"Techno-Risk - The Perils of Learning and Sharing Everything" from a criminal information sharing perspective

September 3rd, 2012, Cambridge, England

John Sliter, Superintendent
Director, Field Services
Canadian Police Information Centre
1200 Vanier Parkway
Ottawa, Ontario
K1A0R2
jsliter@rcmp-grc.gc.ca

The views expressed herein are those of Mr. John Sliter and do not reflect the views of the Royal Canadian Mounted Police, nor those of the Government of Canada.

At the 2011 Symposium on Economic Crime in Cambridge England, this author spoke of Government agencies coming a long way in ensuring that all law enforcement information is shared, and shared quickly. It was also asserted that government and law enforcement information should be shared with private sector investigative agencies[1].

"The only good is knowledge and the only evil is ignorance." – Socrates, (469BC – 399 BC)

The focus of this particular paper will be on the perils or risks associated with this type of information sharing – when everyone knows everything about criminal activity.

The author will suggest that we are entering an era where soon we will be able to learn and know everything about anything. There will be nothing that we will not be able to learn, and quickly - soon to be instantly.

Learning everything from the Internet

Let me begin by asking you to consider the fact that every day, the internet grows by a phenomenal amount. In 2010, the Executive Chairman of Google was quoted as saying that the amount of information being added to the Internet every two days was equivalent to the entire amount of human information that had been amassed from the dawn of time to 2003[2]! And since 2010, this amount has clearly increased and every minute massive amounts of it are being generated from every phone, website and application across the Internet.

According to a leading business intelligence corporation, we are now at the point where every minute of every day in our lives, there are almost 205 million email messages sent, 2 days of video are uploaded to YouTube, over 2 million queries are received by Google, 685 thousand items of information are shared on Facebook, 571 new websites are created, over 3,100 new photographs are added to Flickr and Twitter users send out over 100 thousand tweets[3]. This is each and every minute!

In short, we are living in an information-rich world where we can have vast amounts of information on almost any subject we care to name, all within seconds.

Which leads to other considerations – at what rate of speed can we digest and determine the relevance of this vast sea of information? And, what sort of digital trails are users leaving behind?

It was back in June of 1961 that Soviet cosmonaut Yuri Gagarin became the first man to orbit Earth in a spacecraft[4]. Fifty years later, millions of people have more computing power on their desktops than Gagarin had in his entire spacecraft—and at a fraction of the

[1] Sliter, John R., 'The Risk of Being Un-Informed' - A Paper on the Character and Implications of Risk in the Context of Economically Motivated Crime (September 5, 2011). Available at SSRN: http://ssrn.com/abstract=1926195
[2] Schmidt, Eric, Google CEO, August 4, 2010, Quoted in TechCrunch and web-posted at http://techcrunch.com/2010/08/04/schmidt-data/
[3] Josh, James, Founder and CEO DOMO Inc., web-posted at http://www.domo.com/blog/2012/06/how-much-data-is-created-every-minute/
[4] http://www.aerospaceguide.net/spacehistory/yurigagarin.html

cost. Medicine can treat ailments thought fatal only a few years ago. Significant breakthroughs in the areas of genetic engineering and robotics are being reported daily in our news media.

Consider Google's Project Glass – an attempt to make computers wearable! They are building a smart pair of glasses with an integrated heads-up display and a battery hidden inside the frame[5].

Next, take a moment to imagine yourself organizing your daily schedule each morning with a few touches on your bathroom mirror. Or how about chatting with far-away relatives through interactive video on your kitchen counter? Corning Incorporated purports itself to be the world leader in specialty glass and ceramics and they are engaged in some exciting research in this area[6].

More in line with the wearable computer concept, there are sports jerseys "equipped with electroluminescent wires and surfaces" that track the number of fouls the wearer has picked up, identifies the leading scorer, and which team is winning[7].

There is also a concept called the 'Internet of Things' – in which sensors and other data-generating devices are connected to the Internet. For example, you can also find out what Beer Robot, the Wired office 'kegerator', is thinking - all you have to do is follow @BeerRobot on Twitter. And, you can also take a look at where he lives. Google has been mapping interior spaces in Street View for a while now, showing things like governmental buildings, restaurants, museums, and pieces of art. Since October, 2011, independent photographers and businesses have also been able to upload their own panoramas to Street Views, a project that has delivered a large number of dentists' offices and surprising interiors[8]. Another relevant example might be in the automated traffic monitoring cameras that record 'hit and run' motor vehicle incidents. These automated systems are becoming more and more publicly accessible and this promises to test the standard definitions of, for example, data subject and data controller.

Smart eye glasses, glass computers, the 'Internet of Things' and even computers in our clothing represent remarkable technological developments all heading in the same direction. **The next step is to bring the computer right into the human brain - the ability to control a device using thought alone!**

[5] http://techcrunch.com/2012/06/27/google-glass-future/

[6] Weeks, Wendell, Corning Chairman and CEO, Press Release 2012 – web-posted at http://www.corning.com/news_center/features/A_Day_Made_of_Glass.aspx

[7] Page, Mitchell and Vande Morere, Andrew, "Evaluating a Wearable Display Jersey for Augmenting Team Sports Awareness", Lecture Notes in Computer Science, 2007, Volume 4480, Pervasive Computing, Pages 91-108

[8] Olivarez-Giles, Nathan, Tour the Wired Office in Google Maps Street, August 23, 2012, web-posted at http://www.wired.com/gadgetlab/2012/08/google-maps-street-view-wired-newsroom/

The Brain Chip

Imagine searching the Internet with your mind – the possibilities for semantic search are just incredible. *What about managing your home with thought – switching on the TV, turning off lights and getting a quick update on how much power you've used in a day? Productivity could also be greatly improved – what if you could prepare word documents a sentence at a time rather than typing letter by letter?* In 2008, a University of Pittsburgh School of Medicine research project planted probes in a monkey's brain so that, using thought alone, it could control a prosthetic arm to feed itself[9].

Shortly thereafter, in 2009, Intel Corp. researchers asserted that by the year 2020, we will not require a keyboard and mouse to control our computer[10]. **Instead, users will open documents and surf the Web using nothing more than their brain waves.**

While this might sound scary to some people, these brain implants are to be done on a voluntary basis and researchers are confident consumers will actually ask for the implant, as they really want the freedom they will gain by its use. The belief is that users will soon tire of depending on a computer interface and having to dig a device out of their pocket or purse to access it. Similarly, they will tire of having to manipulate an interface with their fingers[11].

Most recently in May of 2012, a paralyzed patient equipped with an implanted brain chip has been able to use a robotic arm to reach for and pick up a bottle of coffee, bring it close enough to her face so she could drink from a straw, and then place the bottle back on the table[12]. Also, in August, 2012, researchers in Calgary, Alberta, Canada have reported the further development of a neurochip − a microchip with the ability to monitor several functions of the brain. In previous studies, researchers developed a neurochip that could directly stimulate and record brain cell activity. The new novel lab-on-a-chip technology uses an ultra-sensitive component built directly on the microchip that enables direct imaging of activity in brain cells. The current study used snail brain cells and researchers reportedly hope to use human brain cells in the next step.

All of this leads to the assertion that very soon we will have <u>instant</u> access and knowledge of everything there is to know - literally in the blink of an eye!

But what is this knowledge and what are some of the risks – could it be dangerous? And, in the context of this paper, what are the implications for law enforcement?

---

[9] Baum, Michele D., University of Pittsburgh Schools of the Health Sciences, May 28, 2008 "Mind over matter: Monkey feeds itself using its brain".

[10] Gaudin, Sharon, Nov 19, 2009, Computerworld, "Intel: Chips in brains will control computers by 2020". http://www.computerworld.com/s/article/9141180/Intel_Chips_in_brains_will_control_computers_by_2020

[11] Gaudin, Sharon. Nov 19, 2009, Computerworld - "Intel: Chips in brains will control computers by 2020"

[12] Young, Susan, May 16, 2012, Technology Review published by MIT - "Brain Chip Helps Quadriplegics Move Robotic Arms with Their Thoughts"

Knowledge does lead to absolutely incredible advances in technology, but some people may be concerned that there are legitimate reasons not to advance too far. Technological advances in the field of health have resulted in making it possible for people to live longer and to enhance our quality of life. However, conversely some of these technological advances have also resulted in some pretty amazing weapons specifically designed to shorten human life. For example, the U.S. Navy has a 'railgun' that accelerates a 3.2 kg (7 pound) projectile to approximately 2.4 kilometers per second (5,400 mph). They gave the project the Latin motto "Velocitas Eradico," which they translate as "speed I kill"[13].

Knowledge might be defined as a familiarity with something, which can include facts, information, descriptions, or skills acquired through experience or education[14]. This definition would suggest that mere access to unlimited information, no matter how fast or instantly, may not necessarily constitute knowledge. There is also a requirement to digest, interpret and understand all of this information. If human beings rely on computers to perform these functions as well, and artificial intelligence has made significant progress in that regard, some foresee a clear danger in allowing the machines to make literally all decisions for us.

In addition to the concept of attaching fast and powerful computers directly to humans, it does not go without mention that there has also been considerable work done on the converse concept and taking real brains and putting them into machines. For example, after years of research involving the brain of a rat attached to a wheelchair, in 2009, Toyota-sponsored researchers in Japan unveiled a human brain-machine interface system that allows a person to use thoughts to direct the motion of a wheelchair[15]. Now link this idea to the fact that the Defense Advanced Research Project Agency (DARPA) has produced a robot called Cheetah that can run at speeds up to 18 miles per hour, completely shattering the 1989 legged robot speed record of 13.1 miles per hour[16].

This year in the United States, the Pentagon announced their 'Avatar' program which will develop "interfaces and algorithms to enable a soldier to effectively partner with a semi-autonomous bi-pedal machine and allow it to act as the soldier's surrogate.[17]" There is a similar project being reported on from Russia, also entitled 'Avatar', and it involves a ten year plan to construct robots that will actually store a human's mind and keep that consciousness working – forever! The people behind this project are thinking that this will lead to immortality – "A person with a perfect Avatar will be able to remain part of society. People don't want to die.[18]"

In short, researchers around the world are working furious to hasten the convergence of man and machine!

---

13 Borrell, Brendan, February 6, 2009, Technology Review published by MIT, Electromagnetic Railgun Blasts Off
14 http://en.wikipedia.org/wiki/Knowledge
15 CBC News, June 29, 2009 "Researchers Use Thoughts to Drive Wheelchair".
16 Defense Advanced Research Project Agency (DARPA) – March 5, 2012 – "DARPA's "Cheetah" Sets Land Speed Record for Legged Robots". www.darpa.mil
17 Drummond, Katie, Wired Magazine – February 16, 2012 – "Pentagon's Project 'Avatar': Same as the Movie, but With Robots Instead of Aliens".
18 Drummond, Katie, Forbes Magazine – July 19, 2012 – "Russian Mogul to 'Forbes' Billionaires: Limitless Lifespans Can Be Yours"

This convergence, and the related moral and ethical dilemmas attached to related new technology, is a subject of great speculation and debate. One can appreciate the cyber-crime implications as well – malicious viruses will soon have critical implications for our physical well-being! Cyber-police are facing challenges where there is absolutely no room for failure as the most frightening science fiction films are brought to mind.

However, this author wishes to maintain particular focus of this paper on electronic information and how the misuse of this information can be just as devastating as the military 'railgun' referred to above.

> *"The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros--little bits of data--it's all electrons....There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information--what we see and hear, how we work, what we think. It's all about information.*[19]"

Technology Used to Identify Criminals and Track Their Criminal Activity

Technology has provided law enforcement with many new and exciting tools to help law enforcement identify criminals and track their activities – here are but a few examples.

One particularly good example was reported in June, 2011, when researchers at the University of Technology in Sydney, Australia announced that they had developed a new method of securing fingerprints using nanotechnology[20]. Their new nano tech fingerprint system was able to produce fingerprints from cases that were decades old. The collaboration between the UTS Centre for Forensic Science, the University of Canberra, the Australian Federal Police and Northern Illinois University has resulted in a forensic science world first with the preliminary development of a novel immunogenic method to detect latent 'fingermarks'. In fact, nanotechnology can reportedly improve everything from bullet proof armored fabrics, to the effect bullets have on the body once coming in contact with a target's flesh, to reproducing latent evidence from crime scenes by using biological remnants of DNA and other particles[21].

The US Federal Bureau of Investigation also launched a new $1 billion biometric Next Generation Identification (NGI) system[22]. NGI is a nationwide database of mugshots, iris scans, DNA records, voice samples, and other biometrics, that will help the FBI identify and catch criminals — but it is how this biometric information is captured, through a nationwide network of cameras and photo databases, that is making privacy advocates nervous. Some States have begun uploading their photos as part of a pilot program in February and it is expected to be rolled out nationwide by 2014. In addition to scanning mugshots for a match, it is reported that FBI indicated that they are eager to track a suspect by picking out their

[19] Lines from the character "Cosmos," in the movie Sneakers, MCA/Universal Pictures, 1992.
[20] Nanotechnology Now - a forum and format that helps clarify nanotechnology. Located at http://www.nanotech-now.com/news.cgi?story_id=42656
[21] Worldpress.com, Blog located at http://top10daily.wordpress.com/page/3/
[22] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

face in a crowd[23]. Another application would be the reverse: images of a person of interest from security cameras or public photos uploaded onto the internet could be compared against a national repository of images held by the FBI. An algorithm would perform an automatic search and return a list of potential hits for an officer to sort through and use as possible leads for an investigation.

Following this line of thinking, there is a new app in the United Kingdom called Facewatch which provides members of the public with photos and CCTV images of unidentified subjects in an effort to help police find wanted individuals. At first glance, a user will not find anything particularly ground-breaking about the new app as news channels and websites often show photos of wanted people. However, the difference in this app is that you can enter in your postal code to see a list of (potentially) nearby offenders. It has been reported that the Metropolitan Police has uploaded almost 3,000 CCTV images of people during the widespread disorder in August last year onto its Smartphone app. The free Facewatch ID app developed with facial recognition software firm Facewatch Ltd was launched in April, 2012.[24][25]

Another great example stems from vehicle recovery systems - a.k.a. vehicle tracking systems. These are telematic systems that allow their owners to get their stolen vehicles back - often sooner than had they relied solely on the police, and with less damage. OnStar boasts their newest tool, implemented into all 2009 and newer General Motors vehicles, helps lead to quicker recovery—while reducing the property damage, injuries, and fatalities associated with high-speed chases. GPS technology is used to pinpoint the location of your vehicle and provide it to authorities. They can remotely block your ignition, making it impossible to restart the vehicle once it's turned off. They then work with the police to send a signal to your vehicle, forcing it to "*gradually and safely slow down*"[26].

Yet another exciting example builds on the concept of the Google car that recently rolled past 300,000 miles of driving itself. In August, 2012, the Department of Transportation in the United States announced that they are road-testing a safety system that puts vehicles in communication with each other in the hope of reducing crashes. In the program, some 3,000 vehicles in the Ann Arbor, Michigan area have been equipped with wireless technology for vehicle-to-vehicle, or V2V, communications. The vehicles use a Wi-Fi-like system to emit a basic safety message 10 times per second that forms the data stream that other in-vehicle devices use to determine when a potential traffic hazard exists. This info is used in combination with the vehicle's own data to provide warnings to drivers about dangerous lane changes, vehicles speeding around blind corners and other potential accident-causing behaviors[27].

---

[23] Reardon, Sara, September 7, 2012, http://www.newscientist.com/article/mg21528804.200-fbi-launches-1-billion-face-recognition-project.html

[24] http://facewatch.co.uk/cms/more_news/facewatch-id-launch

[25] Wilcock, David, June 26, 2012, The Independent, Police 'Facewatch' app targets London riot suspects

[26] https://www.onstar.com/web/portal/securityexplore

[27] United States Department of Transportation, August 21, 2012, DOT Launches Largest-Ever Road Test of Connected Vehicle Crash Avoidance Technology

Finally, there are detailed instructions on the Internet on how to make use of the GPS in your teenager's smart phone to continuously be aware of their whereabouts[28]. As a parent, you may want to locate your child that has missed a curfew. Are they at the school, or with a trusted friend, or hanging out at the local shopping mall? Employers have also been known to use this technology to monitor the movements of your employees during work hours. Why is Bill still parked out by the golf course - lunch was over 2 hours ago!

These systems for identifying people and tracking vehicles perform a great service – from allowing concerned parents to track errant teenage drivers to recovering stolen vehicles. However, they only work if we have complete trust and faith in those working behind the satellite tracking systems – up to an including our government. If we pause to think about how these devices could be used by those involved in criminal activity or even by corrupt governments, one can understand the nervousness of privacy advocates - the potential risks are great!

Transparency of all Criminal Activity

Police Services around the globe are also gradually opening their windows and permitting the transparency of all reported crime. This is something that has traditionally been discouraged as the risks to opening up crime reporting and criminal record databases to the public were considered far too great. Some jurisdictions feared the potential for vigilantism, extortion or blackmail. One might also foresee an increase in discrimination based on a purported criminal act. However, these notions are gradually falling by the wayside as private sector companies fight to make use of the information for a variety of reasons, least of not which is background screening. There is a general belief that the public has a right to know what is happening in their neighbourhood and the movement of electronic information on the Internet, in particular amongst social media circles, is helping to level off the playing field.

Crime mapping has long been an integral part of the process known as *crime analysis.* The traditional crime map was a jumbo representation of a jurisdiction with pins stuck in it. There is one company 'Spotcrime.com' (Spotcrime) that is doing a wondrous job of melding reports obtained from Media, Police and the general public. Users can enter in an address and review reports and maps outlining the details of all crime occurrences in the immediate area[29]. As more and more police services provide direct access to their crime reports, these companies have to rely less and less on the accuracy of media reports or entries from the general public. Spotcrime has essentially created a pin map of the world with special pins for various types of crimes such as sexual assault, robbery and shootings. These new generation pin maps have come a long way as they are now complete with Google map photos. In fact, the only thing that is often missing is the name and address of the victim and/or the alleged perpetrator.

---

[28] Shmukler, Chad, June 13, 2010, "How to Track / Find Your Child's iPhone Using GPS", Web Posted at http://www.iphonefaq.org/archives/97949

[29] http://www.spotcrime.com/

The following are the types of crime reports accepted by Spotcrime:

- Theft - The act in which property belonging to another is taken without that person's consent.
- Burglary - The criminal offense of breaking and entering a building illegally for the purpose of committing a crime in that building.
- Robbery - Using force or intimidation to take property away from another person in the presence of that person.
- Assault - A physical attempt or threat to use violence with the intent to do harm to another.
- Arson - The crime of intentionally setting fire to a building or property of another or the burning of one's own property to collect insurance.
- Shooting - The act of firing a weapon in order to hit, wound, or kill someone or something.
- Vandalism - The intentional destruction of or damage to the property of another.
- Arrest - The seizure of an alleged or suspected offender to answer for a crime.

The above crime classifications would be considered inappropriate for police referencing purposes as they do not follow the strict legal definition for each type of criminal offence. However, it is important to note that they are starting to capture information that closely resembles that reported and stored in police computers. What we have is law enforcement recording crime information in an electronic database while and we have the public and the media reporting and recording crime in a different electronic database. Spotcrime is a good example of the public demand for an alliance between the two.

It is asserted that there is great public demand for a system that would allow anyone and everyone to see what anyone and everyone was alleging about a particular person or company. One could then determine if any other people also thought the guy that lived at the end of the street was creepy, or if anyone had actually reported him for sexual assault. Business people would find out about complaints of fraud etc, before they invest their life savings. In fact, this author is on record as suggesting that this will also be inevitable[30]. Just about everyone carries a mobile phone, complete with a video camera and are not afraid to use it to take photos or videos of unacceptable behavior, be it socially unacceptable or downright criminal. They then wish to share these images with as wide an audience as possible. And, as we witness on almost a daily basis, it is often the news media that is eager to provide the medium.

There are some risks associated with the transparent identification of those persons involved in criminal behaviour. However, it is obvious that clear progress is being made around the world to inform and protect our citizens from sexual predators. This author would like to see that type of information sharing extended to include perpetrators of other types of serious crime, particularly financial crime!

[30] Sliter, John R., 'The Risk of Being Un-Informed' - A Paper on the Character and Implications of Risk in the Context of Economically Motivated Crime (September 5, 2011). Available at SSRN: http://ssrn.com/abstract=1926195

The Future - Identifying Criminals and Suspects

Societies have long sought security by identifying potentially dangerous individuals in their midst. Registration of criminals, which originated in the 1930s as a means of monitoring gangsters, went largely unused for decades before experiencing a dramatic resurgence in the 1990s. Since then it has been complemented by community notification laws which, like the "Wanted" posters of the Frontier West, publicly disclose registrants' identifying information, involving entire communities in the criminal monitoring process[31]. For example, the New York State Division of Criminal Justice Services (DCJS) maintains a Sex Offender Registry, which provides New Yorkers information about sex offenders living in their communities[32].

Please consider the speed with which information now flows as compared to those 'Wanted Posters' of the wild west. First, along came the newspaper that allowed law enforcement to increase the circulation of their wanted posters beyond a few trees and poster boards across the country to a much wider audience of readers spanning the globe. The introduction of radio and television further sped up the distribution by *pushing* the names and faces of wanted criminals into the homes of citizens. Then along came the Internet in the 1990's which brought the ability to *pull* the information by conducting a general search query of any suspicious person. Providing they were using their real name and identity, and law enforcement had broadcast the related criminal activity, criminals could be quickly identified. When we added a line of Internet and multimedia-enabled Smartphones into the equation, the identification of criminals sped up even faster. People can now query suspicious people right on their mobile smart phone.

Face.com is a company that reportedly developed apps such as the mobile application called 'Klik' that used facial recognition to identify people in real time. If you held up your phone to take a picture of someone, Klik would guess who it was. If the app doesn't get it right, it would give you its top choices and you could teach it to improve. Then Klik would help users to share the tagged photos on Facebook, Twitter, email and its own public social network[33]. However, in June, 2012, Face.com was acquired by Facebook and the Klik app has been discontinued.

In spite of this, there are reports that by the end of 2012, almost 20% of annual Smartphone shipments will include facial recognition capabilities. A major challenge for facial recognition in mobile devices has been incorporating an accurate enough camera and a powerful enough processor to undertake the complex algorithms while limiting power consumption. Recent technological advances have reportedly solved this problem[34].

We are now at a point where governments are being called upon to make some tough ethical decisions and to define where we draw the line on all of this. We are moving towards a

---

[31] Logan, Wayne A., Knowledge as Power: Criminal Registration and Community Notification Laws in America (August 25, 2009). Stanford University Press, 2009; FSU College of Law, Public Law Research Paper No. 387.
[32] http://www.criminaljustice.ny.gov/nsor/
[33] Garside, Juliette, The Guardian News, United Kingdom, June 19, 2012, Web Posted at http://www.guardian.co.uk/technology/2012/jun/19/face-com-facebook-smartphone-photography
[34] Trent, Nouveau, August 8, 2012, TG Daily, "Facial recognition coming to a Smartphone near you".

convergence of man and machine and as we get further away from our own humanity we become more like machines. In fact, some people believe that when technology gets too great it will cause destruction upon itself. The question being asked is - Will new technologies save mankind from all its ills, or will we reengineer ourselves out of existence?[35]

Now, the reader is invited to consider all the information on Google glasses and the new neuro brain chip and come to share the **conclusion that we will very soon have the capacity to identify purported criminals instantly – again, literally in the blink of an eye.** Precisely like some of the science fiction movies, a small virtual identifier will appear over the head of convicted criminals or even would be suspicious persons. **Herein lies a significant concern – the accuracy and reliability of the information must be impeccable else there will be grave consequences.**

The Ethical Questions – 'Just because we can doesn't mean we should'

In fact, on a daily basis one can read of the sort of ethical dilemmas facing legislators and policy makers with respect to the enhanced uses of technology. These dilemmas also include all aspects of privacy and the sharing of vast amounts of electronic information.

'Facedeals' is a new service that uses facial recognition to allow businesses to automatically scan shoppers' faces, track their visits and alert their Facebook friends as to their whereabouts. As might be expected, this has raised the concern of some privacy advocates. In Canada, Ontario's information and privacy commissioner, Ann Cavoukian, raised a number of concerns about Facedeals. Ms. Cavoukian has been quoted as saying the service, if it becomes popular, "*will have the intimate details of the personal lives of millions of people. Protecting that information from unintended uses needs to be the top priority*"[36].

Things move very quickly in the field of technology and in the aggressive and capitalist approach to rush out new innovative technologies, there is often not a lot of time devoted to consideration of the consequences of people voluntarily relinquishing their privacy. In fact, consumers are seemingly becoming less concerned with protecting their privacy. In a recent study released by researcher SAS Canada, more than 46 per cent of Canadians said they would be willing to give up personal information in exchange for personalized discounts or other offerings[37].

[35] Bowmer, William, "Will Mankind Become Obsolete?" Tomorrow's World magazine, May-June, 2002.
[36] Pilieci, Vito, the Ottawa Citizen, "Saving Face", Aug 16, 2012.
[37] SAS. July 3, 2012, "Three in four Canadians expect customized offers in return for their personal information", http://www.sas.com/offices/NA/canada/en/news/preleases/marketing-survey2012.html

Background Screening

In most, if not all western democracies, background screening is used as a method to prevent sexual and financial predators from working or volunteering within our vulnerable sectors of society. This type of screening has exploded in recent years and expanded to just about every type of employment – from hospitals to retail outlets to financial institutions. It has enabled would be employers to screen out those persons with a history of illegal or inappropriate behavior who may pose a danger to public safety.

While this type of background screening was traditionally limited to a check of police databases, there is now general awareness fact-based police information is often quite limited in value. As more and more data became available, many corporate users began making use of *non-government* databases to try and screen out those candidates who might pose a risk to '*corporate'* safety. For example, a person with a history of inappropriate and lewd behavior, as perhaps identified within their Facebook profile, might pose a corporate risk in terms of relationships with other employees which might even result in civil litigation relative to harassment. The marketing slogan of "What goes on in Vegas, Stays in Vegas[38]" is now humorously altered to say "What goes on in Vegas, Stays on Facebook"!

Although it is true that private databases and private sources of information have long surpassed those closely guarded secret databases belonging to law enforcement, at least in terms of volume, one must also question the quality or validity of some of the information. For example, last year a newspaper in Montreal, Quebec in Canada filed a complaint with police after someone hacked into its website and posted a fake story announcing the death of Quebec's premier[39]. This was quickly proven unfounded and the premier was alive and well.

Facebook also recently acknowledged that as many as 83 million of their 955 million accounts could be fake. And up to 1.5% of total accounts are likely "undesirable" profiles specifically set up for nefarious purposes, such as affecting ad results and spamming users[40].

This author has also previously expressed concern that thorough background screening may often dictate violations of applicable privacy legislation[41]. For example, a query of a person's financial status without their consent may be in violation of their expectation of privacy under privacy legislation, as is in most, if not all, western jurisdictions.

This is not to suggest that there is not some great work being done by private sector Background Screening companies. There are some companies that go to great lengths to ensure they have correctly identified the client and that the information compiled is indeed accurate and substantiated. In short, there is good information being used to screen would-be criminals from sensitive jobs working with children, the elderly, financial institutions, or

[38] Advertising slogan reportedly created by R&R Partners Inc, see - http://en.wikipedia.org/wiki/What_Happens_in_Vegas
[39] The Canadian Press, August 16, 2011 "Hacker posts hoax story about Jean Charest's death on Montreal newspaper's website.
[40] United States Securities and Exchange Commission, Quarterly Report of Registrant Facebook Inc., for the quarterly period ended June 30, 2012.
[41] Sliter, John R., 'The Risk of Being Un-Informed' - A Paper on the Character and Implications of Risk in the Context of Economically Motivated Crime (September 5, 2011). Available at SSRN: http://ssrn.com/abstract=1926195

in those companies that make up our critical infrastructure such as nuclear power plants. Without a doubt public safety has been enhanced by these efforts.

> *"For the most part business leaders agree…getting the right people on their team is essential for strong corporate performance and long term growth. With that being said the wrong people can have the opposite effect. For example, 25% of shop theft in Canada or $700 hundred million can be traced back to a retailers own employees. Businesses have a right to understand who they are hiring and how they will impact the organization whether it be positive or negative - a proper pre-employment screening process will help them do this.[42]"*

However, despite best efforts by the government and private sectors to maintain adherence to data quality standards, there is a lot of misinformation on the Internet and mistakes have been made.

In the past five years we have seen some western economies experience the worst unemployment rates since the Great Depression. Background checking companies are sometimes accused of making it even more difficult for workers to obtain employment. In the United States, it is reported that over ninety percent of employers conduct criminal background checks on applicants and although this is believed to be somewhat lower in Canada, we are seeing a significant increase. The widespread dissemination of criminal record histories arguably places significant limits on employment opportunities for an estimated sixty-five million adults (nearly one in four adults) in the United States who have some sort of criminal record. In Canada that is closer to one in ten.

There have also been some recent examples where criminal background checks resulted in incorrect information being passed on to the prospective employer. Two good examples came to light in July of this year in reporting by NBC Chicago[43].

The first example was the story of Samuel M. Jackson, of Chicago, Illinois in the United States who shared a reasonably common name, and found that three other Samuel Jacksons got mixed up into his criminal background report. They are three Samuel Jacksons convicted of sex offenses; two of whom were in prison. A background checking company created a background report that suggested he was a serious sex offender and that he had committed crimes meriting life in prison. Samuel M. Jackson, the job-seeker, is white and was 26 years old when the background report was performed. The three Samuel Jacksons whose reports were attached to his name were all decades older, African-American convicted sex offenders. One of them is incarcerated for a rape that occurred when the job-seeking Jackson was only four years old. InfoTrack reportedly settled for $35,000 and corrected Jackson's record[44].

---

[42] Anstey, Todd, President, Triton Canada. Personal Interview August 28, 2012
[43] Parker, Lisa, July 10, 2012. NBC: "When the Only Crime Is Having a Common Name", web-posted at http://www.nbcchicago.com/investigations/series/target-5/target-5-whats-in-a-name-mistaken-identity-139931853.html#ixzz23AjyQv5r
[44] Parker, Lisa, July 10, 2012. NBC: "When the Only Crime Is Having a Common Name", web-posted at http://www.nbcchicago.com/investigations/series/target-5/target-5-whats-in-a-name-mistaken-identity-139931853.html#ixzz23AjyQv5r

The second example was a little more complicated. In Milwaukee, Wisconsin, there is a Dennis Teague who has a 13-page criminal background report, listing numerous serious gun and drug offenses. But this particular Dennis Teague has never been arrested and has no criminal record. It seems that seven years ago, a cousin of his, wanted by law enforcement, used Dennis Teague's name when stopped by police. Mr. Teague, who has a college degree, complained that the name-based background report delivered to prospective employers by the state of Wisconsin was standing in the way of his employment. He says many interviews that seemed promising went nowhere, which didn't make sense until he says he discovered the misleading records blended with his report. Mr. Teague sued the state Department of Justice, asking that it change the way background information is disseminated, especially in the case of identity theft victims. Wisconsin Department of Justice has said its system is based on the interests of law enforcement. Although Wisconsin did offer Mr. Teague a letter that confirms his identity is separate from that of his second cousin's, and that he has no criminal record, Teague has said he can't get far enough in an interview process to get much use of such a letter[45].

Most recently, just this past month in August, 2012 the Federal Trade Commission in the United States fined an employment background screening company $2.6 million to settle charges that it failed to use reasonable procedures to assure the maximum possible accuracy of information it provided, failed to give consumers copies of their reports, and failed to reinvestigate consumer disputes, as required by law[46]. The FTC has alleged that HireRight Solutions failed to take reasonable steps to ensure that the information in their reports was current and reflected updates, such as the expungement of criminal records. Because of this, the FTC charged, employers sometimes received information that incorrectly listed criminal convictions on individuals' records. In addition, according to the FTC complaint, HireRight Solutions failed to follow reasonable procedures to prevent the same criminal offense information from being included in a consumer report multiple times, failed to follow reasonable procedures to prevent obviously inaccurate consumer report information from being provided to employers, and in numerous cases even included the records of the wrong person. The FTC alleged that these failures led to consumers being denied employment or other employment-related benefits.

In spite of these incidents, background screening has a positive effect on society. Almost every day there is a story in the media about the company, school, hospital or bank, etc. that did not do a proper background screening and some awful thing happened as a result. The internet offers such a treasure-trove of easily accessible information some organizations may find it tempting to take short cuts and just "Google" someone before hiring or allowing them to volunteer. However, because of the ease and quantity of the internet's unverified information, background checking companies are quite adamant that a robust process, complete with consent and discipline, is critical to ensure innocent people don't suffer because 'bad guys' slip through the cracks.

---

[45] Parker, Lisa, July 10, 2012. NBC: "When the Only Crime Is Having a Common Name", web-posted at http://www.nbcchicago.com/investigations/series/target-5/target-5-whats-in-a-name-mistaken-identity-139931853.html#ixzz23AjyQv5r

[46] Federal Trade Commission, Aug 8, 2012, "Employment Background Screening Company to Pay $2.6 Million Penalty for Multiple Violations of the Fair Credit Reporting Act". Web-posted at http://ftc.gov/opa/2012/08/hireright.shtm

> *"We all hate the security lines at the airport, but do you think people would want to do away with them to save a few minutes? Would they still get on the plane? Despite the overload of information and speed of technological advances, organizations and employees or volunteers can still be matched up safely – but it will be that discipline of proper process that will ensure such"*[47].

Discrimination based on a Criminal Record

Every Canadian province has a human rights statute and they all offer a balanced list of prohibited grounds of discrimination including age, disability, sexual orientation, political belief, race or skin colour and religion. Some, but not all, provide limited protection against discrimination based on having a criminal record. For example, the Charter of Human Rights in the province of Quebec contains the following reference:

> "No one may dismiss, refuse to hire or otherwise penalize a person in his employment owing to the mere fact that he was convicted of a penal or criminal offence, if the offence was in no way connected with the employment or if the person has obtained a pardon for the offence."[48]

In the United Sates, the Equal Employment Opportunity Commission[49] has interpreted the Civil Rights Act to require that, where an employment policy of a state, municipal, or private employer that discriminates against ex-offenders will have a disparate racial impact, employers must show a business necessity before automatically disqualifying ex-offenders[5051]. Some statutes prohibit hiring ex-offenders for certain types of jobs, such as health care or education, and forbid licensing boards from distributing licenses to ex-offenders or require the boards to consider the applicant's moral character. Professions requiring licensing can include ambulance drivers, billiard room employees, attorneys, physicians, pharmacists, nurses, barbers, embalmers, septic tank cleaners, realtors, accountants, contractors, and sellers of alcoholic beverages. Such regulations sometimes result from lobbying by professional communities seeking to raise barriers to entry.

As of 1998, seven states absolutely barred felons from public employment. Other states had more narrow restrictions, for instance, only covering infamous crimes or felonies involving 'moral turpitude'. Some laws have been criticized for being over-inclusive; for instance, a law banning all ex-offenders from working in health care jobs could prevent a person convicted of bribery or shoplifting from sweeping the halls of a hospital. California law provides that a criminal record can affect one's application for a professional license only if

---

[47] Dinesen, Dave, President & CEO of BackCheck, telephone interview of 2012-08-27.
[48] Charter of human rights and freedoms, RSQ, c C-12.
[49] U.S. Equal Opportunity Employment Commission, Backgrounder – April 25, 2012 – "What You Should Know About the EEOC and Arrest and Conviction Records.
[50] Sharon Dietrich, Maurice Emsellem & Catherine Ruckelshaus (1998), *Work Reform: The Other Side of Welfare Reform*, 9, Stanley L. & Policy Review, pp. 53, 56.
[51] U.S. Equal Opportunity Employment Commission, Backgrounder – April 25, 2012 – "What You Should Know About the EEOC and Arrest and Conviction Records.

"the crime or act is substantially related to the qualifications, functions and duties of the business or profession for which the application is made." Further, a certificate of rehabilitation can prevent a person from being denied a license solely on the basis that he has been convicted of a felony. Texas law requires that a variety of factors, such as the nature and seriousness of the crime, the relationship of the crime to the purposes for requiring a license to engage in the occupation, the amount of time since the person's last criminal activity, and letters of recommendation, be taken into account even when the applicant has a felony[52].

It does not go without saying that data on criminal histories is widely disseminated by private sector agencies. It is difficult for a job applicant to prove that a prospective employer illegally discriminated against the applicant based on information on expunged convictions or dismissed charges. The State of California does not erase an individual's criminal history but rather replaces "Conviction" with "Dismissed in Furtherance of Justice" in the disposition. Some state justice systems do not allow arrestees to deny arrests for which the charges were dismissed, and some do not allow those whose charges were expunged to deny the conviction.[53]

Information used for Immoral, Unlawful or Illegal Purposes

The explosive growth in the quantity and quality of personal data has created a significant opportunity to generate new forms of economic and social value for society. However, it is critical that we all consider these opportunities carefully and ensure we have the necessary rules, regulations and appropriate policy frameworks in place.

We have also seen unscrupulous people abuse new forms of social media as they strive to exploit opportunities for financial gain. There are numerous methods used to compromise social media accounts, most of which pertain to some form of Identity Theft or Identity Fraud. These include Hacking Accounts, Commandeering Accounts, Profile Cloning, Cross-Platform Cloning, Phishing, Fake Facebook, Affinity Fraud, Mining Unprotected info and of course, simple spamming[54]. **All of these situations share a common theme – there is a critical need for a secure electronic identity for both personal and corporate Internet users.**

The World Economic Forum has recently reported that Consumers and citizens are losing trust in the ability of business and governments to handle their personal data safely.

[52] American Law Facts – www.americanlawfacts.com – "Employment Discrimination Against Felons in the United States".
[53] Ben Geiger (Jul., 2006), *The Case for Treating Ex-Offenders as a Suspect Class*, 94, California Law Review, pp. 1191–1242.
[54] Sauter, Michael B., Poltrack, Adam, Allen, Ashley C., 24/7 Wall St., May 16, 2012.

> "*Among the three actors – individuals, organizations and governments - dialogue about personal data is currently anchored in fear, uncertainty and doubt*[55]".

Yet, at the same time, it was also reported that consumers continue to share personal data like never before and online retail continues to grow[56].

Many consumers and privacy advocates have voiced their fear of '*Big Brother*' but this author wishes to put some focus on another actor here that often gets missed - '***Bad Brother***'. While we have been focused on worrying about what government departments were doing with our personal and private information, we perhaps should have been looking at how the data is being used. There are sophisticated white collar organized crime groups who are quietly making unlawful use of these new technologies to gain access to confidential and private electronic information and often going relatively unnoticed. These people do not have to play by the rules and can be far more dangerous than any alleged government abuse of our personal information. **In short, Bad Brother can be far more dangerous than Big Brother!**

Electronic identities can be forged, fraudulent background checks sought and obtained. Official looking background check reports can be forged as well. Misinformation can be planted and cause certain individuals immense harm. Credit ratings can be tampered with. Secrets can be leaked. Employees may never get promoted, or perhaps never even get a job without ever knowing why. Travelers can experience difficulty crossing borders. Electoral candidates can be smeared. Organized crime, often buried away in the form of unethical and/or unlawful corporate strategies, can quietly shape the future of select people. Everyone has a secret - these may range from a long-time criminal record for which a pardon has been obtained to a seemingly harmless off-colour joke told at a party twenty years before and caught on film. **What is your secret?**

The Need for Credible and Secure Information

All of the above information supports the argument that there is a clear need for a very credible and secure source of data for use in background screening. Each country requires a common and credible source of information for use by both the public and private sectors. It must also be sufficiently secure that all stakeholders are confident it cannot be tampered with. If it is indeed evitable that people will continue to discriminate based on criminal activity for employment purposes, then surely it is much better to discriminate based on credible and reliable information.

[55] Rethinking Personal Data: Strengthening Trust – Report by the World Economic Forum, May, 2012.
[56] Rethinking Personal Data: Strengthening Trust – Report by the World Economic Forum, May, 2012.

Credibility:

Credibility is paramount and therefore it is suggested that this common source of information be controlled by governments, but in partnership with the private sector. A public portal to the government systems could be created complete with data validity checks and audit capacity. Great care must be taken as to precisely what information could and should be attributed to a given person or company. Reporting must be verified and substantiated with the view that an individual's life style or well being is at stake. Similar to the process used by credit bureaus, a challenge function must also be built into the system to allow a given reported person the right to question the accuracy of a given entry. All levels of users must be confident in the accuracy of the data and the foundation of each entry could consist of a basic criminal record check coupled with information pertaining to all police contact.

Security:

Security is another critical factor in consideration of a common and credible data source. Again, all users must be confident that it is indeed tamper-proof. There are measures that can be taken for both name-based and fingerprint-based searches. There are numerous user authentication systems available, some of which are biometric based[57]. Others use questions derived from separate secure and sensitive data systems to authenticate each user[5859]. The risk of a criminal gaining access to another criminal's criminal record might perhaps be considered comparable to that of a criminal gaining access to another's banking card. The financial risks have been mitigated to an acceptable level by user authentication and so can the risks pertaining to exposure of criminal activity information.

There is one particular best practice that has a mission worth noting here. The International Justice and Public Safety Information Sharing Network in the United States is entitled Nlets. Nlets is an interstate justice and public safety network dedicated to the exchange of law enforcement, criminal justice and public safety-related information. The Nlets system strives to provide reliability based on a network built to endure threats without impacting performance. The system is owned by the States and is a 'not for profit' organization that was created over 40 years ago by the principal law enforcement agencies of the States. The user population is composed of all of the United States and territories, all Federal agencies with a justice component, selected international agencies, and a variety of strategic partners that serve the law enforcement community—all cooperatively exchanging data[60].

[57] NIVID Biometrics in the United Kingdom advertises the VAJRA server that employs a users fingerprint biometric data to establish the identity of the user trying to access the system from any endpoint whether within network perimeter or outside it. http://www.nividbiometrics.com/Products/Online_Authentication.asp

[58] Equifax Credit Bureau offers an on-line authentication system – 'eIDverifier' - http://www.equifax.com/EFX_Canada/services_and_solutions/ecommerce_solutions/eidsol_e.html

[59] Transunion Credit Bureau also offers an on-line authentication system - http://www.transunion.com/corporate/business/solutions/financialservices/bank_identity-manager-authentication.page

[60] https://www.nlets.org/mission-vision

The Nlets concept is a great place to start and to partner with private sector agencies such as Spotcrime would entrench the 'duty to warn[61]' capacity for law enforcement and ensure that all stakeholders share a common goal - Public Safety!

Each country could model their own unique system with due consideration to their respective legal and political ambiguities. While all levels of Government around the world may be currently preoccupied with economic issues, it is critical that government experts and private sector stakeholders be encouraged to seize this opportunity to work closely together to design a new non-coercive system that is balanced and effective. There is great potential for a public-private partnership and with full cost-recovery for government.

Summary

As the world edges closer and closer to the convergence of man and machine, the human capacity to retrieve information is increasing by leaps and bounds. We are on the verge of knowing everything and anything there is to know and in the blink of an eye!

This means that police will have the capacity to learn everything about everyone with the only restriction being privacy legislation. But it also means that those involved in immoral, unlawful or illegal activity will have that same capacity and with no such restriction. 'Bad Brother' may be far more dangerous than 'Big Brother'!

The global community requires a secure and credible system to retrieve and assess all of the information 'generally available to the public'. A system that will strive to keep 'Big Brother' in check and 'Bad Brother' out, all the while providing a means of alerting citizens to genuine risks or to dangerous people. Such as system would help diffuse the systemic inaccurate and harmful profiling that is often based on rumours and innuendo.

There is an identified public-private partnership opportunity. A chance to work with privacy advocate groups and background checking private companies to define, design and deliver on something that will be of immense benefit to citizens around the globe. We have an opportunity to create something that will work to ensure that only the best information gets used and in a moralistic, lawful and legal way! Technology continues to move forward at incomprehensible speeds – failure to act could have serious consequences.

[61] Sliter, John R., 'The Risk of Being Un-Informed' - A Paper on the Character and Implications of Risk in the Context of Economically Motivated Crime (September 5, 2011). Page 9.

The author may be contacted for further discussion:

John Sliter, Superintendent
Director, Field Services
Canadian Police Information Centre
1200 Vanier Parkway
Ottawa, Ontario
K1A0R2

jsliter@rcmp-grc.gc.ca
Telephone: (613) 993-5172