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

April 11, 2008

Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.,
Washington, D.C., USA
20580

Via Email

Dear Mr. Clark:

Subject: Behavioral Advertising, Moving the Discussion Forward to Possible Self-Regulatory Principles

The Canadian Internet Policy and Public Interest Clinic ("CIPPIC") is a legal clinic based at the University of Ottawa, Faculty of Law. CIPPIC's mandate is to provide a public interest voice in the policy-making process at the intersection of law and technology. We write to you today to offer our comments on the Federal Trade Commission's ("FTC") document, "Behavioral Advertising, Moving the Discussion Forward to Possible Self-Regulatory Principles" (the "Principles").[1]

CIPPIC has developed considerable expertise in privacy issues raised by technology. This expertise partially stems from the fact that we operate out of Canada, a jurisdiction with a well-developed privacy regulatory framework. This expertise, combined with the reality that any regulatory framework championed by the FTC will impact Canadians, provides the impetus for these comments.

COMMENTS

1. General Comments

a. Scope of Application of the Principles

The FTC has defined "behavioral advertising"[2], for the purposes of the Principles, as "the tracking of a consumer's activities online – including the searches the consumer has

[1] See the proposal: http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[2] Note that CIPPIC has used the Canadian spelling of "behaviour" in these comments when not referencing a specific quotation from the FTC documents (which utilize the American spelling of "behavior").

Université d'Ottawa • University of Ottawa
Faculté de droit • Faculty of Law
57 Louis-Pasteur, Ottawa (Ontario) K1N 6N5 Canada
(613) 562-5800 (2553) • (613) 562-5417 (Téléc/Fax)
www.cippic.ca • cippic@uottawa.ca

conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests." The FTC characterizes this definition as "broad" and indicates that the definition is meant to encompass various tracking activities engaged in by diverse companies across the online environment. CIPPIC commends the FTC for recognizing that consumer profiling and behavioural targeting is problematic in terms of privacy (even when the targeted individuals remain nameless). CIPPIC views the FTC's efforts as aligning the United States' privacy framework more closely with international and regional frameworks that recognize privacy as a human right.[3]

b. The Principles Should be Legislated (Not Voluntary)

The Principles should be legislated, not left to industry to adopt voluntarily. The Principles, as draft, reflect existing Canadian legislative obligations[4] – legislative obligations that we have had in place since 2001, and which have been uncontroversial for the most part. The Canadian (and European) experience demonstrates that industry can live with – indeed, protests of American industry notwithstanding, flourish under – a comprehensive privacy protection regime.[5]

It is clear, based on experience over the past two decades, that industry self-regulation cannot and will not deliver appropriate data protection in the marketplace. The combination of technological capacity and market incentives tends to push toward ever-increasing profiling and targeting of individuals. Only mandatory rules can effectively limit this growing threat to individual privacy.

In order to be effective and to gain the public trust, voluntary codes require genuine industry commitment as well as administrative and monitoring structures. Without these, they are no more than rhetoric, and indeed have the potential to mislead consumers and to slow the introduction of needed laws.

Voluntary codes also have the potential to create an "uneven playing field" for industry. Non-participating companies can enjoy a "free ride" on the positive image that a code helps create while not actually incurring the costs of conforming to the code. Companies that do conform to the code may not get credit for their good corporate citizenship if the

---

[3] See *Universal Declaration of Human Rights*, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948, Article 12, available at http://www.un.org/Overview/rights.html; the *International Covenant on Civil and Political Rights*, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976, Article 17, available at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

[4] The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") was approved by the federal Parliament in April 2000, and came into force January 1, 2001. Part I of PIPEDA deals with data protection, and applies to private sector organizations that collect, use or disclose personal information in the course of commercial activities, with the exception of provincially-regulated organizations in provinces that have enacted their own privacy legislation deemed to be "substantially similar" be the federal government. As of 2008, the provinces of Alberta, British Columbia and Quebec have all enacted "substantially similar" private sector privacy legislation.

[5] The first review of Part I of PIPEDA was undertaken by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), with hearings held between November 20, 2006 and February 22, 2007. The ETHI heard from 67 witnesses and considered 34 submissions from individual Canadians and Canadian organizations. While many suggestions for improvement were made, no submission called for the shelving of PIPEDA. See the STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA), Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics (May 2007), available at: http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?COM=10473&Lang=1&SourceId=204322.

public is not well-informed about the substance of the voluntary code or of the identities of its adherents.

c. The Principles Should be Fully Fleshed Out and Comprehensive (Not Vague)

CIPPIC urges the FTC to elaborate on its Principles to articulate more precisely the standards to which companies must adhere in order to make their tracking activities transparent, secure, consumer controlled, and no more intrusive than necessary. CIPPIC recommends that the FTC look to legislative privacy regimes for guidance in establishing Principles bolstered with more definitive language. While PIPEDA does a good job of providing a general structure, its general principles have been difficult interpret for enforcement purposes. CIPPIC accordingly recommends that the FTC look to subsequent provincial legislation in Canada, which has done a better job of defining and setting out legislative requirements, such as the criteria for valid consent.

Clarity at this junction is important. The Canadian law is based on a private sector Code that was developed by a multi-stakeholder committee of the Canadian Standards Association (CSA).[6] When it became obvious that voluntary self-regulation was not working, the government adopted the Code as the basis for a new law. While this approach had the benefit of ensuring industry support for the content of the new law, it has led to interpretive difficulties because of the vagueness of many provisions. We recommend that the FTC attempt to provide as much clarity now as to the application of each Principle, through such means as listing non-exhaustive examples after a statement of general principle.

Clarity and precision now will set the stage for more effective regulation in the future – had the CSA been drafted with such precision, PIPEDA would be a more effective statute today.

d. The Principles Should be Treated as Baseline Requirements, not Aspirational "Best Practices"

The Principles proposed by the FTC represent a positive effort to identify norms that govern behavioural advertising. CIPPIC urges the FTC to characterize these Principles as minimum protections, above which companies are encouraged to go. CIPPIC also strongly recommends building on those base protections now, while the opportunity to create solid privacy protection exists. The longer the wait to establish protections that citizens expect, the more difficult it will be to change business practices that do not meet those expectations.

e. The Principles Should Extend to Outsourcing

CIPPIC recommends that specific attention be paid to outsourcing in the Principles. Companies frequently retain third parties to provide services to the company in respect of

[6] A national standard: CAN/CSA-Q830-96.

the processing or use of consumer data on the company's behalf. Just as companies adhering to the Principles should be expected to meet minimum protection standards in their own operations, companies who outsource targeted marketing should remain responsible for external compliance with the both the Principles – regardless of whether or not the third party service provider voluntarily adheres to the Principles – and with specific promises the company has made to consumers with respect to its own collection, use, retention and disclosure of consumer data.

f. The Principles Should be Properly Enforced so as to Ensure Industry-Wide, Uniform Compliance

In Canada, PIPEDA's effectiveness is limited by the law's weak compliance mechanisms. Those mechanisms rest largely in the hands of Canada's federal Privacy Commissioner ("the Commissioner"). The Commissioner receives complaints, conducts investigations and issues non-binding findings on matters related to PIPEDA, along with recommendations as to private sector privacy practices. The Commissioner has broad investigatory powers, including the power to subpoena witnesses and compel testimony, to enter premises in order to obtain documents and to conduct interviews. The Commissioner is also charged with conducting periodic audits of private organizations to determine their compliance with PIPEDA. However, she has no power to order companies to comply with the legislation, and no powers to order remedies. Individual complainants must take their complaints to the Federal Court, an extremely costly endeavour, in order to obtain a binding decision and redress. PIPEDA's weak enforcement/compliance regime has seriously undermined its promise of substantial privacy protection. A rigorous study conducted by CIPPIC in 2006 confirms widespread non-compliance with PIPEDA by large as well as small businesses.[7]

Unless backed up with a meaningful enforcement regime, the FTC Principles will undoubtedly enjoy a worse compliance rate than PIPEDA. Based on Canada's experience, we conclude that consumers will not be well served by any voluntary code of behaviour no matter how well-drafted, unless strong inducements for compliance are put in place by the FTC. Legislated standards are required in order to ensure full participation, and rigorous enforcement of such standards is needed in order to ensure compliance.

2. Comments on Specific Proposed Principles

a. Principle 1: Transparency and Consumer Control

This Principle, as stated by the FTC, reads:

> Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing

---

[7] CIPPIC, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (May 2006), available at http://www.cippic.ca/uploads/May1-06/PIPEDAComplianceReport.pdf.

> advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.

While we support this Principle, we are concerned that the "opt-out" consent to behavioural advertising provides insufficient protection to consumers. Research in psychology and economics shows that opt-out consent mechanisms take advantage of consumer tendencies to trust businesses, and suggests that opt-out consent protocols will always result in a large number of cases in which consent is wrongly assumed.[8] The only effective way to ensure that consumer preferences for data protection are respected is to require opt-in consent.

As the FTC has recognized in these draft Principles, opt-in consent should be required for "sensitive data". While certain kinds of data should always be treated as sensitive (see below), any personal data can be sensitive depending on the context. For this reason, opt-in consent mechanisms are always preferred to opt-out.

Opt-in consent would also make the marketplace more efficient by providing consumers with a greater opportunity for meaningful participation. Behavioural marketing is largely "invisible" to consumers. This form of advertising is often justified as the basis for the value proposition supporting the provision of free web services, such as social networking applications. Such justifications assume that the "proposition" is being put to and accepted by consumers. That is seldom the case, with unfortunate consequences for individual privacy. An opt-in requirement would ensure that consumers would receive such propositions, and have the opportunity to weigh their merits.

Should the FTC Principles retain "opt-out" consent, it is essential that notice of the consent being assumed is clearly and prominently brought to the attention of the consumer, in a manner that cannot be ignored and that unequivocally communicates the nature of the activities for which consent is being assumed. For "choice" to be truly informed, consumers must know (1) what information is being collected, (2) how this information is being used or will be used in the future, (3) how long it will be retained, and (4) to whom it will be disclosed. The FTC Principle does not go far enough to require effective notice. CIPPIC therefore recommends that the Principle be amended to require that the "prominent statement" provided to consumers include these features. CIPPIC also recommends that the notice include a brief explanation of the specific "targeting" purposes for which the information is being collected ("tailored advertising" is not clear enough, and may be misleading) so that consumers can make informed choices.

We recommend that the FTC work with consumer and privacy groups to develop standardized notice forms for this purpose.

---

[8] See, *e.g.*, Ian Kerr et al., "Soft Surveillance, Hard Consent," *Personally Yours* 6 (2006):1-14; Eric Johnson, Steven Bellman and Gerald Lohse, "Defaults, Framing and Privacy: Why Opting in ≠ Opting Out," *Marketing Letters* 13(1) (2002): 5-15.

b. Principle 2: Reasonable Security and Limited Data Retention

This Principle breaks down into two sub-Principles: security and retention. We recommend that the FTC similarly articulate these obligations as distinct Principles.

(i) Reasonable Security

The proposed FTC Principle reads:

> Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with the data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company.

This Principle aligns with 4.7 (Safeguards) of PIPEDA, which imposes duties upon companies who collect, retain, and use personal information. When companies begin to collect personal information, the cost of the breach is shifted to the consumers (as they stand to lose from improper use of the information), so companies should be prepared to handle that information in the most secure way possible.

CIPPIC recommends that the FTC articulate what is meant by "reasonable" security measures by providing specific examples, to the extent possible given the evolving nature of technology. Such examples could be updated by the FTC periodically in order to take into account evolving technology.

(ii) Limited Data Retention

The proposed FTC Principle reads:

> Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.

The problem with this standard is that businesses can always find a "legitimate business need"; consumer information will always be "valuable" to a company. Respectfully, consumers deserve greater respect than that afforded by this retention standard. CIPPIC recommends that the FTC adopt the specific standard set out in PIPEDA, Schedule 1, Principle 4.5.3: personal information that is no longer required to fulfill the identified purpose for which it was originally collected or subsequently agreed to by the consumer via an opt-in process must be destroyed (with certain exceptions for longer retention when the information could be required by law enforcement).

c. Principle 3: Affirmative Express Consent for Material Changes to Existing Privacy Promises

The FTC Principle reads:

> Before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

CIPPIC strongly supports this Principle, particularly if the requirements of Principle 1 are strengthened to provide for a stronger form of notice (*i.e.*, documented notice that addresses collection, use, retention and disclosure of consumer information). A company should have to communicate and obtain consent from the consumer to any new use or disclosure, or to a change in its retention policy, before undertaking that new dealing. To require otherwise would permit the company to unilaterally change the terms of a bargain without the knowledge or consent of the other party to that bargain.

d. Principle 4: Affirmative Express Consent To (or Prohibition Against) Using Sensitive Data for Behavioural Advertising

The FTC Principle reads:

> Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising. FTC staff seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioral targeting should not be permitted, rather than subject to consumer choice.

This Principle raises three issues: (1) in what circumstances should companies be required to obtain express (as opposed to implied) consent to the collection and use of consumer data? (2) if only "sensitive" data triggers an express consent requirement, then what constitutes "sensitive data"? and (3) should companies be prohibited from using sensitive data?

Collection, retention, use, and disclosure of personal information for secondary marketing purposes, whether it is considered "sensitive" or not, should require express consent. This is because all personal information can, depending on the context and the individual, be sensitive.

With respect to the definition of sensitive information, CIPPIC recommends that any information which identifies a person or discloses fundamental characteristics about them should be considered "sensitive." Similarly, information is "sensitive" when it is capable of being correlated with an individual. Correlation with an individual can be achieved by, among other data relationships, association with a name, a phone number, home

address, work place, or a non-public computer. Additionally, information can be correlated with an individual even if it cannot be associated with a particular name or physical location if the profile is large enough and of sufficient detail.

Specifically, sensitive information is information about personal characteristics (not preferences) which cannot be determined simply by observing an individual when s/he carries out an activity in a public space. The types of information that automatically falls into this category are:

- Financial information (credit cards, bank account numbers, debit cards, insurance policies, investment portfolio)
- Government records (government identifying numbers, applications for government programs, government documents, criminal history)
- Educational background (educational institution, specific qualifications or traits, does not include level of achievement or level of education)
- Medical information (medical conditions, use of prescription or non-prescription drugs, medical characteristics, history of treatment, visits to particular web-sites, biometric information)
- Religious information (religious affiliation, donation history)
- Information in respect of sexual matters (including gender and sexual preference)
- Information regarding family members (names of family members, family structure, including participation in family therapy, counseling and other family service programs)
- Employment history (work history, employment locations, nature of employment)
- Political affiliation (voting history, party membership)

With respect to prohibitions, CIPPIC recognizes the consumer's freedom to bargain away these types of "sensitive" information, with informed consent, in return for free or customized services that incorporate behavioural marketing. This may be appropriate in some circumstances, but in other circumstances, such as the collection and use of children's data, such a bargain is inappropriate.

Based upon the lack of capacity to contract independently, it is reasonable to classify all information relating to individuals under the age of 14 as sensitive, and behavioural target marketing at minors should be prohibited.[9]

e. Call For Additional Information: Using Tracking Data for Purposes Other than Behavioural Advertising

The FTC ends its notice with the following request for comment:

---

[9] If one creates a site targeted at minors but does not ask them their ages that should not be seen as permitting target marketing to that population.

> FTC staff seeks additional information about the potential uses of tracking data beyond behavioral advertising and, in particular: (1) which secondary uses raise concerns, (2) whether companies are in fact using data for these secondary purposes, (3) whether the concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data, and (4) whether secondary uses, if they occur, merit some form of heightened protection.

Consumer privacy concerns are not limited to behavioural advertising. While we applaud the FTC for this initiative, we cannot help but question whether these efforts would be better directed towards a regulatory framework of general application, rather than a "silo" approach focusing on behavioural advertising. The value consumers place in privacy that justifies these regulatory mechanisms surely justifies a broader approach.

(i) Which secondary uses raise concerns?

The potential for secondary use of consumer data gathered for behavioural profiling is enormous. CIPPIC takes issue with any secondary use that lacks adequate consumer consent. Indeed, this is the standard under PIPEDA and most other privacy regulatory frameworks: the law requires notice and consent to all collection and use of personal information, including secondary uses.

Particular uses that raise concerns are those associated with price and service discrimination. In addition, secondary uses of data in decision making that has implications for the particular consumer – such as service offerings (*e.g.*, insurance) – also raise concerns.

(ii) Are companies in fact using data for these secondary purposes?

While CIPPIC has not investigated secondary use directly, plainly, companies either *are* or *could be* using data for secondary purposes: wherever such use offers a competitive advantage, such use will occur. In any event, there is a need for greater information on these issues, and the FTC should consider playing a leading role in filling that need.

(iii) Are concerns about secondary uses limited to the use of personally identifiable data or also extend to non-personally identifiable data?

CIPPIC's concerns extend to any circumstances in which decisions are being made about the consumer that can affect the consumer and are not necessarily related to personal identification of that consumer. Much "anonymous" data, such as demographic data, can be used in a manner that can affect the consumer.

(iv) Do secondary uses merit some form of heightened protection?

In our view, effective notice and opt-in consent to all uses of data collected through behavioural advertising mechanisms would obviate the need for "heightened" protection.

In any case, because they are not expected by individuals, secondary uses of personal data should, in appropriate cases, require a stronger form of consent, such as an opt-in requirement. Similarly, if the secondary use affects the consumer, robust consent may be required. Information that was not sensitive in one situation may be sensitive in another. For example, gender is not sensitive information in certain circumstances, but is in other circumstances. The robustness of the consent required should reflect the situation.

Summary

CIPPIC offers the following general comments on the FTC's approach in proposing Principles:

- CIPPIC commends the FTC on the scope of application of the Principles.
- CIPPIC contends that the Principles should be legislated, not left to industry to adopt voluntarily. The experiences of the past two decades have demonstrated that industry self-regulation cannot and will not deliver consumers appropriate data protection.
- CIPPIC recommends that the FTC elaborate the Principles to articulate more precisely the standards to which companies must adhere in order to make their tracking activities transparent, secure, consumer controlled, and no more intrusive than necessary.
- CIPPIC supports the Principles as baseline requirements, above which companies are encouraged to go.
- Canada's experience suggests that without enforcement mechanisms, the Principles will not enjoy widespread compliance. CIPPIC recommends that the FTC investigate putting in place inducements for compliance.
- CIPPIC support the extension of the Principles to outsourced services.
- CIPPIC supports a regulatory framework of general application for privacy protection.

CIPPIC offers the following comments with respect to specific Principles:

Principle 1

- CIPPIC strongly supports the requirement for companies to obtain affirmative express consent from the consumer before engaging in targeted behavioural advertising.
- CIPPIC recommends an "opt-in" consent requirement for data collection, use, retention and disclosure for data collected for behavioural targeting.
- Should the Principles retain a requirement for "opt-out" consent, CIPPIC recommends that the FTC work with consumer and privacy groups to develop clear and standardized notice for "opt-out" be provided to the consumer.

Principle 2

- CIPPIC recommends that "reasonable security" and "limited data retention" be treated as distinct principles and tightened in their explanation (through examples or specific instructions) so as to offer the marketplace clear guidance.

Principle 3

- CIPPIC supports this Principle's requirement for a company to communicate and obtain consent from the consumer to any new use or disclosure, or a change in its retention policy.

Principle 4

- CIPPIC argues that any information which identifies a person or discloses fundamental characteristics about them should be considered "sensitive."
- CIPPIC argues that behavioural target marketing at minors should be prohibited.

With respect to the FTC's call for additional information in respect of the use of tracking data for purposes other than behavioural advertising, CIPPIC offers the following comments:

- CIPPIC argues that secondary use, like primary use, should be based on principles of notice and consent.
- CIPPIC observes that effective notice and opt-in consent to all uses of data collected through behavioural advertising mechanisms would obviate the need for "heightened" protection for secondary use.

* * *

We trust you will find these comments helpful to your deliberations. We thank you for having presented us with the opportunity to address this important issue.

Yours truly,

David Fewer
Staff Lawyer
CIPPIC

Jocelyn Cleary
Articling Student
CIPPIC

for Philippa Lawson
Director
CIPPIC

for Tom Jarmyn
CIPPIC Volunteer