REVIEW OF THE EXPERT REPORT BY FRED H. CATE

Dated September 22, 2013

Condon et al v. H.M. the Queen

Norman P. Archer

October 21, 2013

Professor Cate's Report is very extensive and contains a lot of detail that may be relevant to the Human Resources and Skills Development Canada (HRSDC) Student Loans case. To avoid getting into too much detail in these comments on his report, the following addresses only the seven summary points included on Page 2 of his report, III Summary of Opinions. In each of the numbered points that follow, Professor Cate's statement appears in italics, sometimes including some related material from the remainder of his report. My comments in regular text follow each numbered statement.

1. The risk of identity theft is lower than popular claims suggest, and in the case of true identity theft—the only type of fraud that conceivably could be facilitated by the data on the missing HRSDC hard drive—appears to be declining over the past decade in real terms, as a percentage of frauds reported by consumers, as a percentage of households, and as a percentage of total identity theft cases.

"True identity fraud" is suggested by Professor Cate to be declining over the past decade in real terms… but the decline he shows is actually reported in percentage of total frauds reported in a U.S. survey by Sentinel (Figure 1 on page 5 of his report). Although it may be declining in percentage terms, the actual number of such identity frauds continues to INCREASE, as he shows in Figure 1 of his report, and this reflects the trend that is of interest in the current discussion.

On page 5, Professor Cate argues that "It is common for journalists, politicians, and entities selling identity theft "solutions" to decry identity theft as one of North America's the fastest growing crimes." The plaintiffs are not trying to sell identity theft solutions, so this is of no interest in the current presentation.

On page 4, Professor Cate says that "The data provided by identity theft solutions is very valuable, but may underestimate the prevalence of identity theft since many people do not report suspected identity theft to law enforcement." I agree that it has long been known that the prevalence of identity theft is very much underestimated by reports to law enforcement agencies in Canada. The percentage of cases of identity fraud reported in Canada are: to the police (13%), to credit reporting agencies (6%) and to PhoneBusters (the RCMP/OPP fraud reporting agency at that time) (0.5%) according to a 2008 publication[1] .

[1] Susan Sproule and Norm Archer, "Measuring Identity Theft in Canada: 2008 Consumer Survey", *McMaster eBusiness Research Centre (MeRC) Working Paper MeRC#23*, July 2008.

2. Data breaches do not appear to contribute in any statistically significant way to identity theft. Not only are most data involved in "breaches" never exploited, many breaches—including some of the largest—never involve access to data at all. That appears to be the case here. Despite approximately one-fifth of the potentially affected individuals taking advantage of fraud flags on their credit reports, there is no evidence that the missing data have been found or accessed or that fraud is occurring at a higher than usual rate. Even in cases where the data have been deliberately targeted and exist in bulk or in combination with other sensitive information the available evidence shows that data breaches do not contribute significantly to identity theft.

A major risk of criminal use of SINs (Social Insurance Numbers) and related identity information arises from situations where credit checks are not required. This leads to identity fraud victimization of 0.3%[2] of Canadians each year. Also, as Professor Cate's report indicates, there are a number of federal agencies that require the use of SINs when applying for benefits of some type. One would expect that criminal use of stolen SINs would be likely to target these agencies. A 2005 Ipsos-Reid survey of Canadians[3] found that 9% percent said "they, or they and someone they know personally" had been victims of identity theft. Of the classifications of identity theft found in that survey, 24% were classed as obtaining government benefits or healthcare. This results in a total of 2% of those surveyed that had suffered identity theft of this nature. In the case of the 583,000 people in the stolen or mislaid database, this would put more than 11,000 people at risk without even considering the additional risk from the Student Loan data breach (the percentage number is larger than the other numbers discussed here because it is not an annual number but is based on all the recollections of individuals surveyed). Although overall statistics on the fraudulent use of SINs is not publicly available, a related example is the fraudulent use of health cards in Ontario for obtaining healthcare services. Here, the Ontario Health Insurance Plan, after being chastised by the Ontario Auditor General about the high rate of health service fraud in Ontario, has been in the process of converting their identification cards to photo ID cards[4]. To my knowledge, no security measures of this sort are being contemplated by the federal government for SIN cards.

3. "SINs are widely available elsewhere. The inability of HRSDC to locate the hard drive does not materially contribute to any increased availability of SINs or diminish any individual "control" over the widespread use of SINs." Professor Cate also states on Page 12 of his report that "SINS are widely available today. This fact suggests the fallacy of the argument that disclosure of an SIN (or an SSN in the United States) leads inexorably to identity theft." On page 13 he states "Second, the fact that SINs are so widely available elsewhere—electronically, in bulk, and in connection with other sensitive information such as date of birth—suggests how unnecessary the lost hard drive is for identity theft." He also indicates "The most recent survey data suggest that half of Canadians still carry their SIN cards in their wallets or purses, despite having been advised not to do so."

Nobody is arguing that disclosure of a single SIN leads inexorably to identity theft. And whether or not Canadians carry SIN cards on their person is not relevant to this case. What is being argued by the plaintiffs is that massive numbers of SINs plus associated identity information in criminal hands

---

[2] Susan Sproule and Norm Archer, "Measuring Identity Theft in Canada: 2008 Consumer Survey", *McMaster eBusiness Research Centre (MeRC) Working Paper MeRC#23*, July 2008. This is an average rate of victimization of Canadians from new account and other identity fraud each year (does not include existing account fraud).

[3] Ipsos-Reid, "Concern About Identity Theft Growing in Canada", Insurance Canada, Feb. 28, 2005, http://www.insurance-canada.ca/market/canada/Ipsos-Reid-Identity-Theft-503.php

[4] Auditor General of Ontario, Chapter 3 Section 3.08 Ministry of Health and Long Term Care Ontario Health Insurance Plan 2006

may have led to a significant incidence of identity fraud. Further, the meaning of Professor Cate's statement that "SINs are widely available elsewhere – electronically, in bulk." is not at all clear. Are these data being sold off in bulk right now? This could indicate that related criminal activity is already underway. Does this mean that anyone who wishes can get access to lists of SINs and the other associated identity information about the owners? Canadians are truly in jeopardy of identity theft and fraud if this is the case.

One cannot draw exact parallels between the SIN and the U.S. Social Security Number (SSN). Unlike in the US, in Canada there are specific legislated purposes for which a SIN can be requested. In fact, some Americans complain that the SSN has come to be used as "a defacto ID number and the Social Security card is being used as a defacto ID card"[5].

Professor Cate's report tends to focus on the widespread use of SINs. It is true that anyone applying for one of a list of federal government services must provide their SINs to access those services but, under privacy legislation[6], citizens can refuse to provide SINs to any organization that is not entitled to use them. The HRSDC required that information from citizens applying for student loans, and citizens would trust that this agency would take appropriate steps to safeguard their personal information so it would not fall into the hands of criminals. In fact, there are Treasury Board guidelines on information management[7] with which federal agencies must comply in order to prevent this from happening (including the encryption of such files); HRSDC ignored these guidelines, thus enabling the theft of the contents of the portable memory device.

4. The financial risk from identity theft is borne almost entirely by financial institutions and other businesses; rarely do individuals suffer economic loss"

Here, Professor Cates is attempting to portray SIN identity theft as a victimless crime. This is not the case. From a 2008 survey of identity theft in Canada[8], after eliminating credit card fraud from the incidence rate and costs of identity theft and fraud (IDTF), the estimated annual number of IDTF victims in Canada was 700,000, who spent 12 million hours and more than $110 million dollars of their own money to resolve IDTF problems. This amounts to an average of 17 hours and out-of-pocket costs of $160 per victim, and does not include several hours that plaintiffs have already spent taking the steps recommended by the defendant in this case. To illustrate how such crimes can affect individuals, the following is an extreme example of Social Security Number theft in the United States:
"Social Insurance**:** Audra Schmierer's social insurance number has been used by at least 81 people across North America. The federal government took years to discover the number was being used illegally but took little action once it was discovered. Ms. Schmierer has had erroneous tax bills, has been denied jobs and has been detained because of felony arrest warrants that all belonged to other people that are using her social insurance number."[9]

---

[5] Jim Kouri, "Social Security Cards: De Facto National Identification', American Chronicle, Nov. 29, 2005.
[6] Office of the Privacy Commissioner of Canada "Social Insurance Number" http://www.priv.gc.ca/resource/ii_4_02_e.asp
[7] Treasury Board of Canada Secretariat "Guideline for Employees of the Government of Canada: Information Management (IM) Basics" http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16557
[8] Susan Sproule and Norm Archer, "Measuring Identity Theft in Canada: 2008 Consumer Survey", *McMaster eBusiness Research Centre (MeRC) Working Paper MeRC#23*, July 2008.
[9] Peter Prengaman "One Social Security Number, 81 People", AP/ February 11, 2009

Although statistics are not publicly available on the rate of SIN identity theft in Canada, the following are some examples of how SIN identity theft has affected Canadians, gleaned from status reports by the Auditor General of Canada. All are due to SINs and related identity information falling into the hands of criminals. These also illustrate the fact that the theft of the unencrypted database by HRSDC could create a crime bonanza, even if only a limited number of the missing SIN files were used for criminal purposes. Does anyone believe that the following cases did not cause a lot of problems for the actual owners of these SINs, some of whom may have been charged criminally as a result, and all of whom had to work hard to straighten out the resulting mess? This probably involved having to face hostile government agencies and bill collectors, perhaps even having to hire lawyers to defend their rights as honest citizens. And what about cases where the criminal use of a stolen SIN was never identified by the government agency where it was improperly used? SIN identity theft is definitely not a victimless crime.

"An individual was caught making false documents and using them to impersonate individuals. At the time of his arrest, he had in his possession various fraudulent cards, including SIN cards with various names. With the false documents, he had been able to change the victims' personal identification numbers for access to their lines of credit, credit card accounts, and chequing and savings accounts. Using similar methods, he succeeded in obtaining thousands of dollars from two victims' bank accounts."[10]

"An individual entered a major retail food company's warehouse and obtained a number of SINs from employees' time cards. These SINs were used to register 27 fictitious companies, which filed Goods and Services Tax (GST) net tax refund returns totalling approximately $254,000."[11]

"An individual used the SINs of six persons to register 22 fictitious companies and filed 133 GST returns declaring fictitious purchases in the amount of $680 million. He attempted to obtain GST refunds for an aggregate amount of $12,440,918."[11]

"An individual used phony help-wanted ads to obtain personal information about people, including SIN numbers, and then used this information to generate fictitious income tax returns for which Revenue Canada issued tax refunds. Using the SINs of 86 persons, the individual managed to fraudulently obtain $239,000."[11]

5. The individuals whose data were included on the missing hard drive are at no greater risk of identity theft as a result of the inability to locate the hard drive.

It has been established, after several thorough searches ("a full physical search of the building and a digital search of the email accounts of four workers")[12] that the portable drive in question could not be found at the HRSDC site. This is not a thumb drive that could be put in one's pocket and

[10] Status Report of the Auditor General of Canada. Exhibit 1.2—Crimes involving the Social Insurance Number, Sept. 2002

[11] Status Report of the Auditor General of Canada. Exhibit 16.8—Crimes involving the Social Insurance Number, Sept. 1998

[12] Jordan Press, "RCMP clears HRSDC workers of criminal wrongdoing in student loan data breach." **POSTMEDIA NEWS** August 8, 2013

forgotten or mislaid. The drive has been described as a Seagate Goflex 1 TB drive[13]. According to the manufacturer's specifications, its dimensions are 158 mm x 124 mm x 44 mm, and it weighs over a kilogram. Devices like this do not get up and walk away on their own. There were at least two investigations, first by Public Works and Government Services Canada (PWGSC) in January 2013[14], and secondly by the RCMP to determine whether an employee might have appropriated the drive in question. According to a report by PostMedia News[15], by August 2013 the RCMP had cleared all federal employees involved in the loss of the hard drive, and had no plans to launch a criminal investigation. HRSDC said that an internal investigation into the incident had not found that the hard drive was stolen. The PostMedia report also indicated that the drive had been stored in a locked filing cabinet.

The finding that the device was not stolen is not credible, because of the extensive searches that were directed at finding the missing drive. The only conclusion possible is that it was stolen, since it cannot be found at the HRSDC offices. The most important questions that result are a) By whom was it stolen? and b) Why was it stolen?

a) The RCMP was not called to investigate the case until two months after the drive was reported missing, and everyone involved had been interviewed by HRSDC and PWGSC security. The RCMP investigation therefore did not have an undisturbed crime scene or fresh witnesses to work with as a result of these delays. While having the greatest respect for the RCMP investigators and their decision not to launch an investigation, the drive could have been stolen by an HRSDC employee who would clearly have everything to lose (being fired and subjected to criminal prosecution) by admitting to the theft. The other possibility is theft by an outsider, but are outsiders allowed into the HRSDC offices and if they are, can they roam about freely without being accompanied by an HRSDC employee? And how could an outsider know about the drive and how would it be possible for a visitor to gain access to the locked filing cabinet? It therefore seems highly likely that the drive was stolen by an HRSDC employee or an accomplice.

b) There are a number of plausible motives for the theft of the drive. The first is that it was stolen for personal use as a drive for regular or backup purposes or for re-sale to an outsider. It is difficult to imagine that anyone, especially those with access to the drive and who knew what was on the drive, would risk being caught stealing a drive that is worth only approximately $100 CDN new (recent quote from Amazon.ca) from an HRSDC office. Surely an insider thief would recognize the uproar that would be caused by this major data breach, and the millions of taxpayer dollars spent by HRSDC in recovering from this event, in addition to the fallout from the loss of trust by those identified on the drive. The second possible motive is that the thief knew what was stored on the drive and wanted to either use that information for criminal purposes or to sell it to other criminals, realizing a substantial sum from the use or sale of the drive's contents. Since the data were not encrypted, this would not a technically difficult task. It therefore seems that the most plausible explanation, until it can be proved or disproved, is that the drive was stolen so the

[13] Tab 5 of Undertaking. "Description of the Hard Drive"
[14] PWGSC Memorandum to the Deputy Minister for Information. "Subject: Assistance With Investigation" February 15, 2013.
[15] Jordan Press, "RCMP clears HRSDC workers of criminal wrongdoing in student loan data breach." **POSTMEDIA NEWS** August 8, 2013

information it contained could be used for criminal purposes. This obviously places those identified on the drive at substantial risk of identity fraud.

6. Stolen personal data are usually exploited quickly, within "days" or "months," rather than "years," and the use of stolen data is likely to stop once the theft is made public. It therefore appears that any use of the data on the missing hard drive, assuming the drive had actually been stolen and the data accessed, would have already ended. The Government of Canada's offer of six years of fraud flags is therefore for a substantially longer period than the data suggest is necessary.

It is the case that, historically, the threats of identity theft from data breaches begin to subside soon after the breach occurs. Professor Cate has demonstrated this with a discussion in pages 8 to 12 of his report. He also points out that data breaches frequently do not lead to identity theft. For example, a shipment of data backup tapes is lost, or laptops that are stolen for the laptops themselves and not their contents.

It seems obvious that the HRSDC theft was an inside job, and it appears likely that the device was stolen by someone who knew what it contained. The thieves were likely to move quickly to take advantage of the stolen identity and other data before the theft was discovered and certain illegal activities on existing accounts were blocked. This may have happened in this case. However, HRSDC did not exactly move at flank speed to offer credit monitoring to those affected by the loss of the device. The loss of the device was determined on November 5, 2012 to have happened (the last known use of the device was apparently in late August 2012); the credit flagging arrangement was set up with Equifax in January 2013, and with TransUnion in May 2013[16]. Data have been provided by Equifax on the relative numbers of credit reports provided for those who agreed to the credit monitoring service, both before and after it was offered – in Q2 2013 versus Q2 2012[17]. However, we have not yet been provided by either Equifax or TransUnion with data for the intervals of greatest interest which are Q3 and Q4 of 2012, which include the time interval when the device was stolen. According to Professor Cate, these would be the intervals where the greatest activity with credit agencies would occur, if the theft occurred sometime between August and November of 2012. Data from these quarters should therefore be examined on a monthly basis in order to judge whether a spike in credit applications occurred during this interval, along with data from the corresponding months in 2013, to check for increased activity in those months as well, and to correct for seasonal variations.

But there are also data that represent the other types of identity fraud, for which credit monitoring is essentially useless, and no effort was made by HRSDC to determine how much of this fraud occurred after the discovery of the theft of the device. Since these would represent a variety of identity frauds, perhaps the best way to track them effectively would have been to invite victims to notify HRSDC when such events happened, so the events could be followed up and their actual causes determined. There was an opportunity to do this by advertising a willingness to receive calls from individuals whose identities appeared on the stolen drive, and who had actually been victimized by identity fraud. This could have been arranged when the call centres were established to handle calls about the loss of the drive itself and how those affected could protect themselves. However, this was not done, and the result was that only a "handful" of such calls were received[16]. The actual expected rate of

[16] Federal Court Proposed Class Proceeding Court File T-132-13. Cross Examination of Marc Lebrun, June 29,2013
[17] Tab 6 of Undertaking. Equifax "HRSDC Data Breach Monitoring Report" Report Quarters Q2 2013 & Q2 2012

such calls (at an estimated 0.3% per person per year[18]), even if there were no additional identity frauds due to the theft of the device, would be in excess of 140 each month. Assuming that only half of these were reported to HRSDC by concerned people affected by the data breach event, 70 per month is enough to represent more than a "handful". It appears that very few of these were reported and captured by the call centres; furthermore for some reason an analysis or listing of these few reports does not seem to be available. This represents another missed opportunity to determine whether identity data from the stolen drive were actually being used fraudulently.

7. While six years of fraud flag service is far beyond what is necessary to protect the individuals whose data is on the missing hard drive, additional services such as credit monitoring are unreasonable not only because of the absence of any credible threat and the fact that even if there were a credible threat that the SINs might be exploited, the available research data indicates that such a threat has already subsided, but also because credit monitoring would be no more effective in preventing identity theft and would likely be considerably more burdensome for individuals.

In his report, Section VI "How Effective is a Flag System in Preventing Identity Fraud and How Does That Compare with Credit Monitoring?" Professor Cate states "I can personally attest to the annoyance of credit monitoring. As a scholar in this area, I was offered free access to early credit monitoring services. After initially accepting, I rapidly cancelled the monitoring service because of the annoyance of daily "alerts." In the years since, although frequently offered credit monitoring when my data have been involved in a breach, I have consistently declined the service both to avoid the irritation of often meaningless warnings, and because the risk of identity theft did not warrant taking action, supporting the point that I made previously."

Professor Cate's statement supports a statement I made on this case in a previous report, that individuals covered by flags on their credit files have to put up with a great deal of inconvenience as a result, as follows: "2 (b) Whether or not the unencrypted database has fallen into the hands of criminals, flags on credit files will result in additional inconvenience to the persons participating in the credit alert program. Most of these individuals are at the beginning of their careers and will be making major purchases such as vehicles and homes over the next few years, with the majority of these purchases on credit. The firms asked to provide credit for major items such as these will almost invariably do credit checks and will find the credit flags. In order to safeguard their interests, these firms will then require additional meetings, identification, and references from the individuals applying for credit, resulting in further delays and frustration to the affected individuals." [19]

Respectfully submitted

Norman P. Archer
October 21, 2013

[18] Susan Sproule and Norm Archer, "Measuring Identity Theft in Canada: 2008 Consumer Survey", *McMaster eBusiness Research Centre (MeRC) Working Paper MeRC#23,* July 2008.

[19] Affidavit of Norman P. Archer, Exhibit B re "Canada Student Loans Case", July 23, 2013