CANADIAN JOURNAL OF CRIMINOLOGY AND CRIMINAL JUSTICE
FORTHCOMING 2008

TESSLING ON MY BRAIN: THE FUTURE OF LIE DETECTION AND BRAIN PRIVACY IN THE CRIMINAL JUSTICE SYSTEM

IAN R. KERR, MAX BINNIE and CYNTHIA AOKI

Abstract

The criminal justice system requires reliable means of detecting truth and lies. A battery of emerging neuroimaging technologies make it possible to gauge and monitor brain activity without the need to penetrate the cranium. Bypassing external physiological indicators of dishonesty relied upon by previous lie detection techniques, some neuroimaging experts believe in the possibility of reliable brain scan lie detection systems in the criminal justice system. Because future generations of neurotechnology will get smaller and sleeker, will have greater read ranges and could one day have the ability to interface with implantable microchips, some of those experts also believe in the possibility of remote, surreptitious brain surveillance. In this article, the authors examine such possibilities and assert that Canadian courts' current approach to protecting privacy cannot easily accommodate the challenges caused by these emerging technologies.

The article commences with an examination of the 'reasonable expectation of privacy' standard adopted by the Supreme Court of Canada, arguing that various courts across Canada have misunderstood and misapplied the *Tessling* decision by way of an inappropriate analogy. After a description of brain scan lie detection systems, the authors then examine the courts' use of the *Tessling* analogy in the context of brain privacy. In addition to demonstrating the danger in a generalized judicial proposition that there is no reasonable expectation of privacy in information emanating from a private place into a public space, the authors conclude that a more robust account of brain privacy is required and speculate about possible sources of law from which this might derive.

Introduction

When lawyers and judges describe criminal procedure, they often boil it down to two core goals: finding facts and determining guilt (Friedland and Roach, 2004). Understood in this way, the criminal justice system requires reliable means of detecting truth and lies. Research indicates that the capacity for deception is to some extent biologically programmed (Lewis, et al., 1989), that it is an important stage of moral development commencing in children as early as age three (Lewis, et al., 1989) and that, as children, we learn to deceive in order to avoid punishment for acts of disobedience (Freud, 1965; Spence, 2001). It is therefore not surprising that lie detection has become a major preoccupation within the criminal justice system. Although philosophers (Bok, 1982; Frankfurt, 2005), psychologists (Mann et al., 2004) and sociologists (Barnes, 1994) have appreciated the complexity of distinguishing truth from lies, our courts are increasingly looking to neuroscience as a means of reducing the search for truth to the existence or non-existence of certain brain states.

It has been said that we are entering "the golden age of neuroscience" (Bailey, 2003). While neuroscience remains a nascent field of inquiry, there are those who believe that it will one day unlock the mysteries of the human brain. Up till now, the biggest barrier has been the skull. Recently, however, a battery of new imaging technologies makes it possible to gauge and monitor brain activity without the need to penetrate the cranium (Evanson, 2003). A number of emerging neuro-imaging techniques can be used to facilitate lie detection (Ford, 2006). Some allow electrical activity occurring in the brain to be measured externally and remotely. Some can even map and associate electrical activity with certain brain regions and functions.

While the spectre of intercepting brain waves to determine whether someone is telling the truth may seem the stuff of science fiction, some courts have already adopted nascent forms of these technologies (*Harrington*, (2003)). Brain scans are thought by some to have the potential to revolutionize lie detection because they bypass unreliable physiological indicators of anxiety used in older polygraph technologies, focusing instead directly on the brain states provoking those physical reactions (Appelbaum, 2007). While current imaging devices are bulky, obtrusive and conspicuous, future generations of neurotechnology promise to be smaller and sleeker. We are also told that they will have greater read ranges and could one day have the ability to interface with implantable microchips (Gasson et al, 2005).

If these technologies ever live up to their hype, the possibility of remote, surreptitious brain surveillance — whether used by the police or by private actors — poses a potential threat to privacy. Would the constitutional safeguards in our present criminal justice system protect citizens from unwanted intrusions of this sort? Surprisingly, when one considers the current approach to the "reasonable expectation of privacy" pursuant to section 8 of the Charter, adopted by our courts in the context of other imaging

technologies used in the war against drugs, it is uncertain whether we would be protected without clarification from our Supreme Court or the introduction of new legislation

Several courts across Canada have already been called upon to determine whether heat patterns, electrical activities or odours emanating from a private source carry a reasonable expectation of privacy once they enter public space (*Kang Brown,* (2006); *A.M.,* (2006),; *Tran*, (2007) and *Ly*, (2005)). In answering this question, a number of courts have interpreted the Supreme Court of Canada's decision in *R v. Tessling* (2004) as standing for the proposition that once bits of information emanate into a public space, they are no longer private and are therefore not subject to constitutional protection.

In this article we argue that this interpretation of *Tessling* is flawed and that, as brain scanning technologies increase in their ability to monitor and measure electrical information escaping from the skull, this mistake could have potentially disastrous consequences for personal privacy. In the face of the *Tessling* decision, which intentionally conflated the distinction between 'bodily', 'territorial', and 'informational' privacy, we assert that the interception of brain waves emanating from the skull, though functionally similar to the heat emanations at issue in *Tessling*, are not analogous. We briefly contemplate the implications of this in light of broader considerations around 'brain privacy' in the future. In section I of this article, we discuss the Supreme Court's approach to privacy in *Tessling* (2004) and the manner in which that case has been subsequently applied in courts across Canada. Section II examines the current state of neuro-imaging technology and its potential application in the criminal justice system. In section III, we investigate the potential application of *Tessling* (2004) to brain scans and the need to implicate other *Charter* rights, such as the right to security of the person (*Charter*, s.7).. In section IV, we discuss its future implications for brain privacy.

I The *Tessling* Analogy

In the Canadian criminal justice system, a central aspect of the right to privacy is contained within "the right to be secure against unreasonable search or seizure" (*Charter of Rights and Freedoms,* section 8). In determining the scope of this right, courts generally ask whether the police interfered with a person's "reasonable expectation of privacy" (Bailey, 2008). There have been many important section 8 cases, the most relevant in the current context is *R v. Tessling* (2004).

In *Tessling*, the Supreme Court of Canada was asked to determine whether the RCMP infringed the right to privacy when one of its planes flew over Mr. Tessling's house one night without a warrant and fired infrared beams against its walls, measuring the escaping heat in order to determine whether he had a grow-op in his basement. The Supreme Court decided that, because the escaping heat was freely available and easily measured in a public space without entering Mr. Tessling's home, and because the heat patterns were, on their own, meaningless insofar as they did not reveal core biographical information about Mr. Tessling, his "right to be secure against unreasonable search or seizure" remained intact. The Supreme Court concluded that these activities did not interfere with Mr. Tessling's privacy, nor did they constitute a police search in a manner that ought to attract *Charter* scrutiny.

Writing for a unanimous Court, Justice Binnie overturned the decision of the Ontario Court of Appeal, where Justice Abella had decided in favour of Mr. Tessling. Justice Abella focused on the broad intention of the police in using the infrared technology, which was to gain information about activities going on inside of the home without a warrant. At the Supreme Court, Justice Binnie rejected this philosophical approach, choosing instead to focus on the actual capability of the infrared camera used by the RCMP. According to Justice Binnie, the RCMP's infrared picture taken that night was:

> more accurately characterized as an external search for information *about* the home which may or may not be capable of giving rise to an inference about what was actually going on inside, depending on what other information is available. (*Tessling* (2004): para 27).

While explicitly recognizing the potential for gaining insight into the home by aggregating the information, Justice Binnie concluded that:

> External patterns of heat distribution on the external surfaces of a house is not information in which the respondent had a reasonable expectation of privacy. The heat distribution, as stated, offers no insight into his private life, and reveals nothing of his "biographical core of personal information". Its disclosure scarcely affects the "dignity, integrity and autonomy" of the person whose house is subject of the FLIR image (*Plant* (1993): p. 293)" (*Tessling* (2004): para 63).

In addition to this, Justice Binnie was adamant that each technology should be addressed individually according to its present capacity:

> technology must be evaluated according to its *present* capability. Whatever evolution occurs in future will have to be dealt with by the courts step by step. Concerns should be addressed as they truly arise. [original emphasis]. (*Tessling* (2004): para 55)

Despite this clear call for a case-by-case approach, several courts across Canada have since been quick to generalize the *Tessling* decision *by way of analogy*, drawing a comparison between "external patterns of heat distribution on the external surfaces of a house" and other kinds of information that emanate from a private source into a public space (Kerr & McGill, 2007).

The *Tessling* analogy has recently been adopted in the "sniffer dog" cases, where police dogs are used to detect the odour of drugs emanating from the private contents contained in a piece of luggage (*Kang Brown,* (2006)). For example, the Provincial Court for New Brunswick made a direct analogy between drug odours emanating from a duffle bag and heat emanations in *Tessling,* noting that the accused had knowingly exposed the odour to the public (*McLay,* (2006)). In this case and in many other sniffer dog cases, the courts have relied on the *Tessling* analogy to conclude that individuals do not hold a reasonable expectation of privacy in external information emanations. The very same approach has been adopted with digital recording ammeter (DRA) devices used to detect emanations of electricity in and out of a home (*Tran*, (2007)*; Ly*, (2005)).

Crown attorneys in future emanation cases are sure to cite the *Tessling* analogy as a precedent for the following general rule, paraphrasing Justice Binnie in *Tessling*:

> external patterns of [X] on the external surfaces of [Y] is not information in which a respondent has a reasonable expectation of privacy.

While the logic of this general analogy offers elegant explanatory surface appeal, its broad application would have serious negative consequences and in fact requires a significant intellectual leap. By reducing potentially coercive or restrictive state action to atoms, molecules, bits and bytes escaping from a building, backpack or electrical device, by stripping police investigation entirely of its social context, this reductionist approach makes it practically irresistible to think of the information that is emanating into public space as "meaningless" insofar as it does not, by itself, reveal any core biographical information. The *Tessling* analogy therefore has the potential to substantially diminish the scope of section 8 protection in a manner that can only have the effect of significantly shrinking our reasonable expectations of privacy.

What are the implications of this analogy for technologies used to measure brain waves emanating from our skulls? After describing the technologies that do so and their likely future use within the criminal justice system in section II, we will try to answer this question in section III.

II Brain Scans and Lie Detection

Using high powered magnets to intercept, monitor and map brain waves leaking from the skull as a means of determining the truth in a criminal trial would have sounded as bizarre to an attendee of the trials in Salem, 1692, as the notion of "trial by fire" sounds to us today. And yet, this could be where we are heading.

Two neuro-imaging techniques, in particular, have shown promise in brain scan lie detection: Electro-encephalogram (EEG) and Functional Magnetic Resonance Imaging (fMRI) (Ford, 2006).

An EEG is a device that measures the electrical activity within the brain via external sensors (Wolpe, 2005). It is cost-effective and non-invasive. It measures electrical activity with great precision but lacks the sensitivity to determine exactly where in the brain this activity is occurring (Illes, 2005; Wolpe, 2005). The EEG has been employed by researchers as a significantly improved version of the polygraph machine in a technique called "brain-fingerprinting" (Farwell & Smith, 2001). The premise underlying this technique is that the brain releases a recognizable electric signal when processing a particular memory. Unlike the polygraph, which measures and records physiological factors, the EEG is used to measure the brain itself. Using this technique, a subject is shown a quick succession of relevant words and pictures, and the EEG measures the brain waves spontaneously emitted by the brain in response. If the subject is shown something that is recognized, the brain will react by accessing the memory and the EEG will, in turn, record that specific reaction. The Iowa Supreme Court accepted brain-

fingerprinting evidence in the case of *Iowa v. Harrington* (2003). In that case, brain-fingerprinting was used to help exonerate a person wrongfully accused of murder twenty five years after the conviction by demonstrating that he had no recognition of the crime scene.

Since that time, the scientist who performed the test on the accused, Dr. Lawrence Farwell, has patented the technique through a private company called *Brain Fingerprinting Laboratories* with the goal of commercializing it. Dr. Farwell's claim is not that the technology establishes honesty. Rather, it determines whether specific information is or is not accessed by the brain. If a subject were shown a photo of a crime scene, the technique is said to establish whether there were pre-existing memories of the crime scene (Farwell & Smith, 2001). If the subject hears a specific sound, brain-fingerprinting determines whether the sound had been heard before. From a law enforcement perspective, what is remarkable about this technology — assuming it could ever live up to its current hype — is its potential to enable significant transparency. Unless the technology can be circumvented, a suspect interrogated by question and answer would not be able to pick and choose which thoughts to keep private. Should it ever come to pass, a fully functioning version of the technology employed in police investigations or the courts could allow the State to, so to speak, "google" critical facts within the brain of an accused, not exactly as a computer searches a hard drive but with a similar effect — determining whether the memory of a crime scene or murder weapon resides in the data banks of the accused's brain. At least, that is how the technology is sold (www.brainwavescience.com).

While EEG brain-fingerprinting may have the potential to uncover information that an accused person might wish to keep private, it doesn't directly detect deception. fMRI, however, seeks to do just that. fMRI is non-invasive and readily available, but the machinery is expensive and difficult to maintain (Illes, 2005). It currently requires rather large machinery, though that may not continue to be the case in the coming decades. It functions by placing the subject's skull into a magnetic field and then bombarding it with radiowaves (Kozel et al. 2004). The fMRI uses the different magnetic signatures of oxygenated and deoxydenated blood to measure blood flow within the brain. Active areas of the brain require more oxygenated blood than non-active areas. Traditionally, subjects lay on a table with their head surrounded by a large cylindrical magnet like the familiar Computed Axial Tomography (CAT) Scan. Recently, however, designers have begun to create patient-friendly versions with less intimidating readers, raising the possibility in the coming decades of surreptitious use.

The usefulness of fMRI as an alternative approach to truth verification and lie detection is already being tested (Kozel et al., 2004; Langleben et al., 2005). Langleben *et al*. (2005) used fMRI technology to study the neural patterns associated with deception. Male volunteers were attached to an fMRI machine and were instructed to either truthfully or falsely confirm or deny having a particular playing card. When the participants gave truthful answers, the fMRI data showed increased activity in certain areas of the brain. When they provided deliberately deceptive answers, additional areas of their brain (parietal and frontal lobes) were activated. This data along with the results of previous

studies (Ganis, Kosslyn, Stose, Thompson, & Yurgelun-Todd, 2003; Langleben et al., 2002; Lee et al., 2002) suggest that truth is the baseline condition, and that deception is the inhibition of the truth. In other words, telling lies requires more neural circuits than telling the truth. Whenever a person attempts to deceive, additional oxygenated blood is required. One advantage of fMRI is its ability to map the relevant brain regions involved in deception, a process that cannot be achieved by EEG brain finger-printing. The potential of fMRI in lie detection is significant. The brain acts differently when inventing rather than remembering information — and fMRI can detect that difference (Lee et al., 2002).

EEG and fMRI have both enjoyed much positive attention in the scientific community and in the popular press (Abbott, 2001; Talbot, 2007). While neither technique has been broadly adopted in the criminal justice system as of yet, it is not difficult to imagine that technological advances could provide sufficient reliability to gain widespread acceptance in the near future. As noted above, one U.S. court has already accepted EEG brain-fingerprinting as evidence in *Iowa v. Harrington*, (2003). Canadian courts will no doubt have to grapple with similar issues. Whether these technologies will ever measure up to Wonder Woman's "Lasso of Truth" as a means of inducing truth-telling is speculative at best (Moulton, 1943). There is certainly no shortage of hype in the literature. (Talbot, 2007) The future is but a question mark.

III *Tessling* on my Brain

When considering the future of brain scanning in the criminal justice system, it is interesting to contemplate how courts might approach the emerging issue of brain privacy. Given the preceding discussion, it is obvious that brain scanning could have an enormous impact on various *Charter* rights, not only the reasonable expectation of privacy that accompanies the right to be secure against unreasonable search and seizure (*Charter*, s.8) but also the right against self incrimination (*Charter,* s.11c) and the right to security of the person (*Charter,* s.7). While these are subjects of our ongoing research, the focus of our discussion in this section is the reasonable expectation of privacy standard discussed above in section I.

Tessling remains the leading case on the reasonable expectation of privacy and the case most on point for a discussion of surreptitious brain scanning. Recall that the Supreme Court said in that case that

> External patterns of *heat distribution* on the external surfaces of a *house* is not information in which the respondent had a reasonable expectation of privacy.

According to the Court, heat information available on the outside of Mr. Tessling's house was not protected because the information was, on its own, meaningless. This is because the heat patterns themselves did not reveal core biographical information about Mr. Tessling.

The same analysis might be said to apply if the technology in question was not an infrared scan of Mr. Tessling's house but a remote scanning of his brain. Brain scanning technologies measure external patterns of electricity (and magnetism) on the external surfaces of the skull — information which is, on its own, "meaningless". If neuro-imaging technologies really could scan the brain the way a computer scans a hard drive, then there would be a strong argument in support of the claim that brain scans are not meaningless since they would clearly reveal intimate details about an individual's life. However, this is not the current state of the art. EEG scans merely determine whether information is recognized by the subject and fMRI scans can only pinpoint brain activity; neither can actually read a person's mind in a way that WIRED magazine and other popular culture sources would have us believe (Silberman, 2006; Talbot, 2007). These technologies, at best, provide indicia of knowledge and honesty. In essence, this is analogous to the heat patterns in *Tessling,* which merely provided indicia of activities occurring in his house (because thermal imaging cannot differentiate heat produced by a sauna or fireplace from heat produced by a grow-op). Because brain scans, on their own, cannot differentiate or determine thoughts in any meaningful way, one might argue that the scan itself is likewise not a search and that the *Tessling* analogy applies: external patterns of electricity on the external surfaces of a skull is not information in which a person has a reasonable expectation of privacy.

Although, on its face, the *Tessling* analogy appears solid, there are differences in the nature and quality of the information collected by neuro-imaging technologies that have the potential to undermine the analogy. These differences revolve around the "personal" nature of the brain information.

In her more detailed discussion of *Tessling* earlier in this special issue (Bailey, 2008), Professor Jane Bailey outlines three tiers of privacy protection recognized by Canadian courts: (i) personal, (ii) territorial, and (iii) informational. As she points out, personal privacy enjoys the highest level of protection, informational, the lowest. As Justice Binnie put it in *Tessling:*

> Privacy of the person perhaps has the strongest claim to constitutional shelter because it protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal. (*Tessling* (2004): para 21).

Professor Bailey rightly asserts that the Supreme Court's decision to characterize heat emanations from Mr. Tessling's home as implicating "informational privacy" (rather than, say, "territorial privacy") affected the outcome by placing it into a less protected category (Bailey, 2008). If the heat patterns had been deemed "territorial" (or, better yet, "personal") in nature, they would have enjoyed a higher level of privacy protection. Do patterns of electricity emanating from the brain likewise implicate "informational privacy" interests or are they of a more "personal" nature? How ought courts to deal with this intersectionality when pretty much every bit of surveillance evidence can be reduced to raw information?

Applying the *Tessling* analogy, one could argue that the electrical activities collected during a brain scan can be characterized as information *about* the brain rather than a search *of* the brain, in which case they would, like *Tessling,* fall into the category of informational rather than personal privacy.

Without question, the manner in which the courts will characterize brain emanations in the future will have a significant impact on the ultimate outcome. To illustrate, recall that the Ontario Court of Appeal decision in *Tessling* (2003) characterized the police's use of thermal imaging as implicating territorial privacy (the second highest level of privacy protection), thereby concluding that the infrared picture constituted an unreasonable search. By contrast, the Supreme Court characterized the police's use of thermal imaging as implicating informational privacy (the lowest level or privacy protection), thereby concluding that the police's use of FLIR did not constitute an unreasonable search. Only if brain information is considered "personal" will it enjoy a higher level of privacy protection than Mr. Tessling's heat. But does the information collected by brain scans meet this standard for protection?

The basis of a standard was established by the Supreme Court in *R v. Plant* (1993). Like *Tessling,* the facts of the case involved police reacting to informant tips about marijuana grow-ops. In *Plant* the police accessed the computer records of Plant's hydro provider and discovered abnormally high electrical usage, leading to a closer inspection of his home, a search warrant and ultimately an arrest. Justice Sopinka decided that the hydro records were not private information.

> ... in order for constitutional protection to be extended, the information seized must be of a "personal and confidential" nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual." (*Plant* (1993): p. 293)

To date, Canadian courts have not clearly articulated what constitutes a "biographical core of personal information" other than by enumeration. For example, according to the Supreme Court in *Plant,* information gathered from hydro records are not. According to the Alberta Court of Appeal, odour emanations from a backpack are not. (*Kang Brown*, (2006)) Personal information like name (*Harris,* (2006)) and DNA (*Peddle*, (2006)) may be or may not be depending on the context. Breath samples (*Padavattan*, 2007) and items placed in the garbage do not qualify (*Patrick,* (2005)) but a personal diary definitely qualifies (*Shearing,* (2000)).

There are two additional Supreme Court decisions that are useful in the determination of whether the information obtained using brain scans is "personal" in nature.

In *R v. Dyment* (1988) the court made it clear that personal privacy is paramount, indicating that it is often implicated in the use of a person's body:

> [T]he use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity. (para. 27)

A surreptitious brain scan would allow the police to gather information about a person from his or her body without that person's consent or control. However, the information gathering does not directly affect a person's body. Brain scans fall somewhere in between the removal of bodily samples (like blood or hair) and the measuring of heat patterns emanating from Mr. Tessling's home. Brain waves are involuntarily emitted from the brain but do not represent *tangible* matter in any sense that constitutes the physical person. While brain emanations into public space do not fit easily into the category of bodily specimens and samples, they certainly do involve and implicate the body. On this basis, brain scans could be understood as "personal" rather than merely "informational", thus weakening the *Tessling* analogy. If evidence gathered by brain scans is understood as bodily information then, according to *Dyment,* its nonconsensual use does violate personal privacy.

The second additional Supreme Court privacy decision worthy of consideration is *Dagg v. Canada* (1997). In that case, relying on Alan Westin's seminal work (Westin, 1963), the court held that

> "[P]rivacy is grounded in physical and moral autonomy – the freedom to engage in one's own thoughts, actions, decisions (para. 65).

Whereas thermal imaging can only detect the presence of heat (coinciding with heat-generating activities going on in the house), neuroimaging has the potential to gather information about the brain (coinciding with the thoughts and memories of an individual). Effective neuroimaging technologies would not read minds but, if used surreptitiously or beyond the scope of an individual's consent, they could one day interfere with an individual's autonomy by removing the ability of the individual to control the knowledge or dissemination of important personal information about themselves. If brain scans are ever actually able to drastically reduce or remove the potential for deceit, they would undermine moral autonomy. As the Kantian dictum goes, "ought implies can." (Kant, 1997: Chapter 8) If one cannot do otherwise, one is no longer acting within the realm of morality. Morality entails the ability to choose. When one is *compelled* to tell the truth — whether by Wonder Woman's lasso of truth, by torture, or with a No Lie fMRI™ device (http://www.noliemri.com/index.htm) — that person is precluded from the possibility of full moral agency. Aside from being unable to morally praise that person for telling the truth, how could we say that this person is a moral actor if she can no longer freely engage in her own thoughts and decisions?

IV The Future of Brain Privacy

The fact that the neuroscience community is aggressively pursuing lie detection techniques, combined with the fact that the criminal justice system is interested in employing reliable versions of these technologies suggest that brain privacy is likely to

emerge as a significant legal issue. However, the issue is unlikely to emerge in the context of reasonable expectations of privacy, as discussed above. That context presumes the far-off possibility of surreptitious and remote brain scanning which are, at best, distant possibilities. Still, in our view, there is value in such speculation.

Whether the technology arrives or not, *Tessling*-on-my-brain sheds light on the shortcomings of the current approach to information emanation in a number of ways. First, it provides a *reductio ad absurdum* in response to the hypothesis that a general privacy rule should govern all information emanations. There are good reasons to treat heat patterns, drug odours, brain waves and other forms of emanation differently in different contexts. The *Tessling* decision was never meant to provide a single rule. Second, the example also illustrates an important distinction between predictive and normative expectations — while it may be reasonable to *predict* that information will emanate from private to public spaces and that new technologies will be able to measure and monitor those emanations, it does not follow that we cannot reasonably *expect* to maintain privacy in at least some of that information. As Justice Binnie said in *Tessling,* "[e]xpectation of privacy is a normative rather than a descriptive standard." (*Tessling*, 2004). Third, the example highlights problems with the current trifurcated privacy hierarchy (personal/territorial/informational). In a world where so many things can be reduced to bits and bytes of information, a privacy hierarchy which gives very little weight to information and no reliable means of determining which privacy category applies risks too much. Is a brain wave merely information or should we consider it part of a person? How do we deal with an intersectionality of privacy interests where more than one zone of privacy is implicated? Neither scholars nor our courts have addressed any of these questions. The *Tessling*-on-my-brain example illustrates the need for a more robust theory of privacy.

Although there is much to learn about brain privacy from the above speculations, the three issues most likely to arise in the near future pertain to (i) the nature of consent, (ii) the right against self incrimination and (iii) security of the person.

The consent issues are not new ones. There are at least two aspects. The first relates to the tort law concept of consent to treatment (Solomon et al. 2003: p.161). If a lie detection procedure involves any risk of harm to the body, a failure to obtain consent could result in an action for battery (Downie et al., 2007: p.90). But what if there are no negative health implications? There is still a consent issue in the context of informational privacy. The challenge here is also not a novelty. Even assuming a voluntary and informed consent, the problem of secondary uses of the information is sure to arise (PIPEDA 4.5 Principle 5). How do we ensure that brain scans undertaken for one purpose are not collected, used or disclosed for some other purpose? Although these issues are not new ones, they will have new currency in a world where employers, insurance companies, bankers, teachers, lovers, lawyers, law enforcement agencies and judges all clamor to learn more about a person's brain states.

The second issue likely to emerge is the risk against self-incrimination; the *Charter* protects individuals against being forced to act as a witness against themselves (*Charter,*

s. 11c; 13.). The state is required to prove all aspects of a crime without the assistance of the accused. Neuroimaging techniques have the potential to remove the individual from their role as the gatekeeper of their own personal information, bypassing the person by simply seizing the information from snapshots of their brain activity. Dr. Farwell's claim that Brain Fingerprinting can determine if an individual recognizes a particular person, place or thing could be used to exonerate, but could just as easily be used to violate *Charter* protections against self-incrimination. Future courts are sure to be called upon to determine whether the information gained via brain scans is protected due to its potential for self-incrimination or whether it is not protected, like breathalyzer information, because the protection only applies to statements (*Stasiuk,* 1982).

The third issue likely to emerge reflects the fact that neuroimaging has clear potential to intrude on the physical and psychological autonomy of the individual. *Tessling*-on-my-brain presents the moral intuition that brain emanations are somehow fundamentally different from emanations of heat from a house, odour from a suitcase, etc. Section 7 of the *Charter* clarifies that intuition. It protects the life, liberty and security of the person of all Canadians (*Charter,* s.7). The Supreme Court has determined that security of the person protects both the physical and psychological integrity of the individual (*Rodriguez,* 1993: para 21). For example, security of the person has been applied to protect against psychological stress caused by removing children from the care of their parents. (*G.J.*, (1999)). It is unclear whether section 7 would be found to protect against brain scans but the issue will likely arise in the context of brain scan lie detection. In a society that is ordered around risk (Giddens, 1999; Beck, 1992) and sees technology as the antidote, the connection between privacy and security is apparent.

V Conclusion

It is difficult to draw a tidy conclusion with clear policy recommendations about a technology still in the laboratory. This article is meant more as an appreciation of that which lurks around the corner. As the art and science of discovering and understanding the information that emanates from our brains surges fast-forward toward the future, proliferating exponentially in an era where our intelligence will become increasingly nonbiological and trillions of times more powerful than it is today (Kurzweil, 2005), we suggest that the goal of using brain based lie detection in our criminal justice system will require better developed theories of privacy.

If we are to maintain our "dignity, integrity and autonomy" (*Plant,* (1993)) in the face of emerging brain surveillance techniques that might one day be capable of re-telling the stories of our personal lives with or without our permission and yet in ways that are personally and territorially unobtrusive, scholars and jurists must confront the social implications of informational privacy much more deeply than they have, interrogating its normative implications in an empirical universe of information emanation.

LIST OF REFERENCES

Abbott, A.
2001 Into the Mind of a Killer. Nature Magazine 410: 296-298

Appelbaum, P.S
2007 The New Lie Detectors Neuroscience, Deception, and the Courts. Law & Psychiatry 58 4: 460-462

Bailey, Jane
2008 Framed by Section 8: Constitutional Protection of Privacy in Canada. Canadian Journal of Criminology and Criminal Justice. 49 2:

Bailey, Ronald.
2003 The Battle for Your Brain. Reasononline: February, 2003

Barnes, J.A.
1994 A Pack of Lies: Towards a Sociology of Lying. New York: Cambridge University Press

Beck, Ulrich
1992 Risk Society: Towards a New Modernity. London: Sage Publications

Bok, Sissela
1982 Secrets: On the Ethics of Concealment and Revelation. New York : Pantheon Books

Downie, Caufield and Flood.
2007 Canadian Health Law and Policy. 3rd ed Toronto, ON: 190-91

Evanson, Brad.
2003 The Guilty Mind. National Post 02/10/03

Farwell, L. A. and Smith, S. S.
2001 Using Brain MERMER Testing to Detect Concealed Knowledge Despite Efforts to Conceal. Journal of Forensic Sciences 46,1:1-9

Frankfurt, H.G.
2005 On Bullshit. Princeton,NJ: Princeton University Press

Ford, Elizabeth
2006 Lie Detection: Historical, neuropsychiatric and legal dimensions. International Journal of Law and Technology 29: 159-177

Freud, A.
1965 Normality and pathology in childhood: Assessments of development. New York: International Universities Press.

Friedland, M.L. and Roach, K.
2004 Criminal Law and Procedure: cases and materials. Toronto: Emond Montgomery

Ganis, G., Kosslyn, S. M., Stose, S., Thompson, W. L., & Yurgelun-Todd, D. A.
2003 Neural correlates of different types of deception: an fMRI investigation. Cereb Cortex 13 8: 830-836.

Gasson, M N., Hutt, B D., Goodhew, I., Kyberd, B D., Warwick, K.
2005 Invasive Neural Prosthesis for Neural Signal detection and Nerve Stimulation International Journal of Adaptive Control and Signal Processing, Vol 19 5: 365-75

Giddens, Anthony
1999 Risk and Responsibility. Modern Law Review 62 1: 1-10.

Illes, J., & Racine, E.
2005 Imaging or imagining? A neuroethics challenge informed by genetics. Am J Bioeth, *5* 2: 8-9

Kant, Immanuel. Trans and Ed Mary Gregor
1997 Critique of Practical Reason. New York: Cambridge University Press.

Kerr, I. & McGill, J.
2007 Emanations, Snoop Dogs and Reasonable Expectations of Privacy. The Criminal Law Quarterly 52 3/4: 392

Kozel, F. A., Revell, L. J., Lorberbaum, J. P., Shastri, A., Elhai, J. D., Horner, M. D., Smith, A., Nahas, Z., Bohning, D. E., & George, M. S.
2004 A pilot study of fMRI brain correlates of deception in healthy young men. J Neuropsychiatry Clin Neurosci 16 3: 295-305.

Kurzweil, R.
2005 The Singularity is Near. Viking Penguin Books.

Langleben, D. D., Loughead, J. W., Bilker, W. B., Ruparel, K., Childress, A. R., Busch, S. I., & Gur, R. C.
2005 Telling truth from lie in individual subjects with fast event-related fMRI. Hum Brain Mapp 26 4: 262-272.

Langleben, D. D., Schroeder, L., Maldjian, J. A., Gur, R. C., McDonald, S., Ragland, J. D., O'Brien, C. P., & Childress, A. R.
2002 Brain activity during simulated deception: an event-related functional magnetic resonance study. Neuroimage 15 3: 727-732.

Moulton, C.
1943 Wonder Woman, No. 6. In WonderWoman archives Vol. 3. New York: DC Comics.

Lee, T. M., Liu, H. L., Tan, L. H., Chan, C. C., Mahankali, S., Feng, C. M., Hou, J., Fox, P. T., & Gao, J. H.
2002 Lie detection by functional magnetic resonance imaging Hum Brain Mapp, 15 3: 157-164.

Lewis, M., Stanger, C., & Sullivan, M. W.
1989 Deception in three-year-olds. Developmental psychology, 25: 439−443.

NATURE
2004 True Lies. Nature Magazine. Volume 428 Issue no 6984

Ross, P.
2003 Mind Readers. Scientific American Vol. 289, Issue 3

Silberman, Steve.
2006 Don't Even Think About Lying. Wired Magazine 14.01 Jan 2006

Solomon, R., Kostal, R. and McInnes, M.
2003 Cases and Materials on the Law of Torts. Thomson Carswell.

Spence SA, Farrow TF, Herford AE, Wilkinson ID, Zheng Y,Woodruff PW
2001 Behavioural and functional anatomical correlates of deception in humans. Neuroreport 12: 2849–2853.

Sullivan, E.
2001 The concise book of lying. New York: Farrar, Straus and Giroux.

Talbot, Margaret.
2007 Can Brain Scans Uncover Lies? New Yorker Magazine. July 2 2007.

Van Wyhe J.
2002. The History of Phrenology on the Web. Retrieved July 29, 2007, from http://www.victorianweb.org/science/phrenology/intro.html

Westin, Alan
1967 Privacy and Freedom. New York: Atheneum

Wolpe, P. R., Foster, K. R., & Langleben, D. D.
2005 Emerging neurotechnologies for lie-detection: promises and perils. Am J Bioeth, 5 2: 41

APPENDIX B: LEGISLATION CITED

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11

Criminal Code of Canada, R.S.C. 1985, c. C-46

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5: 4.5 P5

APPENDIX C: CITED CASE LAW

R. v. A.M., 2006 209 O.A.C. 257

R. v. Brown, 2006 ABCA 199

*Dagg v. Canada (Minister of Finance)***,** [1997] 2 S.C.R. 403

R. *v. Dyment*, [1988] 2 S.C.R. 417
S.
Iowa v. Harrington 2003 659 N.W. 2d 509 (Iowa Sup. Ct.)

R. v. Harris, 2006 ONCJ 106

New Brunswick (Min. Health & Community Services) v. G. (J.), 1999] 3 S.C.R. 46

R. v. Ly, 2005 ABPC 32

R. v. McLay, [2006] N.B.J. No. 73

R. v. Padavattan, 45 C.R. (6th) 405

R. v. Patrick, 2005 ABPC 242

R. v. Peddle, [2006] N.J. No. 41 (N.L. Prov. Ct.)

R. v. Plant, [1993] 3 S.C.R. 281

R. v. Rodriguez, [1993] 3 S.C.R. 519

R. v. Shearing, 2000 BCCA 83

R. v. Stasiuk, 16 M.V.R. 202

R.v. Tessling, [2003] O.J. No. 186 and [2004] 3 S.C.R. 432

R. v. Tran, 2007 ABPC 90