

Deep Packet Inspection: Privacy, Mash-ups, and Dignity

By Christopher Parsons*

Abstract: Privacy operates as an umbrella-like concept that shelters liberal citizens' capacity to enjoy the autonomy, secrecy, and liberty, values that are key to citizens enjoying their psychic and civil dignity. As digitisation sweeps through the post-industrial information economy, these same citizens are increasingly sharing and disseminating copywritten files using peer-to-peer file sharing networks. In the face of economic challenges posed by these networks, some members of the recording industries have sought agreements with Internet Service Providers (ISPs) to govern the sharing of copywritten data. In Britain, file-sharing governance has recently manifested in the form of Virgin Media inserting deep packet inspection (DPI) appliances into their network to monitor for levels of infringing files. In this presentation, I argue that ISPs and vendors must demonstrate technical and social transparency over their use of DPI to assuage worries that communications providers are endangering citizens' psychic and civil dignities. Drawing on recent Canadian regulatory processes concerning Canadian applications of DPI, I suggest that transparency between civil advocacy groups and ISPs and vendors can garner trust required to limit harms to citizens' psychic dignity. Further, I maintain that using DPI appliances to detect copyright infringement and apply three-strikes proposals unduly threatens citizens' civil dignities; alternate governance strategies must be adopted to preserve citizens' civil dignity.

* Christopher Parsons is a doctoral candidate in the University of Victoria's Department of Political Science. Elements of this paper, prepared for the Counter: Counterfeiting and Piracy Research workshop, are drawn from earlier work presented in his unpublished master's thesis, a presentation at a deep packet inspection workshop hosted by Ryerson University in 2009, and thoughts and reflections from his website. He thanks Joseph Savirimuthu for the invitation to the conference, Omid Payrow Shabani for comments on the sections on privacy, Fenwick McKelvey and Colin Bennett for discussions surrounding citizen advocates, and the peer-to-peer community at large for framing and testing his ideas of copyright.

Table of Contents

What is Privacy?	2
Privacy as the Umbrella of Dignity	5
Contemporary Digital Expression Through Mash-up	8
The Stated Capacities of Deep Packet Inspection	11
Deep Packet Inspection and the Canadian Situation	15
Fundamentalist versus Pragmatic Advocacy	17
The Activist/Fundamentalist	17
The Pragmatist	18
Canadian Privacy Advocacy and DPI	19
Deep Packet Inspection and Civil Dignity	20
Levies, Not Deep Packet Inspection	22
Conclusion	23

Reformations of copyright law and the introduction of new means to detecting infringing use carry with it a heavy task, one that is done taken up often enough. Copyright is a privilege that is provided in the interests of the public good, as a means through which creators can be granted a limited monopoly over a creation so that they can receive some restitution for their work. At issue, of course, is that copyright operates predominantly in contemporary capitalist societies; pure capitalism demands that monopolies be avoided and competition be as free as possible to encourage innovation. Countries such as Canada and the United States operate within constitutional liberal political climates, which carries with it responsibilities, obligations, and rights that are shouldered by each citizen. While the freedom of speech is understood slightly differently by these two nations, the freedom of speech and association are central organizing tenets of both the Canadian and American constitutional democracies. Normative problems related to freedom of expression arise when copyright is asserted in manners that both upset the logics of capitalism and liberal democracies, and these problems are presently upon us.

The assertion of monopoly rights over particular expressions, especially when such expressions function as key tenets of the nation's culture, threatens to limit the range of permissible speech and development of cultural meaning. In particular, rigorous enforcement of copyright can limit the speech of citizens and consequently injure the civil discourse that citizens participate in with one another. Such limitations carry with it consequences for the political, the domain of the people, insofar as citizens are subsequently limited in their capacity to radically critique dominant

socio-economic ideologies and paradigms through practice in instances where such practices constitute infringing uses of copywritten cultural content. This is particularly the case with digital music mash-ups, where a cultural resurgence is demonstrated, one that strives to (re)generate the participatory culture that has been endangered by extensions of copyright provisions, assaults on fair use and fair dealing laws, and may soon be put to siege by contemporary surveillance appliances being used by Internet service providers.

There are two core aims of this paper. First, I will to argue that it is imperative for civil society that Internet service providers and the vendors of deep packet inspection equipment to be highly transparent in the deployments and actual possibilities of these pieces of equipment so that the public can engage in an honest and full civil discussion of the value and desirability of these surveillance systems. Second, I maintain that using deep packet inspection technologies for the purposes of copyright enforcement via three-strikes laws threatens the civil dignity of the citizen, as they would be increasingly left unable to effectively communicate with the state using either mash-up means of digital expression or, more simply, taking advantage of electronic government services. In making this argument, I maintain that deep packet inspection, as a particularly powerful surveillance apparatus, has the potential to endanger citizens' psychic and civic dignity.

The structure of the argument is as follows; (I) I sketch a definition of privacy that acknowledges it as an umbrella concept used to shelter key democratic values, allowing me to (II) assert that privacy is needed by Western citizens for their psychic and civil dignity. I then (III) outline how mash-ups constitute a particular form of individual, communal, and civil expression. Having provided a concept of privacy, its value, and the value of contemporary modes of generating cultural meaning, (III) there is a brief discussion of what deep packet inspection is and its capacities (IV) that is followed by an analysis of the recent Canadian regulatory proceeding over Internet service providers' use of deep packet inspection. This analysis lays out the fears and concerns of civil advocates, and maintains that for pragmatic civil advocacy – advocacy that is clearly beneficial to both society and corporate agents – then service providers and vendors must be transparent in how and why they deploy and develop these technologies. Central to this is a need for *public* transparency, and such transparency can allay psychic-dignity concerns. There is now rhetoric, and early applications, of using deep packet inspection for copyright enforcement and I (V) conclude by outlining why such uses are arguably harmful to citizens civil dignity and (VI) a suggestions as to how we can avoid the need to use deep packet inspection for copyright monitoring entirely by adopting expanded Canadian levy laws.

What is Privacy?

Privacy is often understood as a state free from external obtrusions or disturbances to one's private affairs. Such a broad understanding of privacy conjoins a series of

interrelated, though distinctive, privacy classifications: freedom to control one's personal information (informational privacy); freedom to physically isolate oneself (accessibility privacy); and the freedom to speak and associate with others without being surveyed (expressive privacy). Broadly classifying privacy as freedom from obstruction fails to transparently distinguish privacy from the closely related concepts of autonomy, secrecy, and liberty. In this section, I briefly outline the three interrelated privacy classifications and distinguish privacy from autonomy, secrecy, and liberty. After providing a granular account of what privacy is and is not, I proceed to discuss privacy's value to individuals in their public and private lives.

At its most basic level, informational privacy describes the right to know who knows what about you and to control the flow of your personal data to other parties.¹ Personal data encompasses information that is on and off the public record, and includes information about daily activities, personal lifestyle choices, medical history, finances, academic achievements, religious or philosophical beliefs, distinctive physical descriptions, employment history, personal relationships, sexual orientation, life goals, and preferred customer habits, to name a few. Under this privacy classification, individuals experience privacy invasions "by publication or even broader publication of such information; by intrusive snooping, observation, or wiretapping; by testing to gain or attempt to gain the information."² This last point is especially important; it is not that someone has successfully collected information without first gaining an individual's consent – the mere attempt to access this information constitutes invasion. Informational privacy often overlaps accessibility privacy, which is infringed upon when another person enters an individual's physical proximity in violation of the individual's reasonable attempts to seclude themselves from the eyes of others. Judith Wagner DeCew, a noted privacy and legal theorist, notes that even "surveillance of normal, everyday activities can lead one to be distracted and to feel inhibited. Such behaviour can intrude on one's solitude or seclusion even if it is not yet noticed or discovered, because of the fear its potential recognition can generate."³ According to Wagner DeCew's account, an individual's accessibility privacy is breached when a person surreptitiously watches a woman shower or undress, for example. This stealthy behaviour intrudes on the woman's reasonable right to privacy and, if the behaviour is left unchecked, can generate fear of discovery in the woman and sense of personal violation. Like accessibility privacy, expressive privacy relates to the individual's ability to control who surveys and records their personal expressions. Expressive privacy protects individuals from the fears or pressures to conform to homogenized viewpoints or attitudes that can follow from suspecting that one's privately uttered speech might be being monitored or could be made public. This kind of privacy is, as an example, intended to protect people so that they can express their sexuality, regardless of whether it accords with dominant social norms. Because expressive privacy tends to involve the collection of information as well as some proximity to collect or verify the collected information, this last privacy classification is often intimately linked with the two previously mentioned classifications.⁴

In addition to commonly compressing the three aforementioned privacy's classifications to a lone and somewhat nebulous privacy classification, privacy is also often unintentionally compressed with the theoretical concepts of autonomy, secrecy, and liberty. While privacy is intimately involved with each of these concepts, it acts as an umbrella that is deployed to shelter individuals' autonomy, secrecy, and liberty, rather than being intimately and unavoidably bonded to any one of them. While autonomy and privacy interests often align when either autonomy or privacy is violated, this is not always the case because people are autonomous insofar as they can make independent and self-legislating choices. When a person decides to blare their car stereo in a busy neighbourhood, their autonomous action cannot be considered private. In contrast, when they make decisions concerning their basic lifestyle, they can reasonably expect to have their autonomous choices kept from the public eye. Moreover, not all privacy invasions directly threaten a person's autonomy – electronic surveillance, for example, doesn't necessarily violate a person's ability to make self-legislating choices so long as they never experience consequences resulting from the surveillance or realize that they are being electronically surveyed. Because of these complications, we cannot legitimately claim that autonomy and privacy concerns are necessarily conjoined.

Similarly, privacy and secrecy often align with one another, though they do not always do so – some events are secret but not private, and vice versa. To expand, a secret treaty or military plan may be kept secret from the public, but the fact that it is kept secret does not mean that it deserves the privacy protections that cloak people's sexual activities in their homes. It is important to note that “[c]haracterizing privacy as what is *intended* to be concealed is no help”⁵ because, while military secrets are intended to remain secret, it does not follow that their intention to be kept secret necessarily means that they are private. In light of the difference between privacy and secrecy, we can say that secrecy aligns with privacy protections when private individuals engage in actions that they can reasonably expect to be concealed from the public eye. This said, there is (again) no necessary equation between privacy and physical secrecy. While physical seclusion is often used to evaluate whether a person's accessibility or expressive privacy has been invaded, it does not stand that secret actions in secluded spaces are necessarily private – politicians who meet in secret to negotiate legislation cannot justifiably expect privacy laws to protect their very public discussions.

Finally, we must make a distinction between privacy and liberty. Privacy is intended to prevent unnecessary interference in our personal lives and, to a limited extent, does promote liberty of action. Personal liberty encompasses the range of actions that a person can perform, whereas privacy shields people from intrusions that would limit individuals' possible ranges of publicly sanctioned actions. In light of this disjunction between liberty and privacy, we can envision cases where a person's privacy could be invaded without infringing on their liberty and vice versa. If, for example, I am unknowingly placed under surveillance, my liberty is not necessarily impeded – I am still free to enjoy my customary ranges of action even though all my actions might be recorded. Alternately, I could be physically assaulted on the

street and have my liberty limited without experiencing a privacy invasion. While privacy and liberty often align with one another, the division between privacy breaches and injustices towards personal liberty reveal that the degradation of one's liberty does not necessarily indicate that a privacy breach has occurred.

Privacy as the Umbrella of Dignity

Liberty, the absence of external restraints or coercion, plays a central role in forming the political bonds between citizens. In the absence of coercion, citizens are free to communicate with one another without fearing that another person is recording their private actions and could later threaten or shame the citizen. With the liberty to act on their autonomous choices, citizens can associate with others, utter statements or participate in publicly controversial actions that can fundamentally shape the values that structure their public and private attitudes – private actions influence public attitudes and vice versa. If citizens believe or expect that their actions might be monitored, while actual restraints (i.e. coercive or preventative techniques or technologies) might not restrict their actions, they can fall prey to imagined restraints and adjust their behaviour in light of imaginary bonds that are as strong (or stronger) than shackles of steel. These self-imposed restraints can diminish the range of liberty that individuals feel safe exhibiting, which is conjoined with a corresponding diminishment of autonomy as citizens feel unable to make self-legislating choices, let alone act on them. In this light, we can say that “the right to liberty embraces in part the right of persons to make fundamentally important choices about their lives and therein exercise significant control over different aspects of their behaviour.”⁶ Privacy is the umbrella that protects core principles that all citizens share, and it ensures that citizens can make the decisions that are fundamental to their private and public development. Privacy facilitates the environment where people can learn, experience, and experiment without fearing hidden or latent punishments for making choices that deviate from public norms in ways that are neither self- nor other-harmful.

Moreover, the right to secrecy is invaluable because it opens a space for individuals to act and express themselves to others in deeply intimate ways, ways that they might be uncomfortable or unable to mirror in the public sphere and that are essential to their personal development. Donald Winnicott, a widely-influential psychoanalyst, notes that in public environments where we must conform to particular rules and norms we adopt a “False Self” to mask our “True Self” so as to avoid being overly vulnerable to strangers. Winnicott notes that some of his patients feel so ashamed of their “True Selves” that they are utterly incapable of accessing their inner world and, as a consequence, cannot manifest it to others⁷ –they are perpetually trapped in the public gaze. ‘Normal’ people do not experience this crippling insecurity, but their relative fearlessness would likely evaporate were they deprived of their privacy rights. If co-workers, police, clergy, and your employer could all learn about anything that you said, the likelihood of freely expressing your “True Self” would diminish alongside your reasonable expectations of privacy. Within zones of

secrecy – in the arms of a lover, the deathbed of a relative, or in letters between distant but good friends – privacy preserves safe spaces where individuals can be vulnerable to one another without being paralyzed by the possibility of their words being disclosed. Privacy rights are legal affirmations that spaces of vulnerability ought to exist so that individuals can develop and express their most intimate thoughts and beliefs.

In panoptic environments, where individuals' public and private actions are persistently monitored (effectively abolishing the substantive realization of physical or communicative seclusion), subjects feel as though the possible application of coercion could occur at any moment. Individuals experience a constant pressure to conform to public norms even before taking actions that deviate from the dominant ethical-political norms. The thought alone of deviating from social norms leads individuals to worry that authorities might have detected the individuals' deviancy. In situations where individuals persistently fear being monitored they reduce the scope of their actions so that none of their actions could possibly be recognized as deviating from the public's norms; they self-censor their words, they feel incapacitated to even ponder certain decisions, they 'rehabilitate' their deviant physical behaviours. In short, they experience deprivations in their ranges of choice. These environments do not just stop individuals from engaging in actions they want to perform, but mould their very behaviour. The operation of bodily surveillance in panoptic environments leads the individual to restructure cognitive pursuits to harmonize their actions with the norms held by the surveying parties.⁸

Discussions of panopticonism almost invariably lead to discussions of Michael Foucault's *Discipline and Punish*, but perhaps rather than attending to his work, we should turn to Oscar Gandy's conception of the 'panoptic-sort'. Gandy, writing with an awareness of the sorting potential of computer databases, suggests that what is at issue isn't so much that we are being watched, but that the watchers allocate those observed into particular categories. These categories are based on normatively ambiguous search and sort criteria that those observed are not made aware of, nor have given their consent to. Generally, three core issues arise when panoptic-sorting causes individuals to experience deprivations of their informational, accessibility, and expressive privacy. The first is that individuals must often bear the burden of proving their innocence rather than others having to prove the individual's guilt. To elucidate, a panoptic-sorting could occur at any time and place an individual in an undesirable category based on an out-of-context comment that was repeatedly quoted in popular media. The individual becomes perpetually guilty of any comment they have made and must be prepared to defend themselves against its potential implications at any point in their lives. The second issue is that these sorting environments impose a set of homogenous norms. As Lawrence Lessig notes,

[w]e all desire to live in separate communities, or among or within separate normative spaces. Privacy, or the ability to control data about yourself, supports this desire. It enables these multiple communities and disables the power of one dominant community to norm others into oblivion.⁹

The plurality of nation-states, and the dignity each person deserves, can become endangered if individuals are not shielded from a totalizing normative structure that forcefully imposes itself across the entirety of their lives. The nation-state, as an inclusive body that remains sensitive to the particularities accompanying new members, faces political stagnation if it cannot continue to resolve the dual problems of legitimization and integration. These problems have been resolved through the use of discourse to legitimize political norms. Importantly, this discourse incorporates a diverse range of privately and publicly generated norms instead of exclusively drawing on homogeneous ethnic-logics. Yet, the compression of normative spaces threatens to return the nation-state to a normative attitude bearing resemblance to that of ethnic-states, which were unsuccessful at generating citizen-solidarity in pluralistic environments.¹⁰ Finally, the panoptic-sort is accompanied by the exertion of micro-control over subjects – discipline develops that can strike perfectly at particular individuals. This micro-control develops as individuals increasingly become wrapped in what Cass Sunstein terms ‘data cocoons’.¹¹ Sunstein, a distinguished professor of jurisprudence, suggests that when a person’s life is entirely accessible and searchable, it becomes possible to accurately determine the person’s preferences, dreams, fears, loves, and hatreds. The accuracy of such predictions lets authority figures perfectly supply information that a person is interested in and, by reinforcing preferred data streams, data cocoons develop as individuals’ liberty and autonomy are eroded alongside the possibility of encountering philosophies, products, or news that deviate from their already established preferences.¹² This creates an especially problematic environment for developing critical political awareness because these cocoons deprive individuals of contrasting political discourse. Without knowledge of divergent political discussions surrounding the common ethical-political narrative and discourse that could resonate and promote shifts in political positions, individuals are effectively isolated from the range of discourse that is aimed at altering ethical-political norms to reduce social injustice and enhance social cohesion. If slavery were still a legitimate practice in North America and all news provided to North Americans offered reasons justifying the validity of this practice, slavery would be less likely to be abolished than in an environment where such cocoons were more challenging to develop and reinforce.

Privacy protects individuals’ liberty, autonomy, and secrecy. It mitigates the problems and dangers brought on by panoptic technologies by ensuring that individuals can freely associate, communicate, and argue with one another without fearing that they are either being surveyed or captured and inserted into meticulously crafted data cocoons. Privacy is valuable because it shields the essential liberties that citizens require in order to develop and express both their private and public normative attitudes, attitudes that provide the foundation for the political discourse responsible for maintaining citizen-solidarity. As we will find, when contemporary notions of copyright accompanied by surveillance infrastructures power by deep packet inspection devices are prevalent, there is an expectation that the negative impacts associated by an infringement on privacy norms will manifest.

Contemporary Digital Expression Through Mash-up

The public domain operates as the basis “for our art, our science, and our self-understanding. It is the raw material from which we make new inventions and create new cultural works.”¹³ Historically, the majority of our culture was found in, and excavated from the public domain but in the face of an ever-extending capture of the public domain by the advocates of copyright term extensions mash-up artists and citizens have taken to the ‘net to (re)generate their cultural heritage. Mash-up matters because it’s the beachhead upon which cultural activists are mounting their critiques about the current legal conditions of their cultural existence on the basis of their need to express themselves as individuals, as communities, and as citizens. Mash-up matters because if the dogs-of-law do not release this mode of cultural formation from their jaws, then the equivalent of the future’s jazz and rock-and-roll will be criminalized, jeopardizing the future electronic culture. Ultimately, mash-up matters because it can be read as the exemplar of the praxis of digitality itself, as a call to arms against the closure of the commons to the amateur.

Contemporary digital technology facilitates massive engagements with culture. Whereas folk and jazz music alike historically saw relatively small groups coming together to ‘remix’, or modify, add, and subtract, pieces of musical scores (often in an ad-hoc process) the Internet has given today’s electronically-enabled equivalent of folk and jazz musicians a global group of collaborators that is accompanied by an international audience. In front of this audience they expose themselves, reveal their communities, and state their civil positions.

Authors such as Lawrence Lessig, Paul Virilio, and Matt Mason have recognized that there has been a shift in the velocity and virtuality of informatic-creation, movement, and communication. In his recent book *Remix*, Lessig argues that there is a kind of ‘Read-Only’ culture – one where citizens can only receive and enjoy culture in relatively static ways – and ‘Read-Write’ culture – a cultural situation where citizens can modify and freely exchange new cultural creations with relative ease.¹⁴ In the former, cultural artifacts are intended to disclose their agency on their creators’ terms, refusing to let the audience engage with the meanings of the work itself to unlock its creative possibilities. In an era dominated almost exclusively by Read-Only culture, expensive equipment and/or highly specialized training was required to take up film, music, and similar ‘technical’ arts to creatively engage with the material itself in a way that directly copied and implicated the content itself in the development of new cultural artifacts. In the latter situation, culture’s agency becomes shared between the artifacts and those engaging with it: culture gains the potentiality of becoming massively ‘active’, as it was in the heydays of folk and jazz music. In this latter situation, the fan of Harry Potter can express herself to the world through fanfics, associations of Potter fanfic writers can express the value of the work to their community, and as citizens can use the Potter novels and their creative appropriation of it to fight against overreaching copyright efforts to silence their creative, active, engagements with dominant cultural artifacts.¹⁵

While discussing the globalization of communications networks and the heightening velocities of contemporary technologies, Virilio ominously writes that we understand nothing of the information revolution, nothing of digitality itself, unless we recognize that it “ushers in, in purely cybernetic fashion, the *revolution of generalized snooping*.”¹⁶ With the shift toward the ever-increasing standardization of the digital ecosystem – manifest in Internet’s technical architecture in the TCP/IP protocol suite, standardized ‘content containers’ such as JPEG, MP3, AVI, and uniform modes of measurement and data traffic signature analyses – comes the capacity to monitor, control, and mediate the content enclosed in such standardized containers. Simultaneously, there is a division of objects themselves, a mass multiplication and exponential enumeration of them because “data objects *are nothing* but the arbitrary drawing of boundaries that appear at the threshold of two articulated protocols.”¹⁷ Protocol, the medium binding and delivering cultural artifacts, functions as an instrumental or technical addition, as a necessary element of control that rests upon and frames the playful capacities inherent with digitally mediated cultural expression. The protocol that facilitates the playful engagements of youth with their culture simultaneously establishes the mesh within which their cultural artifacts can be scanned, probed, analyzed, and censored. The very technologies that lower the barrier of entry to cultural engagement are simultaneously the technologies that are leveraged to make ubiquitous monitoring of copyright infringing cultural objects and expressions possible.

The search for control over intellectual creations maps onto the logic of perfect control announced by James Boyle: there is an argument, routinely touted by copyright holders, that the strength of intellectual property rights must vary inversely with the cost of copying to ensure a vibrant for-profit cultural environment. He calls this ‘the Internet Threat’, the stance that “without an increase in private property rights, cheaper copying will eat the heart out of our creative and cultural industries.”¹⁸ It is (partly) in reaction to this broad notion of the Internet Threat that Mason examines the effects of the rapid development of the digital ecosystem, and digitality’s potential to enable citizens to engage with cultural artifacts in new and novel ways.

A clear result of the digitization of cultural artifacts has been the near-instantaneous delivery of cultural content to meet the desires of particular individuals. This is evidently manifest following Napster’s explosion onto the digital scene, which subsequently led to branding filesharers as pirates. Instead of seeing pirates as the doom of culture, Mason asserts that “[p]irates highlight areas where choice doesn’t exist and demand that it does... this mentality transcends media formats, technological changes, and business models.”¹⁹ A component of transitions to digitality, in particular, include the ability to enjoy and develop culture through ‘remixing’. Somewhat formally, we can define remixing in the digital context as “about taking something that already exists and redefining it in your own personal creative space, reinterpreting someone else’s work your way . . . It’s about shifting your perception of something and taking in other elements and influences . . . your originality should outshine the borrowed elements, or at the very least, present them in a new light. A

good remix adds value to something."²⁰ In the language of generating cultural meaning, this implies that with the emergence of a new set of tools (cheap, yet technically sophisticated computer software and accompanying cheap, yet powerful, computer hardware) and new communications mediums that realign 'personal creative space' from 'a youth's basement' to 'a youth's YouTube channel or BitTorrent tracker', today's cultural provocateurs have begun 'editing out' their own cultural commons. The challenge they face might be put thusly: the public domain and the relative anonymity provided in a world of analogue search-and-lawsuit practices are being dissolved in the face of legally driven protocological conflict. This conflict is one over who has a right to police (or not) the digital containers of culture (.avi, JPEG, etc), who can or can't (un)lock the shackles of law that either do, or threaten to, enclose the technical playfulness and cultural generativity of the digital era.

Witnesses to the neo-capitalist monopolization of the public domain, and to the dissolution of the possibilities of anonymity, youth and other participants in the recombinant digital culture movement are under legally sanctioned siege, a siege that threatens the development of cultural artifacts while simultaneously criminalizing an outrageous percentage of the population.²¹ With the birth of laws intended to sever citizens' communicative connections to their governments, banks, and fellows – laws such as France's 'three-strikes' law and suggestions that are contained in the Anti-Counterfeit and Trade Agreement presently being negotiated in secret from the public – there is a real danger that participating in remix culture, making one's voice heard, could result in year-long (or longer!) periods of digital voicelessness. While copyright is intended as a government grant intended specifically for the benefit of society, *not* necessarily for rightsholders, copyright is being leveraged to potentially silence the population that is becoming involved in the equivalent of active reading in the digital era; copyright threatens to impose passivity and limit cultural creations to those sanctioned by copyright.

As noted by William Patry, Senior Copyright Counsel at Google Inc., ex-copyright counsel to the US House of Representatives Committee on the Judiciary, and law professor, "[t]he fundamental freedom at stake in copyright, therefore, is the freedom of the public to enjoy new innovations, to access and use information, freedoms that can be curtailed if and only to the extent that such curtailment is necessary to ultimately benefit the public by giving limited incentives to authors."²² Given that mash-ups exhibit positive contribution to cultural development (insofar as they develop new modes of perceiving the world and facets of agentic power) and encourage the public's engagement with the media they are immersed in, they must be seen as a public good. Excessive copyright enforcement that limit mash-up cultural expression upset the balance between the privilege granted to rightsholders and the public good; barring a shortening of copyright periods, new approaches to understanding the use and sharing of copywritten material is needed if the public good is to be served.

To summarize, mash-ups matter because they can be seen as the resurgence of the past, of a time where individuals could take up and share the cultural artifacts they

were immersed in. This resurgence shouldn't be understood as a nostalgic reminiscence of the past but as constitutive of practical attempts to reclaim the cultural constructs that citizens have been embedded in over the course of their lives, but are often legally prohibited from engaging with. Mash-ups, in their massively available form, are presently made possible through the usage of contemporary computer systems; the systems of simulation that can be used to play video games, listen to music, and display YouTube videos are the same systems that encourage cultural generativity and massively shared instances of self-expression. Code can be, and is, taken from disparate sources, tinkered with, and subsequently emitted to the Web. This is an example of mash-up culture. Various musical albums that span genres are recombined in fits of creativity to generate new conditions for cultural possibility. This constitutes a mash-up. Citizens draw pieces of video from music videos, news reporting, advertisements, and government announcements to inscribe their own social, political, or banal commentary on the actions of the day. This too, is part of mash-up culture. Each of these three (of many more!) elements of mash-up culture play a role in defining how the digital generation will engage with their world; this generation has moved well beyond the recombination of words in blogging, to the recombination of the audio-visual facets of culture to transmute sterile corporate cultural artifacts into invigorated and vibrate artifacts endowed with cultural meaningfulness and life.²³ Where this capacity to breath life into corporate culture is endangered because of massive new surveillance infrastructures designed to 'better' enforce copyright laws on the public, to better keep cultural artifacts and their associated meanings from being used by the people's themselves, we will find ourselves facing a threat to both psychic and civil liberties. Mass surveillance for copyright purposes threatens to make all communications on the Internet 'public' and automatically subject to search-and-(law)suit. This encourages a normalization of digital communications and a passivity to creative ways of taking up cultural artifacts and meaning. Thus, there are psychic (issues of perpetual publicness) and civil (freedom of expression) issues at play in the ubiquitous surveillance of digital systems for infringing copywritten works, surveillance that infringes on our rights an needs for privacy and runs counter to the encouragement of discursive possibilities engrained in liberal constitutions. Prior to out engaging with this stream of argument any further, however, let us turn to the deep packet inspection technologies and outline how they in particular threaten to more efficiently enforce copyright than any other technology created to day.

The Stated Capacities of Deep Packet Inspection

Internet service providers are generally confronted with the task of ferrying massive amounts of data on the behalf of their customers; this is the core of their businesses. These lieutenants of Charon have historically been expected to limit the 'intelligence' of their networks; they were expected to avoid examining the content of data that coursed through their digital rivers-Styx, similar to how we expect postal carriers to concern themselves with addresses of postcards we send and not the content of our messages. This expectation and (for some time) reality of data transit

did not accidentally emerge, but was seen as key to the development and expansion of the contemporary Internet network.²⁴ As ferrymasters of data, ISPs are expected to be concerned with collecting their silver coins (i.e. customers' payments for the delivery of data) and subsequently sending data to its destination.

Obviously in an era of distributed denial of service attacks, botnets, spam email, and other high-bandwidth threats directed towards service providers' networks the networks must become increasingly 'intelligent' to address the new and rapidly evolving threats that would undermine customers' access to the Internet at large. The ferrymasters cannot remain amnesiac – data patterns, growth projections, and threat analyzes are routine and required – and this paper is not intended as a broad-sided critique against intelligence from a 'smart ends, dumb networks' perspective. Instead, I want to focus on an important technology, deep packet inspection, that has been widely deployed throughout Canadian service providers' networks, and the globe more widely, to make networks remarkably more aware of the data traffic flowing through the networks and modifying transit speeds depending on what traffic is 'in the pipes'.

Many of Canada's Internet service providers use deep packet inspection to modify and mediate the delivery of web content and enhance their networks' security. In Canada, content that is stitched within technical protocols used by peer-to-peer applications such as BitTorrent and Limewire is regularly delayed.²⁵ This means that the users of these peer-to-peer technologies are often unable to achieve the advertised peak data transmission rates because inspection equipment analyzes the data traffic, detects it as peer-to-peer traffic, and subsequently 'throttles', shapes, or otherwise delays it.²⁶ Such delays do not necessarily *prevent* the delivery of content, but can promote highly variable download times. As an example, when reporting on recent regulatory filings about Canadian providers' use of deep packet inspection equipment, the Canadian Broadcasting Corporation noted that they had lawfully made available an episode of *Canada's Next Great Prime Minister* on peer-to-peer filesharing services. Canadian service providers' deep packet inspection equipment delayed data traffic because of the data transfer protocols being used, to the extent that consumers completed downloading the TV episode two-and-a-half to ten hours later.²⁷

Not only do Canadian instantiations of deep packet inspection equipment delay lawfully shared content contained by peer-to-peer protocols, but also infringing content bound in the same protocols. Rapid access to content is contingent upon adopting a protocol that either evades or escapes the service providers' filters, is encrypted and thus more challenging to identify, or is seen as permissible by the provider. In effect, Canadian Internet providers are determining what are appropriate or inappropriate protocols for content delivery. Cultural objects that carry with them meaning can be made available at a speed contingent on the method taken to contain and transmit the content. That telecommunications carriers are taking it upon themselves to choose winners and losers of emerging protocols is not a positive development given that innovative technological development in telecommunications

does not tend to happen when carriers are responsible for the innovation – any brief turn to the monopolistic activities of AT&T during the 20-70s demonstrates this²⁸ - which should raise warnings about the possible implications of Internet service providers controlling what is an acceptable mode of cultural artifact (and thus meaning) distribution.

For our purposes, however, what is perhaps most significant is how deep packet inspection can analyze not just protocols used to contain content, but also analyze the content itself. To give a sense of the power of these devices, we can turn to Nate Anderson's seminal news piece on the technology. Procera's deep packet inspection devices have the potential to "look inside all traffic from a specific IP address, pick out the HTTP traffic, then drill down even further to capture traffic headed to and from Gmail, and can then reassemble e-mails as they are typed out by the user."²⁹ In the case of Canada's service providers they have deployed deep packet inspection in their network infrastructures in varying ways – in some cases the technology only examines the properties of how data is exchanged between parties, in other cases it examines the application layer (protocol space that most closely surrounds and includes content) of data traffic – and many who have deployed the technology note that their deployments could, theoretically, be repurposed to identify data traffic even more granularly.³⁰

There are at least two approaches to identifying, and limiting, the movement of copyright infringing data traffic across service providers' networks in near-real time: fingerprinting, and file hash-based identification and blacklisting. Fingerprinting relies on capturing parts of a file to generate a unique representation of the file in question. Thus, in examining the pieces of data holding one of Girl Talk's tracks, such as 'Like This' – which contains twenty-nine samples in three minutes and twenty-one seconds – it would be possible to recognize its elements as coming from copywritten work. It's less evident that the fingerprinting would uniquely detect the data flows as one of Girl Talk's tracks. This technique has the advantage of identifying infringing material even if it's been changed, or remixed. ipoque notes in one of their whitepapers, "Copyright Protection in the Internet," that the issue with this mode of analysis is that it is computationally expensive, and thus cannot presently be implemented in real-time network environments. You need to capture files for analysis, and this has associated data-retention and privacy issues. Moreover, this mode of examination cannot penetrate encrypted file archives or data traffic. If ISPs adopt fingerprinting, more infringing material will be encrypted, which will render this mode of analysis (effectively) useless. Encryption, not computational power, should be seen as the key issue on the basis that computational power is always becoming more available at lower and lower costs. Key to note is that this mode of content analysis would flag mash-ups, creative modes of cultural meaning generation and expression, which rely on copywritten cultural content as infringing material.

Let's now turn to the second approach, which includes both file hash-based identification and blacklisting. When a piece of software or video is released onto torrent

sites, it is often provided in a series of different formats. Each of these differently formatted files has a unique hash identifier (e.g. playme.avi and playme.mpg would play the same content in a different file type), and the 'format shift' can lead to multiple hash codes being associated with the same content (ipoque sees the common ratio between a title and its copies as 1:3-6). Traffic managers can maintain at least one million hash entries and selectively block/allow file transfers. These managers, and their analysis of hash identifiers, are effectively deployed against unencrypted public file-sharing environments. Under this approach, when mash-ups with infringing content are detected, they could be added to the database of illicit hash identifiers and prevented from subsequently being shared between parties.

At the moment, deep packet inspection appliances allow for this kind of analysis and blocking, but ipoque maintains that whole countries or larger regions would need to participate in a common anti-infringement strategy for hash-identification to effectively stop or limit infringement. The company suggests Internet service providers' subscribers would have to pay roughly 2-3 Euro/year to subsidize the added expense of this filtering regime. Such a system would situate service providers as guardians of content, extending their dominion beyond masters of protocol.

Before moving on to address how either of these surveillance regime impact the capacity to freely generate and express cultural meanings and engage in communications without the experience of chilling speech, it is important to address the two modes by which data traffic can be analyzed. Traffic can be subject to either active or passive monitoring. Active monitoring is reminiscent to how various copyright agencies identifying those infringing on copyright; copyright holders, or agents working on their behalf, use a P2P program to connect to infringing peers, copy their IP addresses, and subsequently associate those addresses with their end-users. Passive monitoring, on the other hand, "inspects the complete Internet traffic, ignoring all uninteresting traffic and looking only for exchanges of copyrighted titles."³¹ ipoque recognizes that this would cause "severe privacy and data protection concerns as it has, potentially, access to all data, including e-mails, web traffic, etc. *The two methods – active and passive monitoring – are totally disparate technologies.*"³² Active monitoring has received incredibly negative attention, and ipoque argues that passive monitoring "is politically unfeasible in most countries"³³

In the case of analysis of data traffic by Canadian Internet service providers and other providers using deep packet inspection equipment, *passive* monitoring is being performed. Virgin Media, in the UK, has gone so far as to deploy passive deep packet inspection systems to monitor and analyze data traffic on their network to identify infringing traffic.³⁴ As such, the worries that privacy advocates are identifying and vocalizing emerge because this kind of packet inspection is primarily being used for passive monitoring that extends beyond 'subscriber management' systems that are meant to permit access to services depending on broadband package, or for allocating bandwidth according to what you pay for monthly. Passive monitoring facilitated by deep packet inspection is, in effect, a dragnet surveillance apparatus that is being massively applied to Canadians, and Western citizens more broadly.

Deep Packet Inspection and the Canadian Situation

In 2008-9 there was a CRTC regulatory hearing about Canadian service providers' use of deep packet inspection equipment to manage their networks, as well as an examination of the technology by the Office of the Privacy Commissioner of Canada. In the face of requests of technical disclosure in Canada, none of Canada's service providers actually provided the equipment or model numbers of their appliances to the public record, and this information is key to engaging in an open, public, debate of the merits and dangers posed by the technology given that each appliance has slightly different characteristics. Many service providers were forced to reveal that they were, in fact, using deep packet inspection appliances at all by the CRTC (this information was initially filed in confidence by many carriers in the proceeding), but none were required to disclose the technical capacities of these devices to the public. The dominant carriers are unanimous that their technologies, as presently configured, do not allow for genuinely massive surveillance, with only CRTC officials knowing full the veracity of these claims.

Cogeco, one of Canada's larger ISPs, has noted in response to privacy and surveillance concerns raised by members of the public and advocacy groups involved in the hearing that, "with respect to the possibility that DPI technology can look into the content of a message sent over the internet, like reading the content of an envelope sent by surface mail, Cogeco would like to make clear on the record of this proceeding that the DPI equipment implemented by Cogeco has limited capacity and is not used in any manner to identify the content embedded in the packets exchanged by P2P users on Cogeco's network. While, like any network device, these devices could allow examination of the content of a packet, it is simply not within the capability or capacity of these devices to do so across the thousands of subscribers and multi gigabytes of traffic that traverse these devices per second."³⁵ Note that, despite 'clarifying' the record, the public is left without a clearer understanding of what is being done to their packets now than prior to the proceeding. Are dominant carriers using deep packet inspection appliances that *can* be configured to respond to copyright infringement? Are the appliances dominantly engaging in heuristic analysis of packet transfers, or are they examining the application layer? Do these devices permit the analysis of packets as they cross a router and, as flows are identified that correspond with input signature types, copy particular streams of data for offline analysis and release to authorities? In a limited fashion, can these devices be used for lawful intercept purposes?

Some deep packet inspection devices are touted as being able to perform all of these actions, but many cannot; in effect, different devices carry with them different surveillance potentials. Without disclosing information on their actual network topologies, consumer groups and interested Canadians are left guessing about what Internet service providers are using to monitor and adjust packet flows. Without an understanding of the technologies, service providers can say that their devices are neither privacy invasive nor particularly useful for law enforcement without having to substantiate their arguments before the public eye. By filing the equipment that is

used to manage networks in confidence with the CRTC, Canada's service providers effectively undermine the public's ability to critically engage with the capacities of these devices in a meaningful way.

Canada's dominant carriers regularly reminded members of the Canadian public that the CRTC was to focus exclusively on traffic management in the proceeding last year, and that deep packet inspection technologies are just an element of that broader effort of managing their networks. As a result, they insisted that the proceeding not be about the technology itself;³⁶ addressing the technology would miss the point – what needed attending to were its particular uses. Only when a worrisome use is realized should the CRTC or other appropriate government agency become involved. Each dominant carrier asserted that a case-by-case approach to the technology needed to be adopted, where particular applications of deep packet inspection and particular instances of traffic management are examined, rather broad rulings about the technology as a whole.

The problem for consumers is that it can be incredibly difficult to learn how packet inspection appliances are actually being used by carriers; in the United States it was largely by happenstance that ad injections³⁷ or Comcast throttling³⁸ was identified as effects of deep packet inspection appliances. The UK's Phorm recognizes that they need to achieve greater 'transparency', but rather than suggesting that this means a greater degree of public divestiture of their operations, it means that end-users should never realize that Phorm is combing their traffic to insert advertising.³⁹ Achieving 'transparency' when using packet inspection appliances often means that individuals cannot determine the source of delayed packet transmissions or modified web pages; is it a bad application, a bad file transfer, or (in the case of a wholesale ISP customer) interference from my Internet service providers' service provider?

Refusing to disclose the discriminatory elements of the information system that Canadians, and other Western citizens, depend on to express themselves and engage with their culture endangers the willingness to participate in one's culture through expression, as denoted in the discussion of privacy earlier where individuals self-censor out of caution and fear. Being genuinely transparent – revealing the intricacies of the technologies undergirding the ISPs' management systems - doesn't *necessarily* require dominant carriers to reveal the particular devices installed on their network, but at the very least requires them to provide complete and honest accounts of the devices' full range(s) of possibilities and capacities. Without detailed accounts of what is possible with these technologies – instead of merely stating that they are 'not privacy invasive' – advocates cannot develop concrete arguments based on the particular merits and disadvantages of the deep packet inspection appliances that are in use. This establishes an epistemic distance between Internet service providers and interested parties; parties are forced to 'trust' service providers. As has been noted by new competitors in the wireless data and voice market in Canada, consumers have long memories when it comes to Canadian telecommunica-

tions companies, and they have developed a significant distrust of the longstanding dominant carriers.⁴⁰

In light of the importance of the network topologies that are presently shrouded in mystery, service providers and vendors alike should come forward to disclose the conditions under which their technology can monitor, delay, block, or censor content. Moreover, parties that have deployed these technologies ought to be regulated and required to provide this information to their customers. It is insufficient to have a provider report in total confidence to a government body, given that this is a matter of dealing with citizens' liberty. In Canada, the CRTC is not ideally suited to deal with privacy concerns, and the federal privacy commissioner similarly unsuited to understand the technical elements of ISP networks. There are, however, civil advocacy groups that regularly present before both government bodies that retain this skill and expertise in-house. Denying the civil watchdogs access to the information needed to either alert the Canadian public to a danger or allay fears is problematic and lends to positions that civil advocates must adopt 'fundamentalist' rather than 'pragmatic' approaches to these new technologies. Arguably, the 'pragmatic' advocacy is more constructive, whereas the fundamentalist approach functions to stop, prevent, or undermine technologies that are perceived as possibly infringing on individuals' privacy. To maintain the use of technologies such as deep packet inspection for positive purposes – security, subscriber billing, and so forth – it is essential that service providers in particular be open and candid with civil advocates so that the discussion can genuinely turn to the uses of the technology as opposed to the technology itself.

Fundamentalist versus Pragmatic Advocacy

In his recent research into the nature of privacy advocates around the world, Colin Bennett developed a six-part typology of advocates. It is his first category, that of privacy activists, that I want to first address and describe how these activists relate to what I am terming 'privacy fundamentalists'. I will follow by briefly offering an account of a privacy pragmatist, and conclude by arguing that the evidence of function creep, combined with dominant carriers' market power and epistemic privileges, mean that advocates logically ought to lean towards fundamentalist stances towards the Canadian use of deep packet inspection given the lack of Internet service providers' transparency on the actual technical systems in use. Such a logical lean can, and should, be countered by service providers by being more transparent about the full capacities of their packet inspection equipment, and such transparency can simultaneously alleviate some of the psychic dangers arising from the perpetual experience of being under surveillance.

The Activist/Fundamentalist

Activists are differentiated from advocates, insofar as they are 'seen to be doing something'. These individuals and groups "do not balance privacy against competing public interests, because they know that the opposing arguments will always be made with force and by people with far more resources than they have. For some

advocates, the privacy argument requires uncompromising articulation rather than negotiation with competing social interests".⁴¹ Principles fuel activists, and they are not interested in 'balancing' their principles with other social interests or technological aims. The ideal type of activist is solely devoted to the 'cause' of privacy (however that happens to be defined), and is rarely forced to compromise their principles for financial or political reasons.

In adopting deep seated, ideally unshakeable principles, activists are often driven by what Daniel Solove terms 'nonconsequentialist accounts of privacy's value.' These accounts can be grounded in a Kantian or neo-Kantian rights-based discourse, where freedom and autonomy of persons are seen as a core, or even necessary, social good.⁴² Securing the individual's, and society's, privacy rights is necessary to guarantee the dignity of each member of society; even when information is gleaned about a person without intent to generate harm or influence their behaviour that inspection must be resisted.

With entrenched attitudes concerning privacy that are (hopefully) grounded in argumentative reason and fact, fundamentalists will oppose new technologies that they perceive entering a market and endangering whatever conception of 'privacy' they happen to hold. Such definitions are not necessarily identical, or based on the same foundations; privacy advocates of various stripes, motivations, economic and social backgrounds are well known to band together when a common threat faces them.⁴³ These groups are not necessarily concerned with the intricacies of a problem – what deep packet inspection might solve, what it might be possible or incapable of doing – and instead argue on the basis of principle. While principle guides the privacy pragmatist as well, they tend to adopt more flexible approaches to privacy concerns.

The Pragmatist

Pragmatists perceive a need to modulate radical or extreme privacy positions if they are to have a seat at the bargaining table that is deciding how to implement a privacy compromising action or policy.⁴⁴ Simon Davies terms these individuals 'pragvocates'.⁴⁵ Daniel Solove writes that these individuals acknowledge that "[p]rivacy should be weighed against contrasting values, and it should win when it produces the best outcome for society. A pragmatic approach to valuing privacy involves balancing it against opposing interests . . . We determine the value of privacy when we seek to reconcile privacy with opposing interests in particular situations".⁴⁶ Whereas privacy fundamentalists will uphold particular understandings of privacy regardless of the social situation, pragvocates want to know what the situation on the ground is; what technology is being deployed, how might privacy be compromised, are there methods of ensuring that privacy interests are upheld while meeting the compromiser's goals?

This stance is sometimes evidenced in the actions of Canada's privacy commissioners; they often work *with* companies, rather than operating as fundamentalist advocates of privacy. Such actions reveal beliefs that cooperation leads to more deeply

engrained privacy protection in most cases than adversarial engagements. Pragmatists, such as Dr. Ann Cavoukian, insist that it is important to work within an existing system and adjust it so that all parties win.⁴⁷ This attitude orients her 'PET+' and 'Radical Pragmatism' approaches to guaranteeing privacy in a digital world; by integrating privacy enhancing technologies into the very infrastructure and code of otherwise privacy compromising activities, it is possible to meet social interests aimed at maintaining personal privacy while also meeting corporate and governmental surveillance objectives.⁴⁸

It would be wrong to assume that pragmatists are somehow themselves 'compromised' or have 'turned coat'. Adopting case-by-case approaches, where they rigorously consider the facts of a situation and then make recommendations based on the facts of the environment, is a challenging and oftentimes socially rewarding task. Their actions are often rooted in empirical fact and grounded in a principle of fairness that encompasses groups that may be compromising privacy as well as those who are being compromised. This pragmatic sensibility, combined with empirical evidence, enables pragvocates to extend their influence to governmental decisions, where providing useful information to regulators leads to heightened personal and organizational respectability.⁴⁹ Such respectability can be leveraged in subsequent privacy-related drives, meaning that 'successful' pragvocates are far more likely to have a hand in steering how privacy compromising policies are developed than fundamentalists, who often stand outside the corridors of power.

Canadian Privacy Advocacy and DPI

What I see as key to these discussions, however, is that the pragmatist often depends more highly on empirical information to engage in a case-by-case approach to potential compromising actions than the activist. While activists are certainly not *opposed* to learning about the situation, they are more willing to modulate information for their own fundamentalist purposes.⁵⁰ The challenge before privacy (and, by extension, consumer) advocates is that it is difficult to engage in an empirical approach towards deep packet inspection devices deployed by Canadian service providers on a case-by-case basis because of the phenomenal lack of empirical data that has been made available to the public. As a result, while a pragmatic approach is needed to *temper* an activist position, we must worry about the potentialities of deep packet inspection devices as they relate to the possibility of massively compromising Canadians' privacy. The danger in focusing on a case-by-case approach, without knowledge of what the devices can natively be configured to do, is that while *at the moment* they may not be configured to massively compromise Canadians' privacy, a reconfiguration might go unnoticed because of the secrecy cloaking ISPs' networking operations. While at the moment the devices are presumably configured for the purposes of economic efficiencies, will they remain so configured in perpetuity?

It is this lingering question and accompanying worries that haunts the activist, and what motivates opposition to these technologies. While pragvocates may work within the system, taking account of the broader variables that likely direct service

providers in their present attitudes with these devices, they would be well served to ask what is next, and what is possible. I would suggest that a full-blown fundamentalist position is unlikely to be helpful in engaging in discussions of deep packet inspection appliances in Canada, but that a strident voice the opposes the compromising of privacy ought to be adopted given the relative lack of information that Canadian service providers have placed on the public record about the potential of their devices. Given that we have already seen Bell take advantage of their devices' potentialities when they expanded their use from subscriber monitoring to peer-to-peer traffic throttling, we would be well served to keep in mind other possible avenues of function creep. Adopting a dominantly case-by-case analysis of technologies without knowing their specific attributes risks missing the concerns and dangers related to deep packet inspection-enabled function creep; it risks missing the forest through the trees.

Deep Packet Inspection and Civil Dignity

Central to the healthy functioning of a democracy is the ability to engage in radical, non-violent, critique of political, ideological, and cultural tropes and actions. This is a long held tradition – going back at least as far as Kant, with his concept of the freedom of the pen – and is intended to encourage the critical engagements of citizens so that they can develop more nuanced understandings of the environments they find themselves in. More of a contemporary than Kant, Habermas recognizes that citizens regularly engage in a discursive process that, ideally, adheres to the following rules;

1. Every subject with the competence to speak and act can take part in the discourse.
2. a. Everyone can question any assertion whatsoever.
 - a. b. Everyone can introduce any assertion whatsoever into the discourse.
 - b. Everyone can express their attitudes, desires, and needs.
3. No speaker can be prevented, by internal or external coercion, from exercising their rights as laid down in (1) or (2) above.⁵¹

Where citizens engage in discursive processes through the creative appropriation of corporate culture and use it as a way of introducing assertions, expressing attitudes, desires, and needs, then the usage should (normatively) be permitted. I am limiting such expressions to the domain of mash-up cultural expressions, on the basis that such works regularly challenge and contest normalized processes of cultural development and citizen-living. That such challenges are nascent in musical mash-ups is evidenced in Mallory O'Donnell's critical appraisal of Girl Talks' 2006 album *Night Ripper*. O'Donnell writes;

While the genesis of the mash-up lies somewhere between the club DJ and the pop fan's smirk, *Night Ripper* eschews dancing and deconstruction for referential meta-ménage and just plain destruction. It's the logic of John Cage's radio

concerts and Philip Jeck's turntable shows applied to the digital pop venue, edited down to milliseconds by Gregg Gillis' maniacal mouse-tapping. Nothing could be more indicative of the position in which we find ourselves in the post-everything world: gleeful, violent, lusty, grinding robots bent on thoroughly devouring both our own souls and those of our creations.⁵²

O'Donnel's language captures the creative and important essence of Girl Talk's contributions; Greg Gillis (the real name behind the stage name) is expressing a cultural epoch through his creations. The language that he uses to communicate is not inherently the critico-rational discursive tones that are associated with 'traditional' discourse, but see culture itself and its performance as a discursive movement. Habermasian sensitivities to religious discourse in his more recent writing certainly indicate that any cultural expression of discursive possibilities must be honestly regarded and taken up as an element of a discursive process. Moreover, with this in mind an effort to prevent such expression, when the prevention itself does harm to the discursive possibilities of the group, should be normatively disallowed. Limiting the distribution of mash-up cultural artifacts intended dominantly for cultural appreciation (read: those not dominantly intended for commercial success) should not be prevented from being created or disseminated. Demands that high tariffs be paid out prior to creation and distribution, on the basis that the creative work infringes on copyright, suggests that the politico-economic understanding of culture is out of line with national principles asserting the value of constitutionally sanctioned free speech for purposes of national development.

Further, and as alluded to earlier, the usage of three-strikes rules to terminate an individual's access to personal Internet services on the basis of copyright infringement creates a powerful disincentive for individuals to actively participate in online environments. Suddenly trying one's hand at a mash-up using Apple's Garageband software, or doing some rudimentary video-editing for political purposes, and disseminating the creation to the 'net at large becomes incredibly dangerous. Depending on one's jurisdiction, just a few seconds of a particular melody or harmony - seconds that the creator might even be ignorant of - can trigger copyright claims. In countries such as the United States such claims can result in demands for thousands or millions of dollars, which is a powerful disincentive to create (and thus undermines the very motivations for providing the privilege of limited monopolies in the form of copyright), but where one might lose the ability to work (in the case of individuals who work for, or freelance from, home), access medical services (with the rise of eHealth initiatives), or read one's power meter (with the coming of the Smart Grid) there is a terrific nervousness that sweeps over any sensible person who contributes a culturally productive mash-up to the global culture machine. This perceived need to avoid radical expression results in a normative unwillingness to exercise one's fundamental constitutional rights based on a fairly evident rational calculus. Thus, to deploy a ubiquitous surveillance apparatus for the purposes of identifying and preventing copyright infringement that would cause substantial harms to rational citizens' capacity to express themselves suggests that deep packet in-

spection devices should not be placed into network architectures without strong laws preventing copyright-related surveillance on freedom of expression grounds.

Levies, Not Deep Packet Inspection

Canadians pay a small levy on some media that is capable of holding recorded music; I wish to briefly suggest that instead of turning to deep packet inspection for surveillance purposes that an exportation of an expanded levy regime offers a superior way to recoup some of the monies that are presumably lost to the trading of file sharing while simultaneously avoiding infringements on citizens' freedom of expression. A hardware-centric (i.e. iPod), rather than an Internet service provider, levy is preferable for a few reasons; (1) a service provider levy puts too much authority and control over content analysis than carriers they explicitly need; (2) service-provider levies might potentially put carriers at risk of legal liability when they misidentify content; (3) a service provider levy would place carriers (which are often for-profit content delivery corporations) in charge of monitoring content without demanding consumers that pay 'full value' for content moving through their networks. This last point indicates that an Internet service provider-based levy may put providers in conflicts of interest (at least in the case of the dominant providers in Canada). It is in light of these issues that I dismiss the notion of an Internet service provider-levy intended to generate a return to content producers because of peer-to-peer file sharing and instead suggest adopting a hardware-based levy.

Canadians, as previously mentioned, are charged a levy on all blank media that is sold. The levy originated several years ago, and was meant to recoup losses from the copying of mp3s (and related audio files) onto disks. The levies on each piece of media is (arguably) very small;

- \$0.24 per unit for Audio Cassette tape (40min or longer);
- \$0.21 per unit for CD-R Audio, CD-RW-Audio & MiniDisc;
- \$0.21 per unit for CD-R, CD-RW (non audio).
- In 2009 the levy on CDs and MiniDiscs rose to \$0.29⁵³

Presumably, fewer people burn mp3s onto disks than in the past – with the advent of cheap and portable storage media, media tends to find its way to mp3 players and similar portable (and slightly less portable) media environments. Rather than imposing levies on service providers' customers a small levy might be imposed on mp3 players/consumer electronic storage equipment. Essentially, were a levy placed on hardware that can store digital content, much of which is arguably copywritten, rightsholders would be compensated and there would be a shift away from demands that ISPs monitor their data networks for infringing content. This shift would be made on the basis that any such content is destined for a storage device, even if storage is temporary. Any levies garnered from devices at their point of sale would then be distributed back to content owners.

Conclusion

Emergent from this piece, it has become evident that in adopting principles of transparency about the development and deployment of deep packet inspection appliances that the public can be assuaged of the psychic harms accompanying worries of ubiquitous, broadly targeted, surveillance of communications. Limiting such surveillance is good on psychological health reasons, but knowing about surveillance doesn't necessarily alleviate the challenges it can pose to citizens' civil dignities, or the rights and freedoms of expression and association bound into Western states' constitutions. Using deep packet inspection that is designed to passively monitor data traffic with fingerprinting technologies for copyright-related purposes, in particular, threatens to deeply stifle the cultural expressions made by mash-up artists such as Girl Talk and, as such, limit the capacity for citizens to develop a language of cultural engagement that feeds into their political involvement.

Given the risks of Internet service providers using deep packet inspection for copyright purposes, a hardware levy-based approach could be adopted. Such an approach would limit worries that service providers have non-network management related reasons for throttling some content, given that they would not be responsible or permitted to track the content crossing their networks. This has the advantage of keeping 'intelligence out of the core' of the network, insofar as the network is made 'smart' enough to address security and network-related threats, but remain 'dumb' enough that it never knows what content, precisely, is crossing through its pipes. As such, it lets providers maintain their core business functions and improve efficiency. So long as service providers are transparent on exactly what they are using deep packet inspection equipment for in a public environment using technical language that can be subject to critical analysis, the psycho-social dangers of a menacing, uncertain, ubiquitous surveillance apparatus being deployed to silently watch all the expression that citizens engage in online might be limited. On this basis, we can conclude with the hope that service providers will either choose, or be compelled through regulation, to not engage in surveillance for copyright-related purposes on the basis that it threatens to infringe on customers' privacy to cause both psychic and civil indignities.

¹ Information and Privacy Commissioner/Ontario (2001) "An Internet Privacy Primer: Assume Nothing," 1.

² Judith Wagner Decew (1997) *IPP*, 75.

³ Judith Wagner Decew (1997) *IPP*, 76.

⁴ Judith Wagner Decew (1997) *IPP*, 78.

⁵ Judith Wagner Decew (1997) *IPP*, 48.

⁶ Judith Wagner Decew, referencing Parrent (1997) *IPP*, 41-2.

⁷ Donald Winnicott (1965) *The Mutational Processes and the Facilitating Environment: Studies in the Theory of Emotional Development*, 140-52.

⁸ While outside the scope of this paper, the issue of what norms the surveying party holds is of particular importance. Without knowledge of the surveyor's norms the problem of ontological security arises, where a person is unable to ground their identity. In environments where actions are being passively monitored without noticeable consequences individuals can experience a compression of public and private spaces and their associated norms. These compressions can lead to extensive spatial neuroses. For excellent evaluations of the effects of the development of neurosis that emerge from the experience of ontological insecurity I refer you to John Russon's *On Human Experience* and R. D. Laing's *Politics of the Family* and *Politics of Experience*.

⁹ Lawrence Lessig (2006) *CV2*, 218.

¹⁰ This analysis of the nation-state is born from Jurgen Habermas' work on the development of the contemporary nation-state.

¹¹ Cass R. Sunstein (2006) *Infotopia: How Many Minds Produce Knowledge*, 97. Hereafter referred to as *I:HMMPK*.

¹² Cass R. Sunstein (2006) *I:HMMPK*, 75 – 102. This is the precise danger that arises when relying on new aggregation services, such as Google News, to collect and deliver targeted news that computational algorithms have identified as 'interesting' to an individuated reader based on their past news interests. Personalized news feeds are useful, insofar as they reduce the time individuals spend searching for news they are interested in, but they simultaneously decrease the likelihood of finding topics that are unrelated to or in contradiction to already demonstrated interests. It is new or contradictory attitudes and philosophies that often spur innovative thinking, whereas persistently receiving the same thoughts and opinions dulls individuals' critical faculties.

¹³ Boyle, James. (2008). *The Public Domain: Enclosing the Commons of the Mind*. P 39.

¹⁴ Lessig, Lawrence. (2008). *Remix: Making Art and Commerce Thrive in the Hybrid Economy*.

¹⁵ For more, see chapter 5, "Why Heather Can Write: Media Literacy and the *Harry Potter Wars*" from *Convergence Culture* (2006) by Henry Jenkins, where he identifies how individual writers use mash-up writing to express themselves, communities are formed to develop and express common thoughts, and the Harry Potter community found methods of enacting resistance to onerous copyright intonations through the lens of politics and civil advocacy.

¹⁶ Virilio, Paul. (2005). *The Information Bomb*. P. 62. Emphasis from text.

¹⁷ Galloway, Alexander. (2004). *Protocol: How Control Exists After Decentralization*. P 54.

¹⁸ Boyle, p. 60.

¹⁹ Mason, Matt. (2008). *The Pirate's Dilemma: How Youth Culture is Reinventing Capitalism*. P. 46. It should be noted that following recent study commissioned by the International Chamber of Commerce, which focused on piracy, Agnete Haaland (president of the International Actors' Federation, stated " [t]o me, piracy is something adventurous, it makes you think about Johnny Depp. We all want to be a bit like Johnny Depp. But we're talking about a criminal act. We're talking about making it impossible to make a living from what you do ... Consumers have to understand that there will be nothing to consume if it's impossible to make money making the content." This is both a manifestation of the Internet Threat and a declaration of war against mash-up, asserting that some modes of content creation (for profit) are superior to others. Link to quotation: <http://www.reuters.com/article/idUSTRE62G3BU20100317>

²⁰ Mason, Matt. (2008). *The Pirate's Dilemma: How Youth Culture is Reinventing Capitalism*. Pgs. 71, 81, and 83. Emphasis added.

²¹ Note to *Remix*

²² p123

²³ I should briefly note: I do not mean to suggest that being a member of today's youth, and connected to the Internet, automatically, mystically, or necessarily endows a subject with a drive to be an active producer and consumer of culture. As put by Terranova in *Network Culture: Politics for the Information Age*, the "process whereby production and consumption are reconfigured within the category of free labor signals the unfolding of another logic of value, whose operations need careful analysis" (p. 75). Mash-ups belong to this category of free labor, where subjects are imbuing their cultural artifacts with this labor and subsequently releasing the mash-up to the world/Internet at large. The danger that the development and deployment of technical systems to monitor, analyze, and limit the sharing of art, to artists, is that this process threatens artists' very 'business'. As Doctorow notes, artists "are in the free expression business, and technology that helps free expression helps artists" (*Content: Selected Essays on Technology, Creativity, Copyright, and the Future of the Future*, p. 70). Thus mass surveillance and control of copywritten material threatens artistic expression, risks condemning copyright infringing mash-up culture to the shadows of law (at best), and generally censors the capacity for individuals to be active readers in the world of hypertext, digital avatars, biodigital hybrids, and recombinant audio-visual fields.

²⁴ Goldsmith and Wu, 22-25

²⁵ For a full categorization of which Canadian ISPs are involved in the mediation of data content using DPI equipment I refer you to my summary document of the January 13, 2009 and February 9, 2009 CRTC filings by major Canadian ISPs.

[http://www.christopher-parsons.com/PublicUpload/Summary_of_January_13_2009_ISP_filings_with_February_9_2009_Updates_version_1.0\(for_web\).pdf](http://www.christopher-parsons.com/PublicUpload/Summary_of_January_13_2009_ISP_filings_with_February_9_2009_Updates_version_1.0(for_web).pdf)

²⁶ The distinction between throttling and shaping traffic is as follows; throttling “applies controls to the amount of traffic flowing into a network in a specific period, buffering (storing) the packets or if necessary dropping packets.” Shaping, in contrast, is “a more complex set of techniques which can control the volume of traffic, the rate at which it is flowing and so on.” (Heavy Reading 2009: 6, Finnie.)

²⁷ News article on this, <http://www.cbc.ca/arts/tv/story/2008/03/26/bittorrent-cbc.html>

²⁸ here would have bit on Carterphone. Also, from Wizards, how AT&T refused to take interest in the ‘net in the first place; didn’t see a reason, didn’t want competition

²⁹ <http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars>

³⁰ Responses to questions 8 and 14 identify conditions that ISPs would consider modifying their present uses of DPI in their networks. Billing, law enforcement/compliance, and security are all cited as possible motivations.

[http://www.christopher-parsons.com/PublicUpload/Summary_of_January_13_2009_ISP_filings_with_February_9_2009_Updates_version_1.0\(for_web\).pdf](http://www.christopher-parsons.com/PublicUpload/Summary_of_January_13_2009_ISP_filings_with_February_9_2009_Updates_version_1.0(for_web).pdf)

³¹ ipoque 2009, p6

³² ibid., emphasis added

³³ ibid., p7. One is left wondering whether passive monitoring would remain politically unfeasible should the shadowy Anti-Counterfeiting and Trade Agreement be formally accepted by participating governments.

³⁴ For more on Virgin’s use of DPI to identify infringing material coursing along their network, I refer you to my summary post, “Aggregating Information About CView” at <http://www.christopher-parsons.com/blog/privacy/aggregating-information-about-cview/>

³⁵ Cogeco 2009b

³⁶ At the Computers, Freedom, and Privacy 2009 panel on Deep Packet Inspection, it is noteworthy that almost all of the participants recognized that DPI does have some valid uses, such as assuring network security. This included consumer groups and researchers who have been critical of the use of DPI.

³⁷ Topolski, Robert M. (2008). “NebuAd and Partner ISPs: Wiretapping, Forgery, and Browser Hijacking,” Free Press and Public Knowledge.

³⁸ Bangeman, Eric (2007). “Comcast shooting itself in the foot with traffic “explanations”,” *ArsTechnica*. Published October 23, 2007. Last accessed June 28, 2009. URL: <http://arstechnica.com/old/content/2007/10/comcast-shooting-itself-in-the-foot-with-traffic-shaping-explanations.ars>

³⁹ BT Retail Technology (2007). “PageSense External Technical Validation”, dated Jan 15, 2007. Last accessed June 28, 2009. URL: https://secure.wikileaks.org/wiki/Image:BT_Report.pdf

⁴⁰ Canadian Telecom Summit (2009). Advanced Wireless Services – The new kids on the block panel. Toronto, June 15-17, 2009.

⁴¹ Bennett, Colin (2009). *The Privacy Advocates*. Cambridge, Massachusetts: The MIT Press.

⁴² Solove, Daniel (2008). *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press.

⁴³ Bennett, Colin (2009). *The Privacy Advocates*. Cambridge, Massachusetts: The MIT Press.

⁴⁴ I adopt the term 'privacy compromising' to reflect the notion that individuals or societies are manoeuvred to offer up facets of information/allow for (re)combinations of information that can be used to discriminate between the delivery of goods, services, and so forth to particular individuals and groups. This diverges from 'invading' privacy, insofar as compromise assumes some process of negotiation, though at differing degrees of legitimacy and explicitness.

⁴⁵ Bennett, Colin (2009). *The Privacy Advocates*. Cambridge, Massachusetts: The MIT Press.

⁴⁶ Solove 2008: 87

⁴⁷ Brown, Jesse (2009). "CCTVs, Biometrics, and self-destructing data," *CBC Podcast*. Published March 15, 2009.

⁴⁸ Cavoukian, Ann (2008). *Privacy and Radical Pragmatism: Change the Paradigm*. Ontario: Government of Ontario.

One can certainly see how the PET+ agenda integrates with Lawrence Lessig's (2006) account of code, where only by integrating democratically legitimated principles within the core infrastructure of technology can democratic and constitutional values be maintained in our techno-code driven societies.

⁴⁹ Bennett, Colin and Charles Raab (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, Massachusetts: The MIT Press.

⁵⁰ Groups such as CASPIAN and Bad Phorm arguably fit within this typography.

⁵¹ Jürgen Habermas (1990) *Moral Consciousness and Communicative Action*, p. 89.

⁵² <http://www.thestyusdecade.com/albums10081.html>

⁵³ http://en.wikipedia.org/wiki/Private_copying_levy#Canada