"The Risk of Being Uninformed"

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

A paper on 'the character and implications of risk in the context of economically motivated crime'

Presented at
The 29th Cambridge International Symposium on Economic Crime

September 5th, 2011, Cambridge, England

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

The focus of this paper will be on a specific type of risk – within the context of sharing of information, or the lack there of - the risk of being uninformed.

Government agencies have come a long way in ensuring that all law enforcement information is shared, and shared quickly. For example, one has only to look at the U.S. based 'Lessons Learned Information Sharing' to confirm that governments, all too painfully, have been made aware of the risk should law enforcement fail to share information between agencies. The LLIS website notes that "*LLIS.gov serves as the national, online network of lessons learned, best practices, and innovative ideas for the emergency management and homeland security communities. This information and collaboration resource helps emergency response providers and homeland security officials prevent, protect against, respond to, and recover from, terrorist attacks, natural disasters, and other emergencies. LLIS.gov provides federal, state, and local responders and emergency managers with a wealth of information and front-line expertise on effective planning, training, and operational practices across homeland security functional area*[1].

This type of integrated information sharing has also been extended to include partnerships with the private sector. For example, in January 2007, the Retail Council of Canada, in partnership with Canada Post Corporation, launched the Retail Organized Crime Task Force. The Task Force's mandate is to raise the level of awareness associated with retail organized crime within the Canadian marketplace through collaborative partnerships, education, communication and information-sharing initiatives[2]. Another good example relates to InfraGard in the United States. *InfraGard is a partnership between the FBI and the private sector and consists of an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States*[3].

There are numerous other good examples within North America, some of which this author was personally involved in developing[4] [5]. In fact, these types of

[1] https://www.llis.dhs.gov/index.do
[2] Canadian Association of Chiefs of Police, Private Sector Liaison Conference *"Building Private Security & Public Policing Partnerships"* January 2008
[3] http://www.infragard.net/
[4] Sliter, John R., 'The New Deal - Ensuring Integrity, Stability and Survival' - The Financial Crisis - A Perspective on Cause and Effect (September 6, 2010). Twenty-Eighth International Symposium on Economic Crime, Cambridge, England, September 6, 2010. Available at SSRN: http://ssrn.com/abstract=1687652
[5] John Sliter, Carl-Denis Bouchard, Guy Bellemare, (2005) "The Canadian response to the Sarbanes-Oxley Act: managing police resources; a competency-based approach to staffing", Journal of Financial Crime, Vol. 12 Iss: 4, pp.327 - 330

community safety partnerships form the very foundation of community and integrated policing in Canada.

A key point here is that we are now approaching an environment where almost nothing is considered sacred when it comes to weeding out terrorists or international money launderers. For the most part at least, personal Income Tax and Health records still remain off-limits. However, the winds are shifting and some suggest that matching social security and personal tax records might identify people who might be claiming benefits while undertaking paid employment[6]. And, this past week the U.K. Government announced an agreement with Switzerland to secure billions in unpaid tax[7].

This type of information could be a topic of discussion in itself but the focus here will be on the other side of the supposed partnership – what does the private sector in turn receive from law enforcement?

Most, if not all, of these partnerships are very one-sided and have a mandate to provide direct support to law enforcement. Is the equation simply one where the motive of good corporate citizenship and moral suasion is sufficient to get the private sector to turn over everything they know about suspected terrorists or hardened criminals? What about the information needs of the private sector?

Background Screening by the Private Sector

To see where the author would like to go with this, one should consider the motive and context of background screening, from a private sector perspective. Let us begin by defining a background check.

Wikipedia defines a Background Check as follows:

> *"A **background check** or **background investigation** is the process of looking up and compiling criminal records, commercial records and financial records (in certain instances such as employment screening) of an individual.*
>
> *Background checks are often requested by employers on job candidates, especially on candidates seeking a position that requires high security or a*

[6] Public Management and Governance, 2nd Edition - 2009, p. 143., Bovaird, A. G. and Loffler, Elke
[7] HM Treasury, Newsroom & Speeches, August 24, 2011 - http://www.hm-treasury.gov.uk/press_98_11.htm

> *position of trust, such as in a school, hospital, financial institution, airport, and government. These checks are traditionally administered by a government agency for a nominal fee, but can also be administered by private companies. Results of a background check typically include past employment verification, credit score, and criminal history.*
>
> *These checks are often used by employers as a means of objectively evaluating a job candidate's qualifications, character, fitness, and to identify potential hiring risks for safety and security reasons. Background check is also used to thoroughly investigate potential government employees in order to be given a security clearance. However, these checks may sometimes be used for illegal purposes, such as unlawful discrimination (or employment discrimination), identity theft, and violation of privacy."*[8]

Providing you are tenacious in nature and ready for some time-consuming effort, today you can find out just about anything or everything about anyone. Examples range from a simple Internet search to viewing the twitter or facebook accounts of high profile politicians to searching through voluminous amounts of civil litigation proceedings in an effort to find out the role of a given participant. In fact, the internet search engine has done far more for the background screening industry than has law enforcement. One recent study notes that in 2011 alone, 1.8 zettabytes (or 1.8 trillion gigabytes) of data will be created, the equivalent to every U. S. citizen writing 3 tweets per minute for 26,976 years[9]. An important point raised within this same study noted that the amount of information people create by writing email messages, taking photos, and downloading music and movies is far less than the amount of information being created ***about*** them.

In essence, 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. The quality or validity of some of the information is another matter. For example, on August 16, 2011 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[10]. This was quickly proven unfounded and the premier was alive and well.

The background screening industry has grown exponentially in recent years and a basic foundation of this screening most often includes a criminal record check. A U.S. based survey in 2010 found that 93% of all organizations conduct criminal

[8] http://en.wikipedia.org/wiki/Background_check, downloaded on August 16, 2011.
[9] Gantz, John and Reinsel, David, "Extracting Value from Chaos", and EMC Corporation Study, June, 2011
[10] The Canadian Press, August 16, 2011 "Hacker posts hoax story about Jean Charest's death on Montreal newspaper's website.

background checks on job candidates[11]. At the same time that the background check industry has expanded, the share of the U.S. population with criminal records has soared to over one in four adults. The above referred survey also queried the motive and industry behind the criminal record checks and the charts on the following page are reproduced with the kind permission of the Society for Human Resource Management. One can immediately see some direct linkages to public safety issues. Based on the nature of the industries involved and the reasons indicated for their queries, it is now suggested by this author that it would be entirely appropriate to include the mandate for private sector criminal record screening within that of public or community safety.

If one steps back a bit and considers both the mandate of law enforcement and the motive of the private sector agencies for conducting criminal record checks, we can see an overreaching broad objective – public safety. The profit motive of the private sector organizations should also not be discounted – the safety of our capital markets and our national economic integrity depend on it. Good due diligence is a legitimate economic security issue.

Some groups have expressed concern that denying any type of employment based on criminality may be illegal in some jurisdictions[12]. This is a valid concern and is not easily addressed but it could be argued that discrimination on the basis of a confirmed criminal record is much better than discrimination on the basis of a suspected or even falsely attributed criminal record. The author notes that legality of private sector background checks in Europe appears to be similar to that in America and often rests on the person conducting the check obtaining full consent of the person being checked[13]. Human Rights legislation often dictates that a test be applied when making employment decisions based on an individual's criminal record, is the record recent? – and, is it relevant to the position?[14] [15]

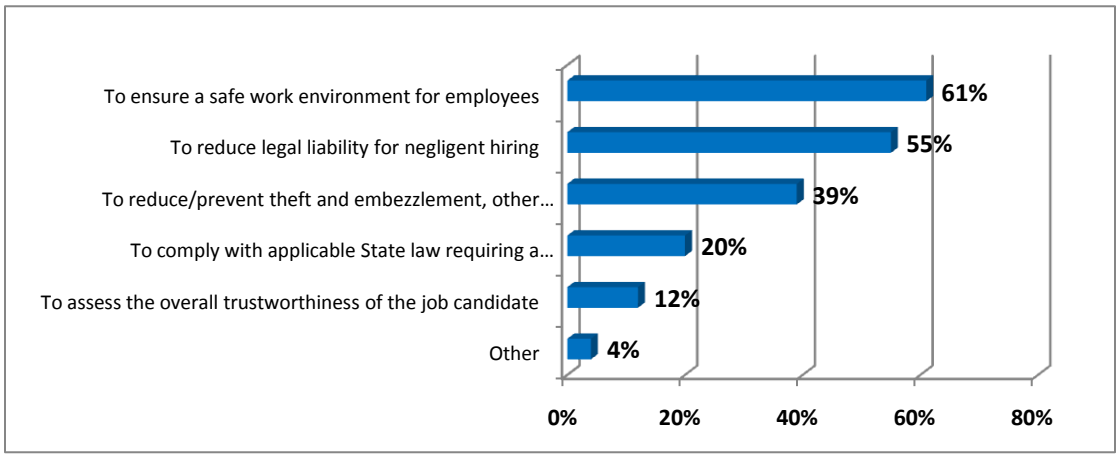
[11] Background Checking: Conducting Criminal Background Checks SHRM Poll, Society for Human Resource Management, January 22, 2010, http://www.shrm.org/Research/SurveyFindings/Articles/Pages/BackgroundCheckCriminalChecks.aspx
[12] Rodriquez, Michelle Natividad and Emsellem, Maurice, "65 Million Need Not Apply – The Case for Reforming Criminal Background Checks for Employment", March, 2011
[13] Wisskirchen, Gerlind. WHO'SWHOLEGAL, Background Checks in Europe, July, 2011
[14] Australian Human Rights Commission – 'Discrimination on the basis of criminal record" – webposted at http://www.hreoc.gov.au/human_rights/criminalrecord/index.html
[15] Canadian Human Rights Commission - http://www.chrc-ccdp.ca/default-eng.aspx

Demographics: Organization Industry

Industry		Industry	
Health care, social assistance (e.g., nursing homes, EAP providers)	18%	Insurance	5%
Services—professional, scientific, technical, legal, engineering	12%	Retail/wholesale trade	4%
Manufacturing—other	11%	Construction, mining, oil and gas	3%
Educational services/education	8%	Other services (e.g., nonprofit, church/religious organizations)	3%
Government/public administration—federal, state/local, tribal	5%	High-tech	3%
Financial services (e.g., banking)	5%	Telecommunications	3%
Transportation, warehousing (e.g., distribution)	5%	Utilities	3%

What are the primary reasons that your organization conducts criminal background checks on job candidates?

16



[16] Background Checking: Conducting Criminal Background Checks SHRM Poll, Society for Human Resource Management, January 22, 2010, Reproduced with email permission from Margaret Clark, August 19, 2011

This author is also concerned that thorough background screening may often dictate violations of applicable privacy legislation. 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.

In order to propagate an analysis, readers are invited to consider the following.

Business has determined that the risk of being uninformed far outweighs the risk of showing little respect for the privacy of a person's life activities.

If the above statement is factual, then there are two ways law enforcement and government could deal with this knowledge. Firstly, we might decide to stand behind the privacy advocates and adopt stricter privacy law, complete with significant penalties for violators.

However, it is at a forum such as the annual Cambridge Symposium on Economic Crime, where academics, law enforcement and policy makers are all gathered together, to share and explore creative ideas, where the author wishes to share a personal position and look towards the future.

Alternative to the reaction above, we might also consider this era of little privacy as inevitable and perhaps even a good thing. In fact, it is asserted that real, solid, fact-based information is beginning to dominate and essentially overwhelm or 'weed out' misinformation. It is also optimistically believed that we are moving closer and closer to that euphoric economic state of perfect information. Law enforcement should not try and fight the enhanced information flow brought about by new technology. In presentations before a Cambridge Symposium back well over a decade ago, this author prophesized at length that the public would soon have the ability to take pictures and videos of crimes they were witnessing and sending them into police in real time[21]. Of course that time has indeed come and we now see where the eyes and ears of the police, and the public, have grown exponentially. One can see and hear everything everywhere from within the comforts of your home living room. There is currently one Canadian company who invites people to visit their website and identify people from a photo of a large crowd and then visit their individual Facebook profile[22]. The photo file is 2,110

[21] Sliter, John. "The Internet and Criminal Law: The Detection and Investigation of Stock Fraud", October 13, 2000 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1152848

[22] See http://www.gigapixel.com/image/gigatag-canucks-g7.html - reviewed August 16, 2011.

megapixels and allows users to zoom in on individuals within the crowd immediately before the Stanley Cup riots in Vancouver, British Columbia on June 15, 2011.

There are also some serious negative consequences to this type of information sharing. We recently witnessed how technology was used to proliferate the riots in London, England which were dubbed 'Blackberry Riots' by media from around the globe[23]. The use of social media and BlackBerry messages were reportedly used to identify targets for destruction and looting.

All of the above said, the author believes it is time for the Government and Law Enforcement to truly come of Internet Age and begin to open up some of those so called secret databases we have selfishly guarded for so many years. This does not mean the complete exposure of current and active criminal investigations. On the contrary, the information contained therein must be guarded with great care. However, there are other records that could, and should, be shared openly with those people about to make conscious and meaningful business decisions, that had they known, they might have thought otherwise. To start with, let's consider criminal record information. Some jurisdictions within the United States already make this information available to the general public and, via the Internet and this should be applauded. What is wrong with conducting thorough background checks on a potential business partner BEFORE you invest several million dollars of your life savings - absolutely nothing! Would that not be considered good due diligence or even crime prevention?

This is not to suggest that law enforcement or government should jump into the background screening business. There are ample private sector entities in existence today and they are doing a fine job. What is being suggested is that law enforcement could take steps to partner with these private entities, open up criminal record and criminal reporting databases and use this information to complement the efforts of the private sector agencies.

We are in an era where law enforcement and the supporting public are often outraged to learn that the private sector was aware of ongoing criminal or terrorist activity and did not report it to police. Why are we not equally concerned when the shoe is on the other foot when police do not share their knowledge of unscrupulous criminals with legitimate and unsuspecting business partners?

[23] BlackBerry riot driven by the mob mentality, The Australian, August 10, 2011.

A Duty to Warn

Many jurisdictions around the globe have determined that police have a duty to warn the public if there is a predator on the loose. The Supreme Court of Canada affirmed the holding of an Ontario court in a case called Jane Doe that looked at a series of sexual assaults where police knew the exact method of breaking in and which women would be likely targets of a serial rapist, but didn't warn women of the threat. The Court found that conduct to be negligent and awarded Jane Doe damages for a sexual assault that was perpetrated on her[24]. This same principle has obviously not yet been extended to complex economic crimes otherwise the police might have an obligation to broadcast extensive criminal records of repeat fraudsters as opposed to guarding them as secrets. All too often, victims of complex economic crime have to rely on media reports or internet searches to look for these warnings.

Online dating is something that has become very popular in recent years and there are reports that it generated $1,863 million in revenue in the United States alone in 2010[25]. Some jurisdictions are taking action with regard to safety and the State of New Jersey passed the Internet Dating Safety Act in 2008[26]. The state requires dating sites that don't perform criminal background checks to prominently disclose that on their Web site. And more recently, a lady in Los Angeles was sexually assaulted by a man she met on the popular dating site Match.com. Afterwards, she did some online sleuthing and discovered that her date had a history of sexual battery. The woman filed a lawsuit against the dating site, stipulating that the company should check members' names against public sex offender registries in order to increase safety. The site has since announced that they do plan on screening members to see if they have a history of sexual assault[27].

The State of Texas in the United States has taken this concept of 'Duty to Warn' a step further and just had their "Teacher Protection bill" go into effect this past week, which puts a requirement for law enforcement to notify school superintendents, teachers and staff of offences committed by their students[28]. Juvenile criminal records were traditionally off-limits.

---

[24] Doe v. Metropolitan Toronto (Municipality) Commissioners of Police, 1998 CanLII 14826 (ON SC)

[25] IBISWORLD Research, "Online Dating in US", May 26, 2011 - http://www.ibisworld.com/industry/default.aspx?indid=1723
[26] Internet Safety Dating Act, http://www.state.nj.us/lps/ca/laws/InternetDatingAct.pdf
[27] Gibson, Megan, TIMENewsFeed, April 18, 2011
[28] Olano Star Courier, June 3, 2011, web posted to http://www.planostar.com/articles/2011/06/05/plano_star-courier/news/9037.txt

In Canada, The Minister of Public Safety also just recently expanded a public listing of Canada's most-wanted suspected war criminals, albeit to the chagrin of Amnesty International[29]. The Minister of Immigration's response to their concerns fits in with the theme of this paper - "*Is it your position that the Canadian public does not deserve to know that these men are hiding among us unless or until each of them has signed a privacy waiver allowing details of their complicity in crimes against humanity to be made public? If so, I respectfully disagree. I believe the Canadian public deserves better*"[30].

Reported Crime in the Media

On August 9, 2011, the news media published the name and a photo of a man charged and convicted in the State of California in the United States for ejaculating into a female co-worker's water bottle[31]. Would you not want your Human Resources department to conduct a background check on this individual before hiring him to work within your office? The story and photograph of 32 year old Michael Kevin Lallana will presumably be stored within the archives of all of the many media outlets covering the story and be searchable and retrievable for an extended period.

Also on August 9, 2011, the news media published the name and a photo of a woman charged, but not convicted, in the province of Manitoba in Canada for Human Trafficking[32]. The media were reporting that the Crown was abandoning the case and dropping all charges. However, the story and photograph of 39 year old Theresa Peebles will also presumably be stored within the archives of all media outlets covering the story and be searchable and retrievable for an extended period.

In fact, most major newspapers market or sell archived information going back well over a decade[33] and sometimes back a century! One particular archive site claims to have the world's largest collection of newspaper archives online, featuring billions of newspaper archives from the U.S. and the world. These news

[29] Globe and Mail, August 18, 2011, Web-posted to http://www.theglobeandmail.com/news/politics/ottawa-notebook/amnesty-defends-its-concern-for-rights-of-canadas-most-wanted/article2133820/
[30] The Hon. Jason Kenney, M.P., Response to Open letter from Amnesty International, August 8, 2011, web-posted to http://www.jasonkenney.ca/news/an-open-letter-to-amnesty-international/
[31] Toronto Sun, web posted Tuesday, August 9, 2011, http://www.torontosun.com/2011/08/09/man-who-ejaculated-in-water-bottle-must-pay-27gs
[32] CJOB News Radio, Winnipeg, Manitoba, web posted to http://www.cjob.com/News/Local/Story.aspx?ID=1515284
[33] The Globe and Mail, http://gold.globeinvestor.com/plus/index.html

archives include obituaries, birth announcements and sports articles, are full-page and fully searchable[34].

The above two scenarios are used to make a point that the opening up of criminal record databases might be a good thing. Please consider the plight of any other person who might happen to have the same name of Michael Lallana or Theresa Peebles. The current system in many jurisdictions often causes suspicious partners, neighbours or even private sector potential employers to rely on open source background checks. In such a scenario where they find the above mentioned newspaper articles 5 or 10 years later, they might be inclined to think they have the right person.

A much better system might be to have the government correctly identify all charged and convicted individuals and allow the public to have full access. Neighbours could query neighbours, employers could query potential employees and those inclined could query potential boyfriends or girlfriends before getting romantically involved. Such a system would go a long ways in reducing risk of economic crime while also helping to ensure there are no mistaken identities.

The author has worked in Canadian law enforcement for over 30 years and can personally attest to having met countless business people who have been swindled, defrauded etc by other people who were well known to law enforcement.

> *"Had I known that he had an extensive criminal record for fraud, I never would have done business with him[35]".*
>
> *"Had I known that he had an extensive criminal record for fraud, I never would have got involved with him[36]".*

The above two generic statements are reflective of many individuals and they range from international corporate financiers who get involved with the wrong people to individuals involved in online dating and victims of romance fraud. The point is – millions of people worldwide are falling victim to shysters of one sort or another, all because they are ill-informed.

[34] Newspaperarchive = http://www.newspaperarchive.com/?gclid=CLa-soqdxaoCFQ7MKgodFnjA6Q
[35] Comment derived from personal interviews of numerous Fraud Victims by Supt. John Sliter, 1986-2011,
[36] Comment derived from personal interview of confidential Romance Fraud victim by Supt. John Sliter, June 23, 2011

Privacy Rights – Criminals vs. Innocents

In Canada, we have approximately 34 million citizens of whom somewhere around 3.3 million, or 10%, have a criminal record[37]. We, like many other countries, are often accused of subjecting the remaining 30 million 'clean' people to significant inconvenience as they strive to prove they are in fact clean. This can have a significant detrimental effect on some organizations, such as volunteers who work with children. We do so in order to protect the privacy rights of the 4 million criminals. We are often asked "Why do I have to prove my innocence?" or "Why are innocent people asked to pay for the indiscretions of criminals looking for anonymity?[38]" Perhaps it is time to consider making the records of the criminal's public and thereby making it significantly easier to prove one does indeed NOT have a criminal record.

Law enforcement are guardians of ALL citizens and have a duty to protect those citizens - even those with criminal records - from UNDUE persecution. While civil libertarian and privacy advocate groups may remind us of this and identify concerns for the well-being of those convicted of criminal offences, we should be reminded that we also owe a standard of care to innocent law-abiding citizens who may fall victim. What about the rights of those unaware business people who may partner with unscrupulous fraudsters? What about the rights of unaware baby-boomers who may invest their life savings to quick-talking con-men? What about the rights of unaware seniors who may hire a cleaning lady, only to find that she stole their banking information and robbed them blind? What about the rights of the online lady who got romantically involved with a long standing violent control freak and financial predator? And, what about the rights of those unaware parents who allowed their children to play in the street in front of the home of the chronic drunk driver? One Canadian citizen points out "*Convicted criminals do not deserve to be protected under the privacy laws since they do not follow the law in the first place*"[39].

Back in 2001, a U.S. based survey of public attitudes toward the uses of criminal history information found that there was substantial public support for making certain types of criminal justice records available outside the criminal justice system when there is a perceived rationale of public benefit and/or safety[40].

---

[37] Bechard, Bob, CPI Centre, Canadian Criminal Name Index file, August 13, 2011, "3,348,253 Active Records".
[38] Edmonton Journal, July 3, 2011, "Police policy kills volunteer spirit".
[39] Anonymous comment to Supt. John Sliter, August 18, 2011.
[40] U.S. Department of Justice, Bureau of Statistics, "Privacy, Technology and Criminal Justice Information – Study on 'Public Attitudes Toward Uses of Criminal History Information', July, 2001.

However, it was also noted that support declined noticeably when the goal is purely private. In general, American adults tend to favour making individual conviction records available to employers, governmental licensing agencies, and other entities. They are far more reluctant, however, to support access to arrest-only (or arrest without conviction) records.

Transparency of all Reported Crime

In spite of that 2001 study referred to above, one could push the envelope even further and state that we also require a public database of all reported crime. This 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 will go so far as to suggest that this will also be inevitable. 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.

On August 11, 2011, Canadian media began publishing the story of a Toronto, Ontario elementary school teacher who had been charged with sexual assault after allegedly having an affair with a 13-year-old student. By early afternoon on that same date, this author was able to determine that Orlando Fusaro, aged 37 had his name and photograph posted to no less than 27 different media sites or special interest crime sites. This man was not convicted nor given an opportunity to claim innocence before this information is spread throughout cyberspace to be searchable and retrievable presumably forever. He was essentially tried and convicted within the court of public opinion within a four hour period. While the appropriateness of this information sharing or flow could be debated at great length, the point being made is that there is no stopping it. It simultaneously travelled in social networking circles such as Facebook. It is the interconnectivity of new technologies that is feeding this evolution. Consider what will happen should Mr. Fusaro later be found innocent of these serious charges. Should the general public become accustomed to searching a credible government managed web-based crime report database, a record would be made of persons later found to be not-guilty.

Of course there are risks to opening up crime reporting and criminal record databases to the public, and detractors will be quick to point out that such an open system would have potential to cause havoc. One might reasonably foresee the potential for vigilantism, extortion or blackmail. One might also foresee an increase in discrimination based on a criminal record. It was not that long ago that we were cautioned as children that it would be important 'never to get a criminal record as you would not qualify for a government job'. This has now been extended to 'you might not qualify for any job'! All sorts of corporate HR departments are relying on candidate consent to conduct criminal record background checks. These include those seeking to hire department store cashiers, bank tellers, or even telemarketers. Again, there is no stopping it – just as there is no stopping the Internet itself – it is simply freedom of information.

One could also argue that such an open system of information sharing will provide enhanced identity confirmation and ensure that discrimination is at least not based on the false identification of a criminal record. The rights of innocent persons who should happen to have the same name and/or date of birth as a criminal would be better protected.

This concept of transparency is not entirely without precedent. In the spring of 2007, the Ontario Ministry of Community and Social Services began to publish photographs and personal information on persons who were not making their required court-ordered child support payments[41]. The website is aimed at finding 'deadbeat dads' but it has been noted that the website looks much like a list of wanted posters[42].

There is also a National Sex Offender Registry in the United States and in Canada. The public does not have access to the National Sex Offender Registry in Canada. However, there is a public National Sex Offender website in the United States that enables every citizen to search the latest information from all 50 states for the identity and location of known sex offenders[43]. The registry in the state of New York includes the following information in its disclaimer[44]:

> *The information in this Subdirectory must be used responsibly. Anyone who uses this information to harass or commit a criminal act against any person may be subject to criminal prosecution.*

[41] See website http://www.mcss.gov.on.ca/en/goodparentspay/gpp_index.aspx, Reviewed on August 11, 2011.
[42] CBC News, February 19, 2007 – "Ontario website features first batch of deadbeat dads"
[43] Federal Bureau of Investigation - http://www.fbi.gov/scams-safety/registry - reviewed August 17, 2011
[44] New York State Division of Criminal Justice Services, http://criminaljustice.state.ny.us/SomsSUBDirectory/search_index.jsp#disclaimer, downloaded August 17, 2011

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 - all that needs to be done is to extend that protection to include perpetrators of all serious crime such as chronic drunk drivers, break and enter artists, and of course, white collar crime specialists!

Opportunity for Creativity

At the annual Cambridge Symposium on Economic Crime it is very appropriate to openly consider different possibilities and opportunities to create some new form of public crime registry system. Imagine a system where parameters could be established so that anyone convicted of more than one serious offence is automatically registered in a searchable public database (i.e. two separate convictions for Assault). Imagine that system to include a crime reported record should someone be reported on by more than three domestic citizens for the same type of offence (i.e. three separate and legitimate complaints of fraud). Imagine a system based on reputational scores, similar to eBay. For example, just as some sellers refuse to sell to any person with a transactional score of less than ten, the crime registry could use parameters to only list suspects that have been reported by more than 3 reputable persons. To use the forest fire analogy, this would essentially mean there are three reputable sightings of smoke and therefore residents should be warned that there may indeed be a fire.

Imagine how the above described system could be fine-tuned to establish an effective early warning system and enhance public safety!

A project such as the one described above, could, should and would, be championed by the private sector. All that is required is the political will and partnership of law enforcement and government. There would be an exciting opportunity for cost recovery for government as well as for profit for the private sector. There is a need for this information, a market demand if you will. There is also a risk - should our governments choose not to get out front to ensure that the system is credible and accurate as the evolution of data mining to produce internet-based profiles on people is moving at a furious rate. This type of profiling will happen, with our without us. For example, in another very recent survey published by the Society for Human Resource Management, slightly more than one-quarter

(26%) of organizations indicated that they use online search engines to screen job candidates during the hiring process[45]. However, it is important to note that a full two-thirds (66%) indicated they do not use social networking websites due to the concern about the legal risks, i.e. discovering information about protected characteristics (e.g., age, race, gender, religious affiliation), an increase from 54% in 2008. Nearly one-half (48%) of organizations do not use these sites because they cannot verify with confidence the information from a job candidate's social networking page, an increase from 43% in 2008. Another 45% indicated that the information found on the social networking sites may not be relevant to a candidate's work-related potential or performance, also an increase from 36% in 2008. In short, this situation begs for a credible and relevant source of data – something like a person's history concerning their relationship with law enforcement.

The Future:

Technology is driving some significant changes in the way law enforcement conducts business. Police worldwide have begun to recognize the benefits of integration with social networking sites. Authorities in the United States recently announced the first mobile application to help parents locate missing children. The Federal Bureau of Investigation 'Child ID' app, available on the iPhone, allows parents to upload photos and descriptions of their children – basically preparation for the unfortunate event should their child go missing[46].

This author can foresee a day in the near future where these types of mobile apps will use facial recognition software to instantly identify missing persons, wanted criminals and even identify participants of crimes in progress! Use your imagination to envision a direct interface between law enforcement databases and those associated with social networking sites to have the immediate effect of identifying the location of all of the above persons of interest. While detractors may think this might be getting perilously close to the old science fiction nightmare associated with microchip implants, in reality it would simply be taking advantage of technologies and systems already in place.

[45] The Use of Social Networking Websites and Online Search Engines in Screening Job Candidates, Aug 25, 2011, Reproduced with email permission from Margaret Clark, Aug 19, 2011
[46] http://www.fbi.gov/news/stories/2011/august/child_080511

Summary

Regardless of our concern for privacy, real-time criminal activity information is being disseminated throughout cyberspace by the private sector. This information is growing very quickly while being archived for search and retrieval on a long term basis. This is inevitable and could not, nor should not, be stopped. Some countries continue to try and censor the Internet[47], but for most part, have had limited success. As technology continues to make Internet access faster, cheaper and accessible everywhere, the only real viable option is to consider the opportunities, get out front and ensure that standards and guidelines are established. Design technical and procedural controls as key enablers for proper information sharing. Law enforcement and government policy makers should consider the risk of sharing with the risk of not sharing and allow the private sector to participate in the management of this risk in an informed way. The private sector has the right to be as well informed as law enforcement – they often have as much, if not more, to lose.

Let us look around us and into the future. The private sector has created some outstanding electronic systems that are both secure and deal with online personal authentication[48] and online reputation[49]. Law enforcement should maintain awareness of these and take advantage of developments as they occur.

Law enforcement should also not be afraid of true partnership with the private sector - meet with privacy experts within government and reconsider the level of secrecy attached to the criminal records and crime reports that have been carefully guarded for all of these years. Whenever and wherever possible, secrecy levels should be abandoned, particularly when one can make a reasonable argument for a 'duty to warn'. There is an opportunity to use valid substantiated information to clarify, correct and override some of the misinformation that is available openly on the Internet.

Fully transparent reported crime along with fully transparent end-results (i.e. criminal records) could be a wondrous thing for the safety of our citizens. It is time that the private sector received more on their side of the private sector law enforcement partnerships. This would undoubtedly go a long ways in preventing much crime before it happens as more and more business people and safety-

[47] Wines, Michael, The New York Times, Asia Pacific, "China Creates New Agency for Patrolling the Internet", May 4, 2011
[48] See Equifax' eIDverifier http://www.equifax.com/EFX_Canada/services_and_solutions/ecommerce_solutions/eidsol_e.html
[49] See ebay - http://pages.ebay.ca/help/feedback/scores-reputation.html

minded members of each community become better informed about who they are dealing with. The risks associated with being uninformed are very high. And, we do have a 'duty to warn'.

The change of thinking required to bring about transparency of crime is significant and would require much support from across all sectors of society. It would take many champions with great determination and moral aptitude. We might consider the words from the recent call to arms by British Prime Minister David Cameron following the British riots.

"We know what's gone wrong: the question is, do we have the determination to put it right? [50]*"*

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

[50] British Prime Minister David Cameron, 'PM's speech on the fight back after the riots', August 15, 2011, downloaded from the office site of the British Prime Minister's Office - http://www.number10.gov.uk/news/pms-speech-on-the-fightback-after-the-riots/