critique of mass digital surveillance systems (such as DPI), and then move to think through how the specter can problematize the very notion of 'ubiquitous' digital surveillance techniques that can penetrate the code-body.

Derrida's specter is a persistently disturbing present that lingers "in the coming-and-going, *between* what *goes* and what *comes*, in the middle of what leaves and what arrives, at the articulation between what absents itself and what presents itself" (Derrida 1994: 29). It is out of joint with time, insofar as it forever stands

before and after a moment of experience; it is never realized in the Now save for as a shadow or whisper of what has, or will, come to pass. Given this, specters are never actualized in reality – they are ontologically incapable of actualizing themselves in any manner other than haunting. A specter “haunts ... without residing, without ever confining itself to the numerous versions of this passage” (Derrida 1994: 21) and given its disturbing uncanniness we (the embodied, the real, the actualized) perform elaborate exercises to find where the specter ‘resides’ so that we can exorcise it.

Exorcisms are intended to drive away that which has never, and always might, Become. Exorcism “pretends to declare death only in order to put to death ... it certifies the death but here it is not in order to inflict it” (Derrida 1994: 59). As agents of temporal-spatial existence (per the Kantian *a priori* concepts of time and space) we work to imbue the specter with a Being that it does not, cannot, actually possess; in a mockery of death, we pretend to kill that which cannot be killed and declare the execution successful. We impose an ontological structure that corresponds with our own understanding of Being-in-the-World in an effort to temporalize and spatialize the specter. Having attributed these characteristics to the specter, we find their haunts and sanctifying them in order to ‘deny’ it a space to reside – we humanize it, and end its existence as we would a human’s. Ultimately, however, our task is a fool’s errand (not even Sisyphean!): uncanniness remains even after the formal ‘vanquishing’ of the specter. The haunting continues...

Hyper-Phenomenology and Justice

What would it mean to find or vanquish the uncanny, to put an end to being haunted? In effect, what would it mean to be successful in a specter-hunt? What would be the consequences of ending the hyper-phenomenology that is always-never embedded in our experiences?

To banish specters we would first need to stand in clear relation to them. This would demand a process that was stridently different from a Hegelian thesis/antithesis/synthesis relationship; the relationship between specters and us is one between Being and Being-without-ever-Being. Banishing a specter by drawing a Hegelian division would confirm our own actualized Being: we have bodies, and we operate in time. It would assume that we are ‘normal’ and demand that we normalize the uncanny by situating it in relation to ourselves without admitting the possibilities of non-spatio-temporal ontological existences that defy our phenomenological orientations in the world. To avoid getting wrapped up in a Hegelian dialectic and actually ‘banish’ the hyper-phenomenological, we would have to actually try and address the specter according to its own ‘existence’; ontologically we would have to understand ourselves as *outside* or *beyond* space and time. We would need to recognize *ourselves*, and not just the specter, as out of joint.

In considering being out of joint, let us focus on its implications for justice. In a hyper-phenomenological situation, justice would be transformed from a universal normative guide to something that is forever yet to come, and always beyond Being. Instead of a regulative ideal of justice (such as in Kant) that we could normatively

evaluate our actualized understandings of justice against, justice becomes something that can never be – moral-juridical norms do not capture justice, and as such law necessarily commits violence instead of justice. Understood hyper-phenomenologically, justice must permanently stand before and behind law. In this sense, to a phenomenological being, justice can only be recognized in moments of exceptionality that are perceptible on the basis of their uncanniness.

Given that we are simultaneously drawn to and repelled by the uncanny, our relationship with justice is such that (like moths to a flame) we are prevented from genuinely experiencing anything more than an apparition of the hyper-phenomenologically understood concept. Justice must haunt us. As creatures of experience, while we can approach the hyper-phenomenological we cannot transcend the realm of experience. The condition for banishing or ‘killing’ the hyper-phenomenological demands an ending of phenomenological biases; such an ending would require passing into the flame of the hyper, and burning just as a moth does when caressed by flame. Barring an end to our Being-Towards-Death, we are left with the uncanny, and perpetually haunted by its open-ended possibilities that can never be substantively actualized in time and space. Justice becomes impossible to realize, but always something that simultaneously attracts and repels us.

Such an impossible-possibility suggests that any assertion of a formal injunctive proposition meant to condition phenomenal behavior is necessarily limited, conditioned, and (likely) engaged in violence against justice as a hyper-phenomenon. Since any attempt to banish the specter (and thus Justice) is doomed to fail, we are left with the question of whether a condition of publicity will meaningfully mediate the intrusions of digital eyes into our code-bodies; can Kant integrate justice into DPI surveillance practices?

Per Kant, the transcendental and affirmative principle of public right requires that any law that accords with external freedom be made public – doing otherwise infringes on citizens’ freedom and is unjust. Kant’s focus on space and time let him speak to *code-bodies* while leaving him with little to say to *code-spirits*. Kant has little to say about specters and can (and does) only address them on his, rather than their, ontological terms.⁸ Hence, if we can assert that a *code-spirit/specter* exists, then Kant’s critique of opaque ubiquitous digital surveillance assemblages (such as DPI) would fail to totally address digital voyeurism.

Code-Bodies and Digital Bugs

The code-body is manifest through its organs, orifices, and meanings in a manner similar to the ‘meat’ body. How might we understand the specters that haunt this digital body, and what spaces does this provide for our discussion of surveillance appliances that penetrate the depths of code?

⁸ Rebellion is an example of the spectres that Kant grapples with; Kant persistently returns to the notion of duty that is mandated by Reason, and the subsequent logical contradictions that arise when universalizing the right to rebellion, as a way of banishing the normative possibility of rebellion.

Code-bodies are developed according to the (supposedly) rigorous protocols and data equipment that shuttles packets across the 'net. In turning to HTTP, FTP, and STMP protocols, JPEG, MPEG, MOV, and HTML data formats, and TCP/IP, IPX, and ATM routing information we think that these bodies can be mapped. Analyzing router hops and understanding the Time To Live (TTL) give let us identify distances that packets can move, and watching for routers that refuse to pass along packets reveals the Internet's 'closed' doors. The code-body is navigated by a 'meat' body or, alternately, is by non-living machines, or code-corpses. Code-corpses, computers that operate without being motivated by direct human agency, move about digital networks beside their 'living' counterparts. Automated email resolution messages (such as those from the seemingly ubiquitous 'Postmaster'), heuristic surveillance analysis protocols, and self-healing digital frameworks are all demonstrations of limited self-agency that is embedded in pieces of software. A step beyond this code as it is meant to be 'played out,' however, is that there is always a danger that something 'weird' happens; a router stops forwarding packets from a particular address based on an unpredicted heuristic analysis, the Postmaster begins sending unintelligible or incorrect messages, or self-healing frameworks get locked into perpetual healing cycles when they perceive a fatal flaw that is intrinsic to the design of the network itself.⁹

In each of these situations, human agents say that a 'bug' has been found and needs to be 'fixed'. Developers who prepare projects routinely engage in 'bug-hunts,' where they aim to 'cleanse' code of imperfections. Operating with a regulative notion of 'normal,' software and hardware jockeys alike always aim to approximate the ideal. These hunts are more effective when good practices and processes have been followed in the development process. 'Good' here means that transparency pervades the development cycle; all changes to the codebase/system are documented and made available to anyone who wants to look at the code. In this sense, 'good' code doesn't just run: it also has clear comments beside the lines so that other developers can read what the code is supposed to/is doing. In the Kantian sense, such code adheres to an affirmative principle of publicity in a broader effort to be good. In terms of DPI appliances, this means that their 'bodies' must be rendered transparent. What, however, are we to do about their souls?

Haunting the Code-Body and DPI

An interesting exercise: what does a code-corpse find uncanny? To put it another way, what is it that draws and repels the DPI appliance, what haunts the technology (at the level of code, rather than the level of politics)?

⁹ Contemporary Computer Processing Units (CPUs) are designed to limit and prevent fork bombs that are caused by bugs in code and viral attacks. Fork bombs ceaselessly create clones of pieces of code until the computer runs out of memory, in the hopes that this will create a memory addressing error and cause a network/computer crash. In a well known case, CPUs from hardware company AMD attempted to 'resolve' fork bombs that didn't actually exist; its efforts to 'heal' the system actually provoked computer crashes. The only solution (for that generation of processors) was to 'turn off' that element of the CPUs' agency.

While the code-body was haunted by expectations/hopes of controlling or mediating the voyeuristic leering of surveillance assemblages, being simultaneously drawn to them (as it moves across digital networks and almost 'touches' the routing equipment) and repelled from them (as it is jettisoned away from the equipment and projected towards another point on the network). In the process of moving, the data packets composing the carapaced code-body is drawn to reveal itself to routing equipment (by providing packet header information to direct the packet to its destination) while repelling itself from divulging its inner being (by encrypting packet payloads to prevent undesired surveillance). What is the equivalent set of relations for DPI appliances?

Whereas the carapaced code-body is caught in a relationship of revealing/hiding its body from the voyeuristic gaze of the DPI appliance's heuristics, the DPI device is haunted by the drive to totally penetrate the code-body without ever being able to do so. Even streams of non-encrypted/secured data packets cannot be perfectly identified using heuristic analyses (Rossenhovel 2008). Further, where 'soft' (i.e. non-encrypted) data packets stream through the DPI routing device, the appliance can identify the code-body's organs (underlying protocols that acted as digital circulatory systems) and orifices (applications on computers 'ate' and 'excreted' data for 'meat' perceptions), but cannot determine the *meaning* of the relationship between these organs. A DPI appliance's capacity to fully investigate the *meaning* of a code-body's movements is crippled because it cannot simultaneously view the relationship between digital data packets and the meat-body's relationship to the digital embodiment. While DPI appliances can assume that particular packet exchanges can be correlated with meaning the follows from how the meat-body values their embodiment, that correlation can never be absolute. The appliance's location in network hubs, instead of in the minds of meat-bodies *and* networking data centers, means that heuristics can only approximate possible meanings from the relationships of organs and orifices; perfect accuracy is denied. The appliance is always haunted by the possibility of penetrating the code-body to realize meaning, but unable to capture meaning through its heuristic relational processes.

The consequence of the 'encryption wars' is that the DPI appliance is always close, but never fully upon, the carapaced code-body for similar reasons as with the non-carapaced, or larval, code-body. With the encrypted body, organs, orifices, *and* meaning are cast into even more deeply confused relationships. Why is the data encrypted? Does the DPI device even *recognize* the data as being encrypted, or is the body masked in a way that totally fools the appliance's analysis? Given the possibility of packet forging, and the chance that the appliance cannot detect the forgery, does this not further problematize the derivation of meanings from organ/orifice relationships? In effect, does encryption fully frustrate an understanding of particular code-bodies?

Towards Resisting DPI Voyeurism

We began this paper with the worry that efforts to shield the individual code-body came at the expense of increasing social surveillance, and that while both Kant and

Derrida could speak to the issue of DPI surveillance that neither theorist would necessarily prevent such a mass 'rending' of digital flesh. In these last few paragraphs, let us reflect on these theorists' respective insights and whether they have provided us with adequate responses to DPI's penetration of the code-body.

In the case of Kant, a real expectation and demand of technological transparency rang out. Since packets must pass along public routers that have DPI appliances integrated into them, standards should be made public, heuristics labeled and identified, and so forth. Failure to do so is found in violation of norms of publicity demanded by reason itself. When considering what haunts DPI appliances through Derrida, we found that the inability to precisely identify the meaning of organ/orifice relationships meant that the ontological drive of these routers to fully *see* is forever frustrated. Unlike a regulative ideal, this paper suggests that meaning can *never* be precisely/perfectly know; at best statistical degrees of accuracy are possible, and such a statistical interpretation necessarily imposes an ontological understanding of what meaning *is* on the code-body, rather than engaging the body in its own ontological terms. Thus, the total penetration of a packet is frustrated, just as a moth is frustrated from touching a candle.

What does this mean for us, today, as 'meat-bodies' who virtually become manifest through packets of data? What do Kant and Derrida have to contribute to David Lyon's project of establishing a normative ethic based on voyeurism that was noted at the beginning of this paper?

I would tentatively suggest that, while spatio-temporally grounded norms have been identified (through Kant) and evasion techniques recognized (through Derrida), that the former presupposes a particular political environment and the latter operates as an ethic of flight. The challenge with Kant's norms of publicity is that even if a law is *not* publicly declared, the citizen remains bound to it. The Kantian subject is forever bound to law, save for if obeying it would prevent them from performing their duty (in terms of Reason). Thus, unless subjection to DPI appliances' gaze undermines the performing rationally prescribed moral duties, subjects may not have theoretically-grounded recourse to alleviate the electronic voyeurism.

Concerning the ethic of flight, this ethic does not prevent the rending of flesh. Instead, it limits the *depth* of the voyeur-imposed wounds, trading critical injuries for flesh wounds. While the code-body itself may limit its exposure to the appliance's gaze, should it shroud itself in a carapace its movements immediately brings attention to the network of other code-bodies that it interacts with. While one is tempted to respond that packet forgery could limit the perfect correlation of code-bodies to the social network they operate within, it would appear as though by individualistically protecting oneself that the society at large is brought into focus. These others may have otherwise escaped notice, may otherwise have kept their presence unseen and avoided the penetrating gaze of total surveillance instruments. The ethic of flight, as discussed here, is an ethic of one that sacrifices the many.

This does not, of course, mean that the ethic *must necessarily* sacrifice the many, nor that a reformed understanding of the Kantian ethos would be similarly ineffective at normatively resisting DPI appliance surveillance. Instead, we should read these efforts conditionally, as a beginning from which a more nuanced and refined ethic might emerge. Of course, this may (will likely?) see a pair of ethics develop that rest on separate ontological foundations. Regardless, a reformed ethic could be adopted and adapted for theoretically rich understandings of digital resistance, an ethic capable of directly addressing digitally mediating surveillance apparatuses.

BIBLIOGRAPHY

- Bell Aliant Regional Communications, Limited Partnership and Bell Canada ('the Companies') 2008. "Supplemental Information as Per CRTC Letter Dated 2009 02 04 – Alternate Internet Traffic Management Practices." Last accessed March 23, 2009. URL: <http://tinyurl.com/cqodym>
- Derrida, Jacques (1994). *Specters of Marx*. Peggy Kamuf (ed.). New York: Routledge Classics.
- Diffie, Whitfield and Susan Landau (2008). *Privacy On the Line: The Politics of Wiretapping and Encryption (Updated and Expanded Edition)*. Cambridge, Mass.: The MIT Press.
- Hansen, Mark B. N. (2006). *Bodies in Code: Interfaces with Digital Media*. New York: Routledge
- Kant, Immanuel (2002). *Political Writings*. H. S. Reiss (ed.). New York: Cambridge University Press.
- Kant, Immanuel (1998). *Critique of Pure Reason*. Paul Guyer and Allen W. Wood (eds.). New York: Cambridge University Press.
- Lyon, David (2007a). "9/11, Synoticon, and Scopophilia: Watching and Being Watched" in Kevin Haggery and Richard Ericson (eds.) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.
- Lyon, David (2007b). *Surveillance Studies: An Overview*. Malden, MA: Polity.
- Parsons, Christopher (2008). "Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials," working paper for *The New Transparency Project*. URL: <http://tinyurl.com/cxae6c>
- Rosshovel, Carsten (2008). "Peer-to-Peer Filters: Ready for Internet Prime Time?" *Internet Evolution*. Published April 27, 2008. Last accessed October 8, 2008. URL: <http://tinyurl.com/clrqrt>
- Solove, Daniel (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.
- Turkle, Sherry (2007). *Evocative Objects: Things We Think With*. Cambridge, Mass.: The MIT Press.
- Virilio, Paul (2005). *The Information Bomb*. New York: Verso.