Université d'Ottawa • University of Ottawa
Faculté de droit Faculty of Law

CIPPIC
Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

November 24, 2003

Mr. Richard Simpson
Director General
Electronic Commerce Branch
Industry Canada
300 Slater St. Room C2090
Ottawa Ontario K1A 0P8

Dear Mr. Simpson,

Re: Proposed *Regulations Amending the Regulations Specifying Investigative Bodies*, pursuant to para.26(1)(a.01) of the *Personal Information Protection and Electronic Documents Act*, *Canada Gazette*, Part I, Nov.8, 2003.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) provides the following comments on the proposed new regulations set out in the Gazette Notice referred to above.

Located at the University of Ottawa, Faculty of Law, CIPPIC represents consumer and other public interests in such areas as intellectual property, consumer protection in e-commerce, domain name governance, personal information protection and privacy. CIPPIC aims to fill voids in public policy debates, ensure balance in policy and law-making processes, and provide legal assistance to under-represented organizations and individuals on matters involving the intersection of law and technology. Upper-year law students work on clinic cases under the supervision of the Clinic Director.

We have reviewed the Gazette Notice, as well as some of the applications on which the proposed new regulations are based. We have a number of concerns with the proposed designations, as well as with the criteria and process applied to requests for "investigative body" status under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). These concerns are set out below, first with respect to the general criteria, and then with respect to a specific application.

CIPPIC's limited time and resources have allowed it to focus only on one of the many applications for investigative body status. Failure by CIPPIC to address other applications does not reflect any determination by CIPPIC of their appropriateness.

57, rue Louis-Pasteur 57 Louis Pasteur
Ottawa (Ontario) K1N 6N5 Canada Ottawa ON K1N 6N5 Canada

(613) 562-5794 ● Téléc. Fax (613) 562-5417

General Principles

The purpose of the PIPEDA is to provide individuals with privacy rights with respect to their personal information, while allowing organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. The core element of this legislation is the requirement for knowledge and consent on the part of the individual concerned to any collection, use or disclosure of her personal information in the course of commercial activities. Exceptions to this principle are specifically set out and limited to circumstances which a reasonable person would find appropriate. *It is essential that the core principles underlying the PIPEDA are not eroded by unnecessary and inappropriate exceptions created under the much less visible and rigorous regulation-making process.*

The "investigative body" regulation is particularly susceptible to abuse insofar as it could be used to legitimize unnecessarily privacy-invasive and prejudicial information sharing, without the individual's knowledge or consent. It is critical that Industry Canada carefully screen all applications for investigative body status, and allow only those that (a) are necessary for an investigative activity that is clearly in the public interest, (b) would be considered appropriate by a reasonable person, and (c) are designed in such a way as to minimally impair the privacy of data subjects.

General Comments

Interested parties need more time to review and comment on the proposed regulations

The proposed regulations are based on eight applications involving multiple organizations seeking investigative body status. Each application is substantial and complex. Interested members of the public cannot provide informed comment on such detailed and complicated proposals without a significant amount of lead time.

Moreover, the proposed amendments would significantly broaden exceptions to the fundamental requirement for knowledge and consent on which the PIPEDA is based. In other words, they go to the heart of the legislation; they are not mere regulatory "window-dressing". In this context, it is incumbent on the government to ensure not only that the regulatory process is fully transparent and open to public input, but also that the public have sufficient time and ability to review and understand the applications, assess them against the legislative principles, and provide informed comment on the proposals.

While the applications were posted weeks in advance of the Gazette publication, and many interested parties were informed of them, only 15 days were allowed for comment on the proposed regulations after publication in the Gazette. Given the complexity of issues and amount of material in question, CIPPIC was unable to review and comment on more than one of the applications. No doubt other interested parties found themselves similarly unable to provide informed comment on the full set of proposed designations. Much more time is needed, from the date of publishing the proposed new regulation, for

parties to provide informed comment.

Criteria for Investigative Body status should be more specific

A criterion is defined as "a standard on which a judgment or decision may be based".[1] Such standards are needed in order for Industry Canada to make reasoned and consistent decisions regarding applications for investigative body status. However, the so-called "criteria" published in the Canada Gazette do not set out standards on which judgements can be based; rather, they merely identify issues that need to be addressed in the assessment process. This point was raised during the first round of designations, but received only a passing response:

> One commentator suggested that the "considerations" for investigative bodies should be identified as strict criteria, that applicants should be required to demonstrate that they could not function without the exception and that a public interest test be added. The "considerations" listed in the RIAS are the "criteria" employed. The listed organizations made the case that they could not function without being specified in the Regulation and also that it was in the public interest that they be allowed to function as investigative bodies to combat fraud [emphasis added].[2]

With the point left unanswered, interested parties (applicants and others) are left to figure out what standards apply, by inference or guess. For example, the first consideration listed by Industry Canada is "the specific contraventions of law or breaches of agreements against which the investigative activities are directed". It could be inferred here: a) that there must be an investigative activity, and b) that the investigative activity must be tied to specific contraventions of law or breaches of agreements. However, this is not clear, and may not in fact be the standard applied by Industry Canada.

The last consideration listed by Industry Canada is "the amount of information provided to individuals about the existence and operation of the body….". It is unclear what standard applies here; in particular, it is unclear how much information an organization must provide, and how proactive the organization must be in providing such information, in order to qualify for investigative body status.

Leaving applicants and interested parties to infer standards from a list of considerations inevitably leads to differing understandings of the actual standards applied, and increases the likelihood that different government assessors will judge applications differently. This is not desirable. To the extent possible, Industry Canada should set out clear standards to which applicants can respond, and by which both the government and the public can accurately and soundly judge whether an application should be approved or rejected.

---

[1] Merriam-Webster online dictionary.
[2] *Canada Gazette Part II*, vol. 135 no. 1 (3 January 2001).

The criterion of "minimal privacy impairment" should be applied in all cases

One of the criteria applied to applications for investigative body status should be that of "minimal privacy impairment". In other words, any investigative body listed in the regulation should operate its information gathering and disclosing service in such a way as to impair individual privacy no more than necessary in order to achieve the goal of the service. This minimal impairment standard should be applied to all aspects of the proposed service.

Proportionality: the public interest in the investigative activity must outweigh the harm caused by associated privacy infringements

Once it is determined that the investigative activity in question serves the public interest, Industry Canada should assess the harm caused by the necessary privacy infringements (i.e., minimal privacy impairment) associated with that activity, and apply a "proportionality" test: is the investigative activity sufficiently important and desirable to justify the necessary associated privacy infringements? Does the public interest in permitting this investigative activity outweigh the harm caused by the associated privacy infringements?

Merely arguing that the organization will perish if it does not receive investigative body status is not in itself a *prima facie* case for designation. The PIPEDA creates certain obligations on the part of businesses, with a view to ending activities that infringe unduly on individuals' right to privacy. Implicit is the expectation that entities reliant on infringing activities might cease to exist – if they do not bring their activities in line with the legislation.

The *Regulations Specifying Investigative Bodies* were created not to serve as a lifeline for businesses that would perish without designation, but rather to ensure that certain privacy-invasive activities are permitted to continue where the public interest in their continuation outweighs the harm caused by the necessary associated privacy invasions. The onus on each applicant is to show that the public interest in favour of their designation outweighs the privacy invasions inherent in their operations.

Designations should apply only to that part of the organization that requires the exception, and only to those activities in question

The minimal impairment standard should be applied to, among other things, the scope of organizational designation made under the regulation. If the designated organization has many functions, and if the purpose of the designation is related to only one of those functions, individual privacy may be eroded more than necessary to meet the organization's needs. Industry Canada should, where possible, designate only that branch

of the organization which needs the designation. This way, the potential for unnecessary non-consensual use and disclosure or personal information will be appropriately limited. For example, instead of designating the entire OCSWSSW an investigative body, only the Complaints and Discipline Committees of this organization could receive the designation.

Designations should be for specific organizations, not open-ended categories

The proposed new regulations list specific organizations in most cases, but not in the case of insurance adjusters and private investigators. Instead, *any corporation or other body* licensed to engage in the business of providing insurance adjusters, private investigators, or detectives will automatically receive designation under subs.1(w) or (x) of the proposed regulation, as long as it has a compliant privacy code and is a member in good standing of a professional association such as the CIAA or the CPIO that has such a code. In other words, there will be no specific mention of the bodies to which the regulatory exemption applies.

Failure to publish specific organizational names seriously compromises the ability of public to determine which organizations may be receiving and disclosing personal information about them. Without such notice, individuals who wish to exercise their right to access personal information will have difficulty identifying the investigative bodies to which they should direct their requests. Furthermore, one of the stated purposes of the investigative body status designation was to facilitate oversight by the Privacy Commissioner. This oversight is far easier to implement if there is a list of the organizations which have status.

CIPPIC appreciates that naming specific organizations risks distorting competition in these industries by creating a temporary "membership monopoly" in favour of specifically named organizations. However, in our view, the public interest in naming specific organizations outweighs countervailing concerns. Individuals should be able to determine, by reference to the Regulations alone, whether a particular association constitutes an investigative body under the Regulations.

Compliance assessment of privacy codes should be conducted by government or an equally neutral and competent third party

Unnamed bodies representing licensed insurance adjusters and private investigators will receive designation under subs.1 (w) and (x) of the proposed regulation, as long as they and their professional associations have privacy codes "compliant with" the Canadian Standards Association Standard CAN/CSA-Q830-96, *Model Code for the Protection of Personal Information*. It is not clear, however, by whom or how this determination of compliance is made. If there is no neutral third party assessment of compliance, this requirement will have little meaning; the associations could simply self-declare, even where their codes do not measure up to CSA standards by any reasonable assessment. If

these sections of the regulation are to be adopted, there needs to be a more rigorous process for assessing compliance of privacy codes with the CSA Model Code. Since there are organizations in Canada who can audit compliance with CAN/CSA-Q830 and register the organization to the standard (e.g., the Quality Management Institute), this seems a reasonable market-based approach.

In our view, there should be a mechanism for routine audit of all organizations with investigative body status. Either the Privacy Commissioner should be provided with sufficient resources to perform routine audits, or organizations should be required to register to the CSA standard. Otherwise, consumer advocates will be forced to complain and demand audits, a situation that will likely occur only if egregious abuses are uncovered.

Teranet Services Inc. Application

Teranet Services Inc. ("TSI") has requested investigative body status for its proposed new data sharing service. This private service will be available to subscribers only. It will allow subscribers to share information on professionals in the real estate business. Teranet describes the service as follows:

> "The primary function of the Non-Public Service will be to aggregate and provide currently unavailable information associated with alleged fraud and material misrepresentation in the property market that is currently unavailable to Real Estate Data Exchange subscribers and may provide, upon request, other products and services to a subscriber investigating an incident. Subscribers to the Non-Public Service will use the information in the databases to determine and monitor the acceptability of business relationships with their professional service providers.
>
> TSI provides specialized services to facilitate investigations only to subscribers. The purpose of investigations is to assist in determining whether or not alleged fraud and misrepresentation has occurred. The Real Estate Data Exchange will maintain a central repository of investigation reports, associated facts or records accessible only by the investigating subscriber. This information combined with the Non-Public Service affords a subscriber access to information to be used in the prevention and prosecution of property related alleged fraud."[3]

There is no question that property related fraud, employment misrepresentation, identification fraud, equity misrepresentation and title fraud are serious offences worthy of attention by law enforcement. Clearly, there is a public interest in reducing the incidence of such fraud. However, the Teranet application raises equally serious privacy

[3] Teranet Application, p.4.

and due process concerns for database subjects of the proposed service. In CIPPIC's view, these concerns outweigh the public interest in favour of TSI's investigative body designation.

Moreover, while the service in question focuses on a narrow sector of the economy, where there may be good reason to improve the investigation of illegal activity, approval of TSI's application will set an important precedent for the approval of similar "negative database" services, possibly involving individual consumer information. There is a dangerous trend, after 9-11, of the private sector assuming the role of law enforcement, without accountability to the citizenry or to Parliament. At a very minimum, before approving this service, Industry Canada should think carefully about the precedent that it will set.

Law enforcement should be handled through public agencies and processes that incorporate fundamental rights of due process

Teranet is proposing a private, unregulated system of sharing information about alleged wrongdoing. An implied theory of the proposed service is that widespread economic shunning of those suspected of fraud will deter fraud in general. Yet, those who might be in the best position to help stop fraud, e.g., the police and professional associations, will apparently have to pay to gain access to the exchange. Whether or not it would be effective in reducing fraud, the proposed service would facilitate widespread sharing of highly prejudicial allegations about named individuals among an unlimited group of subscribers, without the data subject's knowledge and without the safeguards to which a regulated agency such as a credit bureau would be subject. This cannot be construed as a positive contribution to our public systems of justice and law enforcement. Allowing such unregulated and unrestricted sharing of personal data is inconsistent with the rule of law. Stability is achieved in society by citizens being subject to the same laws equally. There should be no interference with one's property, person or liberty without due process. Power should not be used arbitrarily. These principles are threatened if it is left to subscribers to trade unsubstantiated information on individuals and to judge who should or should not be punished.

Investigative purpose not established for disclosure by TSI to subscribers

Under subs. 7(3)(h.2) of the Act, investigative bodies may disclose personal information without consent only where "reasonable for purposes related to *investigating a breach of an agreement or a contravention of the laws of Canada or a province*". (emphasis added)

Yet, the proposed service involves automatic disclosures to subscribers, regardless of whether the subscriber is investigating a breach of an agreement or a contravention of law. Indeed, subscribers are expected to access the database in order to conduct "background checks" or "periodic reviews" on persons or companies with whom they are contemplating doing business. The purpose is not to investigate any suspected breach or

contravention, but rather to determine in advance whether a given individual or company has a record of alleged breach or contravention. Although it is noted that investigations will be undertaken as a specialized service, the primary function of the Non-Public Service is clearly the creation of a forum where alleged incidents of fraud can be reported by subscribers and in turn be viewed by other subscribers.[4]

Thus, the disclosure by TSI of personal information to subscribers is not for the purpose of investigating any breach or contravention by a data subject; rather, it is for the purpose of warning subscribers of alleged breaches or contraventions by specific data subjects.

No process for determining reasonableness of disclosures by TSI to subscribers

As noted above, subsection 7(3)(h.2) applies when TSI discloses information to subscribers via the REDx Non-Public Service. As the designated party, TSI will thus have to show that, in any given case, disclosure to a subscriber is *reasonable* for the purposes of an investigation of a breach of an agreement or a contravention of law.

Yet, because of the automatic nature of the service, there is no process for determining the reasonableness of disclosures to subscribers.[5] The reasonableness test simply cannot be met under the database model proposed by TSI.

Inadequate process for ensuring data accuracy

The proposed service raises serious concerns about the widespread sharing of inaccurate data.

All data is provided by subscribers. While the terms of service require that subscribers "take all reasonable steps to ensure that incident reports submitted to the Real Estate Data Exchange are accurate, timely and complete",[6] there is no method by which the accuracy of data is verified. TSI merely states that "information, when received, is then indexed and categorized either automatically at the time of submission or at the time of data entry."[7]

Indeed, TSI disowns responsibility for the accuracy of data, stating in clause III.1 of the Legal Terms and Conditions that:

> SUBSCRIBER ACKNOWLEDGES THAT TSI DOES NOT, AND

[4] *Teranet Submission*, at 4.
[5] It is a strained notion that the disclosure occurs between TSI and subscribers, not merely between subscribers searching and submitting to the database. However, for the purposes of this comment, a search hit on the exchange is equated to disclosure by TSI to the subscriber.
[6] Application, p.27.
[7] *Ibid*, at 9.

> COULD NOT FOR THE FEES CHARGED HEREUNDER, GUARANTEE OR WARRANT THE CORRECTNESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE INFORMATION PROVIDED THROUGH THE NON-PUBLIC SERVICES. SUBSCRIBER ACNOWLEDGES INFORMATION CONTAINED IN THE NON-PUBLIC SERVICE IS NOT THE PRODUCT OF AN INDEPENDENT VALIDATION OR INVESTIGATION BY TSI.[8]

Instead, subscribers are made solely responsible for the accuracy of data:

> Subscriber acknowledges and agrees that it is solely responsible for the content of an incident report submitted to TSI and shall use all reasonable care to ensure its accuracy, all in compliance with the Real Estate Data Exchange Policies and Procedures Guide. This includes an obligation to update an incident report on the part of the subscriber. An incident report directed to TSI with respect to an incident constitutes a representation and warranty by the Subscriber to TSI that, to the best of Subscriber's knowledge, the information in the incident report is true, accurate and complete.[9]

Yet, as noted above, the terms of service also *require* subscribers to submit reports, thus pressuring subscribers to submit information for the sake of maintaining their subscription. Subscribers are required to submit reports in order to maintain the value of the database. Subscribers with limited resources or cost-cutting pressures may thus submit information that has not been properly checked for accuracy.

The importance of ensuring accuracy of information in this highly sensitive database cannot be overstated. Yet, incident reports from TSI's proposed service are unverifiable and not guaranteed to be true or accurate.[10] Moreover, the service is designed in such a way as to encourage the submission of less-than-accurate data. The potential for highly prejudicial, inaccurate data to be shared among subscribers of this database is reason in and of itself to question the appropriateness of granting "investigative body" status to TSI.

No clear limitation on access to database

TSI states that:

> Potential subscribers to the Non-Public service include financial institutions, government agencies, professional regulatory bodies, mortgage brokerage companies and title insurance companies.[11]

---

[8] *Ibid*, at 21.
[9] *Ibid,* at 22.
[10] *Ibid*, at 21.
[11] *Ibid*, at 8.

This inclusive list places no limits on who else might become subscribers. Other categories of subscriber could presumably be added at a later date.

"Participants" in the REDx Non-Public include subscribers, their employees, professionals, database subjects and TSI's affiliates.[12] In this respect, we note that TSI's affiliates include ChoicePoint, a company that owns a similar data exchange in the U.S. Based in Atlanta, Georgia, ChoicePoint buys and sells personal information. Its clients include the FBI and 7,500 U.S. police departments. Its 30 plus contracts with the U.S. government bring in tens of millions of dollars.[13] ChoicePoint has apparently been the subject of prosecutions in Latin America in relation to its gathering of information on 300 million people on behalf of the U.S. government,[14] and has been strongly criticized by privacy advocates including the Washington-based Electronic Privacy Information Center.

With strategic partners such as ChoicePoint, TSI is not only in a position to benefit from the sharing of personal information across borders and for purposes beyond those understood as the purposes of this database, but will no doubt be pressured to do so. Indeed, with such cited purposes as to"compile and aggregate statistics" and to"communicate with its customers", it appears that TSI is attempting to leave the door open to uses and disclosures that may have little to do with the primary purpose of the database.

The application offers little protection against further uses and disclosures by TSI of the information gathered in the database. Without rigorous oversight mechanisms, the lack of restriction on who can access the proposed database, either professionally or geographically, could very well see Canadians' personal information being traded internationally for purposes other than which it was collected.

Inadequate accountability mechanisms

While TSI proposes to keep "audit trails" of all searches/reports and subscriber incident reports, accountability rests largely on individual subscribers.[15] It is subscribers who are made responsible for the accuracy of data, and for inappropriate reliance on incident reports. Subscribers are required to operate a "defined and credible arms length compliance department."[16] TSI, on the other hand, disclaims responsibility for inaccurate data and inappropriate uses of data by subscribers.

---

[12] *Ibid*, at 10.
[13] Jane Black, "Data Collectors Need Surveillance, Too." Jan. 24, 2002. http://netscape.businessweek.com/bwdaily/dnflash/jan2002/nf20020124_0582.htm
[14] "U.S. data mining riles Latin America" By HUGH DELLIOS, Chicago Tribune http://www.bayarea.com/mld/mercurynews/news/6997061.htm
[15] *Teranet Submission*, at 10.
[16] *Ibid*, at 8.

Lack of effective oversight

Industry Canada lists as one of the considerations in granting investigative body status:

> Whether there are specific legal regime, licensing requirement, regulation or oversight mechanisms to which [the applicant] is subjected and whether sanctions or penalties for non-compliance exist.[17]

Other than the general laws of Canada, general internal corporate reporting systems and oversight of employee practices, and the requirements placed on subscribers under the Terms of Service, TSI has identified no regulatory or oversight mechanism to ensure that this database is not abused. There appears to be no formal system for identifying subscriber breaches of the terms of service. The most severe sanction for such breach seems to be the cancellation of a subscriber's account.

Insufficient independence

TSI's service is totally dependent on its subscribers. The REDx Non-Public Service can not be separated from its subscribers since the exchange is dependant on subscriber use of TSI's investigative status for it to function.

Insufficient awareness by data subjects

Data subjects are likely to find out about their inclusion in the database only if their transactions are being refused, and their clients ask them why this is happening.

Access by database subjects to their personal information in the database

It seems TSI will only entertain applications for access to personal information in the database from database subjects who are licensed professionals – e.g., lawyers, realtors, appraisers, mortgage brokers or closing agents.[18] Yet, it is possible that subscribers submit information on an individual who is not a professional. Such database subjects would be denied access to their personal information under the TSI proposed service. This would of course be a clear violation of PIPEDA; if this is an instance of how well TSI has understood the law, we fail to see why Industry Canada would permit the organization to share information without the knowledge or consent of the data subject.

Method of inquiry

There seems to be only one means of striking an incident report from the exchange: the original submitter (subscriber) must request that their incident report be removed from the database. It would thus appear that data subjects cannot have their personal information removed other than on request by the entity that submitted it. This would be

[17] *Gazette Notice.*
[18] *Teranet Application*, 8-9.

another clear violation of PIPEDA, further tarnished by the fact that data subjects may never know about the information in the first place.[19]

Conclusion – Teranet Application

For all the reasons set out above, CIPPIC submits that the application for investigative body status by Teranet Services Inc. should be denied.

Summary of General Recommendations:

1. The criteria should be clear and specific.

2. The criteria for granting investigative body status should include minimal impairment of privacy rights, and a proportionality test.

3. Investigative Body status should be granted only to that part of the organization, and those activities, that require it.

4. All organizations granted Investigative Body status should be named.

5. All investigative bodies should be audited routinely for compliance with PIPEDA. Industry Canada should consider making certification to the CSA Standard mandatory for investigative bodies.

6. A common code for access rights by data subjects could be set out in regulations, and enforced with the above routine audit. Exceptions to the right of access and correction are limited and specific in the Act, and must not be circumvented by regulation.

7. Comment periods for this kind of substantive change to the Act should be much longer, given the complexity of the issues and the scarcity of players in the public voice in Canada.

Yours truly,

Original signed

Philippa Lawson
Executive Director
(613) 562-5800 x.2556
plawson@uottawa.ca

[19] *Ibid*, 12.