Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko

Tamir Israel, Staff Lawyer
(613) 562-5800 ext. 2914
tisrael@cippic.ca

**April 4, 2011**

***VIA EMAIL***

**Jane Hamilton**
**Daniele Chatelois**
Electronic Commerce Branch
Industry Canada
300 Slater Street
Ottawa, ON, K1A 0C8
Jane.Hamilton@ic.gc.ca
Daniele.Chatelois@ic.gc.ca

Dear Ms. Hamilton and Ms. Chatelois,

**Re: OECD Privacy Guidelines Review Questionnaire**
**CIPPIC Response to Industry Canada Stakeholder Comments**

**The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is pleased to offer its responses to the OECD Privacy Guidelines 30th Anniversary Review Questionnaire.**

**We have enclosed below our responses to this questionnaire and are grateful for to Industry Canada, e-Commerce Branch for providing us with the opportunity to do so.**

**If you have any questions for concerns, please do not hesitate to contact me.**

**Best regards,**

**Tamir Israel**
**Staff Counsel, CIPPIC**

# QUESTIONNAIRE FOR REVIEWING THE OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

## Introduction

This questionnaire has been prepared in support of a review of the Privacy Guidelines. The review arises out of the *Seoul Declaration for the Future of the Internet Economy*, which was adopted by Ministers in June 2008. The Seoul Declaration calls for the OECD to assess the application of certain instruments, including the Privacy Guidelines, in light of "changing technologies, markets and user behaviour and the growing importance of digital identities."[1] The OECD Working Party on Information Security and Privacy (WPISP) discussed the process for conducting this review at its meeting on 2-3 December 2010, and with the subsequent assistance of its Privacy Volunteer Group, has prepared the questionnaire as the first step in its review.

The questionnaire has been structured in five short sections. Each section includes a text box indicating which provisions of the Privacy Guidelines are addressed in that section (the Guidelines are reproduced in their entirety as Annex A). The text box is followed by 2 or 3 questions drafted in an open-ended style to allow delegates flexibility in their responses. The first section of the questionnaire is focused on the objectives of the Guidelines; the second on the strategy reflected in the Guidelines; and sections 3-5 on different dimensions of the underlying policy principles.

The "Main Points" section from the WPISP report on "The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines" has been reproduced as Annex B.[2] This section has been included for the convenience of those who may be interested in key findings from WPISP privacy work over the last year as they prepare their responses to the questionnaire. However, you are encouraged to refer to a wider range of resources in preparing your response. For example, privacy frameworks are under review in a number of OECD countries and other international organisations, aspects of which may help inform the review the OECD Guidelines. You may also want to refer to the Explanatory Memorandum prepared by the expert group that developed the OECD Privacy Guidelines.[3]

Responses to the questionnaire are requested by 28 March 2011 and should be sent to: (Insert public folder link).

---

1 See, http://www.oecd.org/dataoecd/49/28/40839436.pdf.

2 The complete report is not yet available for broad distribution but will be finalized in the coming months at which time we will provide you with information on how it can be accessed.

3 See, http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html#memorandum

# Section 1: The Objectives (the Vision)

**Relevant Provisions of the Privacy Guidelines**

**RECOGNISING** that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

**RECOGNISING** that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

**RECOGNISING** that transborder flows of personal data contribute to economic and social development;

**RECOGNISING** that domestic legislation concerning privacy protection and trans-border flows of personal data may hinder such transborder flows;

**DETERMINED** to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

**Questions**

1. Do the objectives of the Privacy Guidelines, as reflected in the provisions in the box above, continue to be relevant and comprehensive?

2. If not, how should they be adapted or what new ones should be added in light of the mission of the OECD?

**CIPPIC Response**:

The vision underpinning the Guidelines is still relevant. In particular, CIPPIC recognizes that the need to balance, where they compete, the need to facilitate free information flows with privacy and liberties and this balance is well line with the OECD's mission.

However, in the decades since the initial adoption of the Guidelines, it has become evident that over-emphasis on free information flows, particularly when invoked in a commercial context or by government agents, is far more likely to impact detrimentally on privacy than vice versa.

In addition, there is now a robust and global discourse that has defined the parameters of informational privacy concepts and principles. In CIPPIC's view, the 'vision' underpinning the Guidelines should make it clear that reduction of obstacles to transborder data flows should be achieved, to the extent possible, by the adoption of consistent, but robust protections for privacy and liberties across all member states.

As such, CIPPIC would prefer to see an articulation of the vision underlying the Guidelines that expressly does not prioritize free information or transborder data flows over the need to preserve privacy and other civil liberties.

# Section 2: The Strategy

**Relevant Provisions of the Privacy Guidelines**

**RECOMMENDS**:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

**PART FOUR. NATIONAL IMPLEMENTATION**

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;

b) encourage and support self regulation, whether in the form of codes of conduct or otherwise;

c) provide for reasonable means for individuals to exercise their rights;

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

e) ensure that there is no unfair discrimination against data subjects.

**PART FIVE. INTERNATIONAL CO-OPERATION**

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:
i) information exchange related to these Guidelines, and
ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

**Questions:**

3. Is the strategy of the Guidelines, as reflected in the provisions in the box above, well adapted to implementing what you think Canada's objectives for the Guidelines should be, given the current context for privacy?

4. If not, what objectives are not well addressed by these provisions?

5. Are there other strategic approaches that might better address these objectives?

**CIPPIC Response:**
With respect to recommendation 2, CIPPIC reiterates its view that the removal of obstacles to transborder data flows should now be achieved primarily through the adoption of strong and comparable levels of protection for privacy and civil liberties. The Guidelines should not be seen as endorsing weakening of protections in order to facilitate information flows to lowest denominator member states. They should, instead, operate to raise the level of privacy protection while achieving consistency across disparate member states. CIPPIC would welcome a reformulation of recommendation 2 that mirrors this.

With respect to the National Implementation component of the OECD strategy, CIPPIC believes self-regulation has not proven to be an effective strategy for dealing with privacy concerns. In addition, 19(b) conflicts with 19(d), which calls on member states to impose appropriate sanctions and remedies for those who fail to comply with the Guidelines. While industry codes may certainly have a role in the development of privacy protections, the co-regulatory solutions should be a minimum requirement for national Guideline compliance strategies.

With respect to Part Five, International Cooperation, CIPPIC points again to the global discourse that has developed surrounding privacy norms in the decades since the Guidelines were first adopted. In light of this discourse, CIPPIC no longer sees a need to require simplicity in national implementations of the Guidelines, nor a need to cater to lowest denominator member states.

## Section 3: The Policy – Definitions and Scope

**Relevant Provisions of the Privacy Guidelines**

**PART ONE. GENERAL**

**Definitions**

1. For the purposes of these Guidelines:

   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

   b) "personal data" means any information relating to an identified or identifiable individual (data subject);

   c) "transborder flows of personal data" means movements of personal data across national borders.

**Scope of Guidelines**

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

a) as few as possible, and

b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

**Questions:**

6. In your view, are the definitions and scope of the Guidelines, as reflected in the provisions in the box above, well-adapted to the current context for privacy?

7. If not, what issues are not well addressed by these provisions?

8. Are there other policy approaches that might better address these issues or is there a need for additional definitions?

**CIPPIC Response:**

The definitions currently included are sufficiently broad so as to capture activities that may detrimentally impact of privacy. However, CIPPIC notes that some national implementations of the Guidelines have failed to adopt the broad net that the Guidelines intended to capture. Specifically, some member states have adopted working definitions of personal data that do not capture situations where a readily identifiable individual is directly involved. This definition should be clarified to ensure such situations are included. In addition, the Guidelines should apply to *all* personal data and the exclusion in section 2 above should be removed or incorporated into 3(a) which already permits different treatment based on the nature of the information in question and the context in which it is being processed.

With respect to 3(a), differences in data protection premised on the nature and context of the data should follow the PIPEDA model and include an account of the sensitivity of the data and the reasonable expectations of individuals.

CIPPIC notes the Guidelines intend to include within their scope both public and private sector data processes. CIPPIC notes that it is important to emphasize that the same principles apply in the public sector as in the private and limitations on collection, use, disclosure and retention should be implemented as an integral component of any national strategy.

In addition, and perhaps most vitally, in CIPPIC's experience 4 has enjoyed weak implementation in national strategies this has posed a serious threat to the protection of privacy and civil liberties. This section should be strengthened. Suggested language:

> Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:
>
> a) as few as possible;
> b) expressly justified by demonstrable, empirically supported, and legitimate needs; and
> c) made known to the public.

# Section 4: The Policy – Basic Principles of National Application

**Relevant Provisions of the Privacy Guidelines**

**PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION**

**Collection Limitation Principle**

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

**Data Quality Principle**

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

**Purpose Specification Principle**

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

**Use Limitation Principle**

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
a) with the consent of the data subject; or
b) by the authority of law.

**Security Safeguards Principle**

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

**Openness Principle**

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

**Individual Participation Principle**

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

**Accountability Principle**

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

## Questions:

9. Do you think that the basic policy principles, as reflected in the box above, are appropriate to the current context for privacy?

10. If not, what issues are not well addressed by these principles?

11. Are there other approaches or new or revised principles that might better address these issues?

**CIPPIC Response:**
In recent privacy discourse there has been a proliferation of calls for new privacy-based 'rights'. With the exception of the right to anonymity, CIPPIC is of the view that the itemized privacy 'rights' that have appeared in recent discussions can be addressed through strengthening of the general Guideline principles as articulated below. We additionally refer to a 'right of refusal/opposition' and a 'right of oblivion' below, but within the context of broader assessments of the substantive principles already in the Guidelines as opposed to as standalone rights.

### 1. *Right to Anonymity:*

CIPPIC believes a right to anonymity must be expressly included within the OECD Guidelines if they are to remain relevant in an online context. The freedom to speak and act anonymously is integral, in CIPPIC's view, to maintaining any form of privacy in a public space and as the Internet (soon to be 'of things') inserts greater swaths of our once-private lives into public and semi-public spaces, the right to remain anonymous will become increasingly necessary to any continued attempts to maintain individual control of personal information.

At the same time, individuals are under greater pressure from numerous sources to identify themselves in contexts where it is not necessary to do so. Perhaps the most currently prevalent example of this is in a social networking context, where the social network wishes to encourage 'real identities' and takes active steps to prevent anonymous or pseudonymous use of the services being offered.[4] In CIPPIC's view, existing Guidelines limitations on collection do not offer adequate protection to online anonymity.

CIPPIC notes that Schedule 3 of Australia's *Privacy Act*, which currently applies only to the private sector but is in the process of being expanded in application to the public sector as well, includes an 'Anonymity Principle'.

Any such Principle should follow federated identity principles, should prevent entities from requiring identification where it is not necessary for a particular transaction, prevent entities from collecting *greater* identification than necessary for a particular transaction, and enshrining the right of individuals to act and speak pseudonymously. It should, as with all of the Guidelines, apply to both the public and the private sector equally.

### 2. *Problems with Consent:*

The OECD Guidelines are effectively consent-based. The collection limitation principle expressly refers to knowledge and consent, as does the use limitation principle, while initial use and disclosure are premised on purposes which have been specified to the individual further to 9. Further, it is clear that a number of member states have implemented the Guidelines in a consent-centric manner and others are moving in that direction.

The many shortcomings of the consent paradigm have become evident in the decades since the Guidelines were first put in place. While consent remains central to any informational privacy strategy, it is essential that a.) it be explicitly recognized that consent amounts to more than notice;[5]

---

[4] See CIPPIC, Comments on OPC Draft Report on 2010 Consultations on Evolving Technologies, December 20, 2010, <http://www.cippic.ca/uploads/20101220-CIPPIC-Comments-OPCDRAFTREPORT.pdf>, generally, but specifically section III.

[5] See S. Barocas & H. Nissenbaum, "On Notice: The Trouble with Notice and Consent", *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, October 2009, <http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf>.

and b.) that varying levels and forms of consent are necessary for different information types/contexts;[6] and c.) consent is not in and of itself sufficient to addressing all informational privacy harms.[7]

Our comments below on consent are aimed at updating the OECD Guidelines so as to account for these shortcomings.

**Reasonableness**:
The inherent limitations of a pure consent-based privacy model, including insurmountable information imbalances, psychological barriers, and a tendency to import contract law-like notice specifications with 'consent' demand that an overarching 'reasonableness' limitation be placed on any collection, use or disclosure of personal information.

PIPEDA's section 5(3) can serve as a model for the inclusion of an overarching reasonableness requirement of this nature.

**Right of Refusal**:
A right of refusal or opposition should be incorporated for any collection, use or disclosure of personal information that is not strictly necessary for the purpose of a customer-initiated transaction. The inclusion of such a right is integral to any realistic consent-based privacy protection model in order to avoid tied-selling/consent to secondary purposes such as commercial uses.

**Limitation and Proportionality**:
The current limitation on collection specified in 7 is not sufficient. Collection should be expressly limited to collection that is necessary and proportional to a purpose that has been consented to. Further, knowledge and consent should be a minimal requirement, regardless of whether it is 'appropriate'.

One issue that has become critical since the initial adoption of the Guidelines is the problem of retroactive changes to privacy practices. This is currently addressed in 9 & 10, but in adequately so. First, as with 7, a 'not necessary for' standard should be adopted in place of the current 'not incompatible with those [specified] purposes' standard.

Second, the exception in 10 (b) that permits collection without consent "by the authority of law" must be clarified. It has been interpreted to mean 'where not prevented by law' but should instead very clearly refer to "where required by law".

---

6 See also L. Church & A. Whitten, "Generative Usability: Security and User Centered Design beyond the Appliance", *NSPW '09*, <http://www.nspw.org/papers/2009/nspw2009-church.pdf>; L. Brandimarte, A. Acquisti, & G. Loewenstein, "Misplaced Confidence: Privacy and the Control Paradox", *WEIS 2010*, <http://weis2010.econinfosec.org/papers/session2/weis2010_brandimarte.pdf>; and I. Kerr, J. Barrigar, J. Burkell, & K. Black, "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent", in I. Kerr, V. Steeves, & C. Lucock, Eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford: Oxford University Press, 2009), <http://idtrail.org/content/view/799>.

7 See L.M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA", (2006) 56 *UTLJ* 181.

**Fundamental Retroactive Shifts in Privacy:**
This in and of itself remains insufficient, however, to meeting a new breed of *ex post* privacy 'changes', where such changes are of such a scope as to fundamentally change the privacy practices of the site in question.

EU Commissioner Viviane Reding described one such set of fundamental changes as "astonishing", noting that "[a]ll of a sudden there is a complete change of policy…"[8] While it may be important to permit websites and services to make such retroactive fundamental changes, it is also important to recognize that fundamental shifts of this nature strongly implicate all the shortcomings of the consent-based paradigm. While users are provided with notice, they are often given little time and limited information to assess the implications of such a fundamental shift. Further, as existing users are often invested in the site or service, the choice whether to adopt the newly offered privacy landscape will not always be 'genuine'. More robust requirements must be put in place to account for 'fundamental retroactive shifts' in privacy policies.

Such changes must include a right of refusal, robust notice requirements, and specified minimal time limits to permit individuals to assess the scope of the changes.

**Form of Consent:**
The form or mechanism by which consent is currently sought must be strengthened. There is ample social science evidence demonstrating the impact on 'consent' that setting viscosity (the degree to which a given privacy setting is 'resistant to change') and presentation have significant impact on individual choices. These UI design features are becoming rapidly more central to ensuring genuine consent in an online world.

PIPEDA includes provisions that govern the form by which consent is sought. Sensitivity of the affected information and the reasonable expectations of individuals whose consent is sought are both central to assessing what form of consent would be required in any given setting. A similar requirement should be incorporated into the Guidelines wherever notice or consent are relied upon as a mechanism for legitimating collection, use or disclosure of personal data.

**Accountability in Consent:**
In addition, where consent is relied upon to justify the collection, use or disclosure of personal data, it is paramount to ensure data controllers are accountable for gaining effective consent. CIPPIC points to a recent proposed amendment to PIPEDA as central to achieving this level of accountability:

> "the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting."[9]

---

8 M. Newman, "Facebook's Privacy Changes Being Watched by European Commission", Business Week, February 5, 2010, <http://www.businessweek.com/news/2010-02-05/facebook-s-privacy-changes-being-watched-by-european-commission.html>). See also: I. Kerr, "The Devil is in the Defaults", May 29, 2010, Ottawa Citizen – Citizen Special, <http://www.iankerr.ca/>

9 Bill C-29, the *Safeguarding Canadians' Personal Information Act*, 3rd Session, 40th Parliament, 59 Elizabeth II, 2010.

**Privacy by Default:**
Where users are provided with a choice that will impact on their privacy as a basis of consent, the principle of 'privacy by default' should be an express requirement. That is, the default choice should be private and users should be required to take a positive step to indicate their acquiescence to the non-privacy friendly option.

This reflects the assumption, inherent in the Guidelines, that it is the user is in control of her personal information and that data controlling entities are responsible for ensuring individuals have consented to intended collection, use and disclosure of their personal information.

**Right to Oblivion:**
While limitation on retention where the purpose for which information has been collected expires is arguable envisioned within existing principles, many national implementations have seen fit to expressly articulate limitations of this nature and CIPPIC supports including such clarity in the Guidelines.

Such a limitation should be applied to the public and private sectors equally.

### 3. *Security Safeguards*

The security safeguards principle is increasingly becoming a central important component of any effective privacy protection strategy.

It should be expressly clarified within this provision that the adoption and use of technical safeguards is envisioned as within its scope. In addition, consideration should be given to expressly stating a preference for encryption in communications, where possible.

### 4. *Accountability*

The Accountability principle remains at the core of the Guidelines. It should not, however, be used as a mechanism to abrogate the importance of other principles.

## Section 5: The Policy – Basic Principles of International Application

**Relevant Provisions of the Privacy Guidelines**

**PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS**

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

**Questions:**

12. Are the policy principles reflected in the provisions in the box above well-adapted to the current international context for privacy?

13. If not, what issues are not being well addressed by these provisions?

14. Are there other approaches or new or revised principles that might better address these issues?

**CIPPIC Response**

It remains necessary for the Guidelines to be principles of international application. CIPPIC reiterates its view, stated above, that reduction of barriers to transborder data flows should be achieved primarily by encouraging comparable levels of privacy protection, in both the public and private sector, and that this should not involve a 'lowest common denominator' approach.

In addition, CIPPIC believes that the OECD and the Guidelines may be the most appropriate venue for resolving issues of data sovereignty although ultimate resolution of such issues will require multi-stakeholder processes and may be outside the scope of this questionnaire.