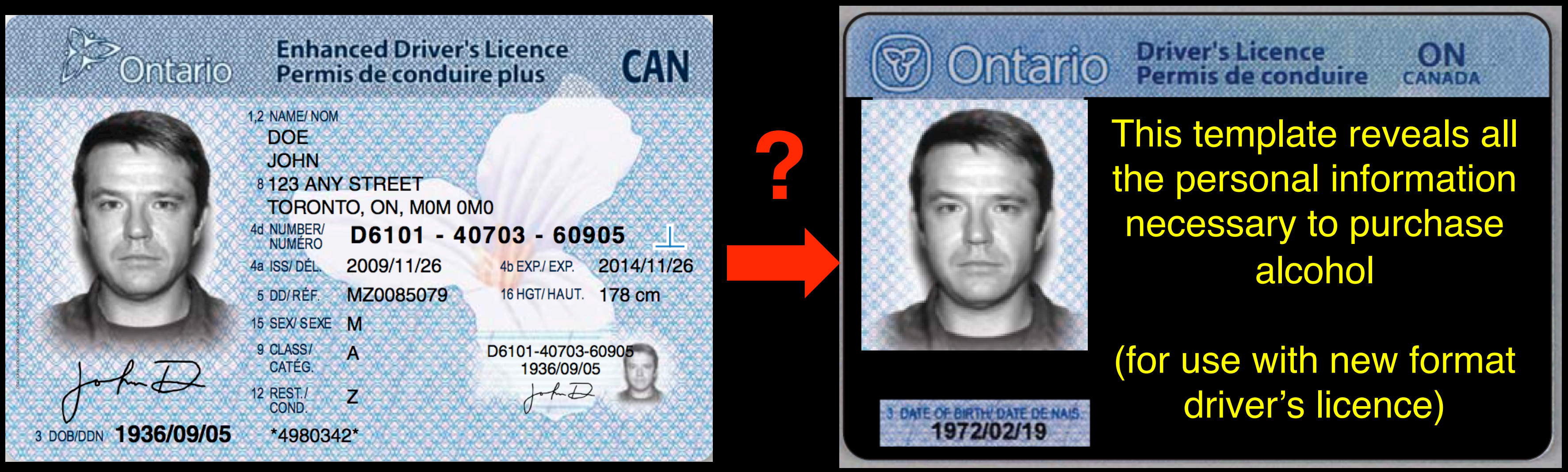
Toward secure and privacy sensitive ID/authentication?



Ontario

Enhanced Driver's Licence
Permis de conduire plus

CAN

1,2 NAME/ NOM
DOE
JOHN

8 123 ANY STREET
TORONTO, ON, M0M 0M0

4d NUMBER/ NUMÉRO D6101 - 40703 - 60905

4a ISS/ DÉL. 2009/11/26

4b EXP./ EXP. 2014/11/26

5 DD/ RÉF. MZ0085079

16 HGT/ HAUT. 178 cm

15 SEX/ SEXE M

9 CLASS/ CATÉG. A

12 REST./ COND. Z

D6101-40703-60905
1936/09/05

3 DOB/DDN 1936/09/05

4980342

Ontario

Driver's Licence
Permis de conduire

ON
CANADA

3 DATE OF BIRTH/ DATE DE NAIS.
1972/02/19

This template reveals all the personal information necessary to purchase alcohol

(for use with new format driver's licence)

IPSI Public Lecture #1 – Fall 2009

September 28, 2009

Andrew Clement[1,2,3],
with Alison Benjamin,[1,3] Krista Boa,[1] Joseph Ferenbok,[1,2,3]
Dave Kemp,[1,3] Brenda McPhail,[1] Karen Smith[1,3] & Alex Tichine[2]

[1]Information Policy Research Program, [2]Identity, Privacy and Security Institute &
[3]Knowledge Media Design Institute
University of Toronto

Overview

- Introduction to IPSI and
  Identity, Privacy and Security
- Update on Ontario’s Enhanced Driver’s Licence (EDL)
- Lessons for identity card/scheme design
- Understanding IDentity as performance
- Toward user-centric, privacy sensitive ID/ authentication

Introducing IPSI

the Identity Privacy and Security Institute

IPSI aims to carry out a pioneering, interdisciplinary program of research, education, outreach, and industry collaboration, combining technological and policy perspectives. Supported by U of T's Academic Initiatives Fund (AIF).

Management Committee:

Dimitrios Hatzinakos (Chair)

Professor, Dept of Electrical and Computer Engineering (ECE)

Andrew Clement

Professor Faculty of Information

Kostas Plataniotis

Associate Professor, Dept of Electrical and Computer Engineering (ECE)

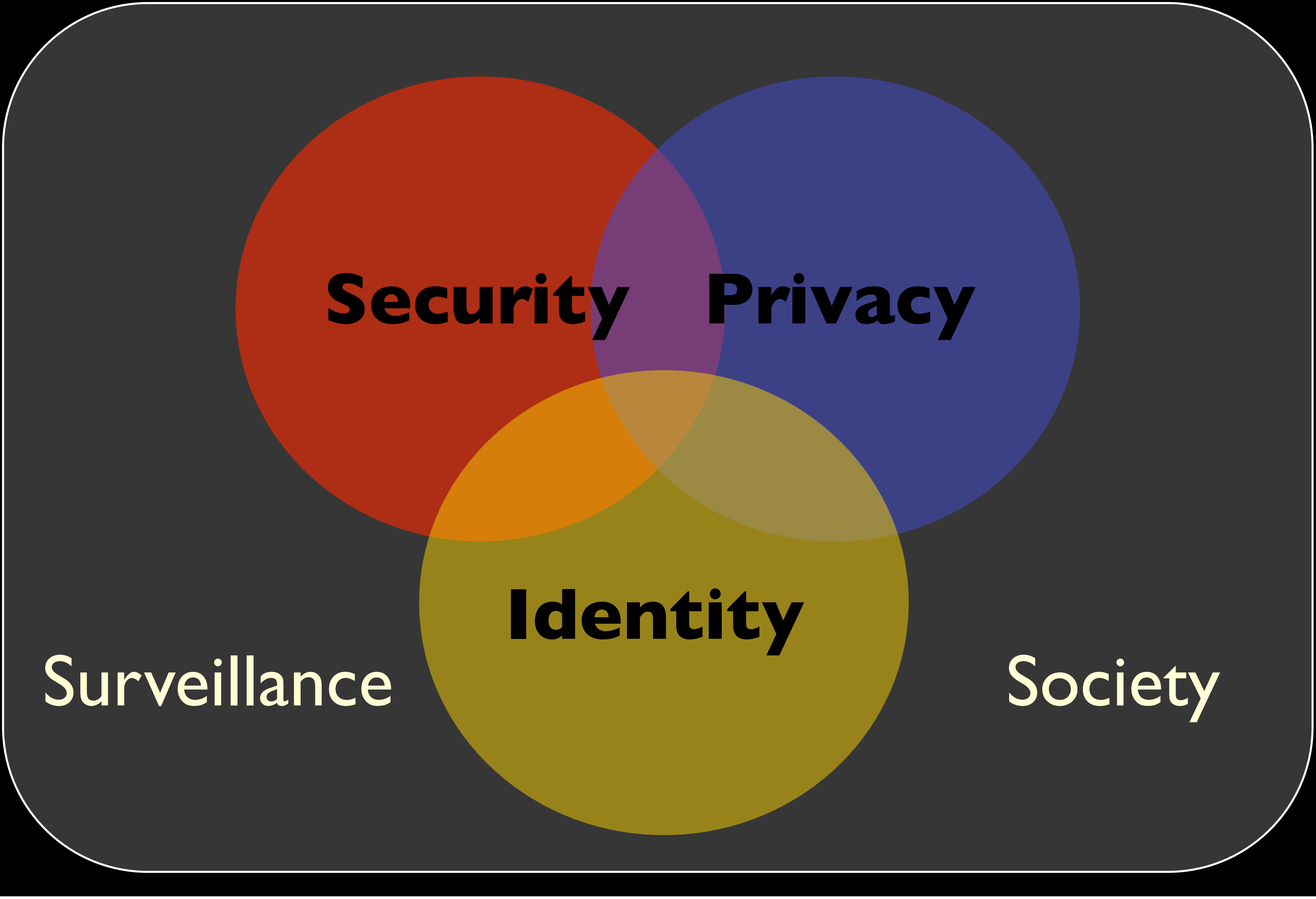
Introducing IPSI

Activities

- Public lectures series
- Graduate course and specialization
  - JIE1001 Seminar in Identity, Privacy & Identity
- Other events
  - Public Information Forums
  - Colloquia
  - Conference presentations (e.g. IEEE TIC STH)
- Research round tables (Spring)
- Research Day (May)

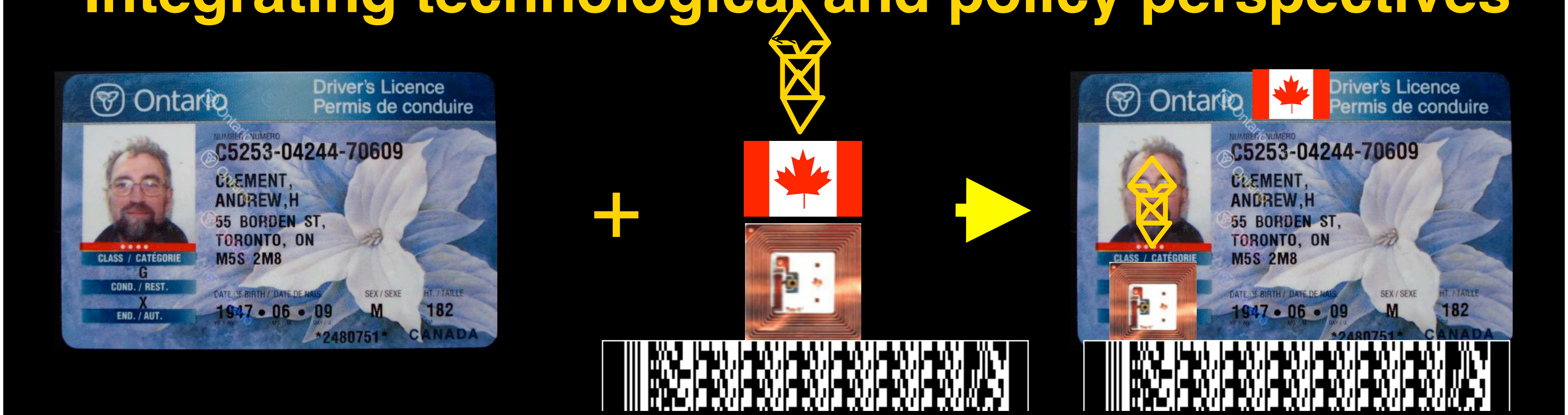
Identity, Privacy & Security

in a Surveillance Society



Designing Ontario's enhanced drivers licence (EDL) for privacy and security:

Integrating technological and policy perspectives



Andrew Clement

Identity, Privacy and Security Initiative &
Information Policy Research Program
Faculty of Information
University of Toronto

IPSI Public Lecture

University of Toronto
Sept. 22, 2008

Summary - EDLs are a bad idea

Stop!
Think again

Stop!
Think again

Still
preferable

Four-part test	FRT	RFID	Passport
Necessary	✗	✗	✓
Effective	?	✗	✓
Proportionate	✗	✗	✓
Minimal	✗	✗	✓

Public Participation in Development process

- What part will the public, civil society organizations and independent experts play in the development of this ID scheme?
  - Timetable
  - Social impact assessments
  - Venues and modes of involvement
    - Legislative review
    - Concept and prototype design
    - Field trials
- What on-going accountability and oversight mechanisms?

Timeline – Bill 85 – Photo Card Act

Jun 3-10, 2008 – 1st & 2nd Reading

Jul 16 - Public Information Forum on the EDL

Oct 20 – Legislative hearings

Nov 27 – Royal Assent

Mar 24, 2009 National Public Forum on the EDL (Ottawa)

Jun 1 – WHTI comes into effect, first cards issued

Jun – slow uptake of EDLs see: http://IDforum.ca

ServiceOntario

making it easier

✓ Convenient

✓ Affordable

✓ Secure

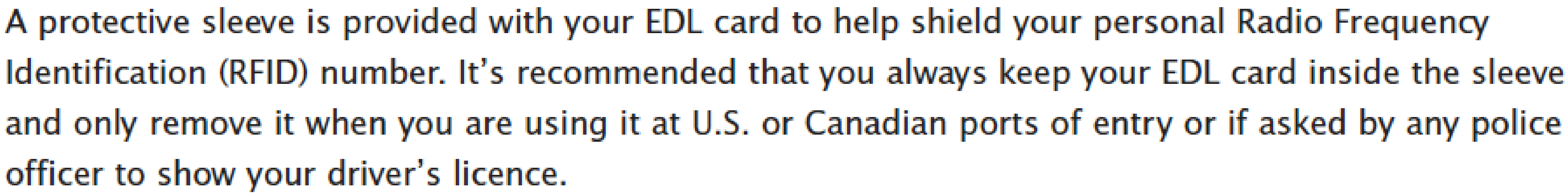
Introducing the NEW

Ontario Enhanced Driver's Licence

Outstanding issues

wit
you
It’s

- Unique RFID tag number – personal info?
  - EDL Applicants Guide: “The chip … contains a unique identification number only and does not contain any personal information” p.4
  - IP Commissioner: “**WRONG**” *Privacy by Design*, p. 209
- Protecting the RFID tag number?



A protective sleeve is provided with your EDL card to help shield your personal Radio Frequency Identification (RFID) number. It’s recommended that you always keep your EDL card inside the sleeve and only remove it when you are using it at U.S. or Canadian ports of entry or if asked by any police officer to show your driver’s licence.

- Creation of a large, biometric, on-line data base for facial recognition
  - Effectiveness? Redress? Scope creep? Oversight?

Outstanding issues

- Lack of public information and consultation
  - Bare minimum of public info, Legislative hearings ill-informed and *pro forma*, No feedback on regulations consultation,
- Access to Information requests
  - Professional handling – timely, courteous, efficient,…
  - Many (excessive?) redactions of key info

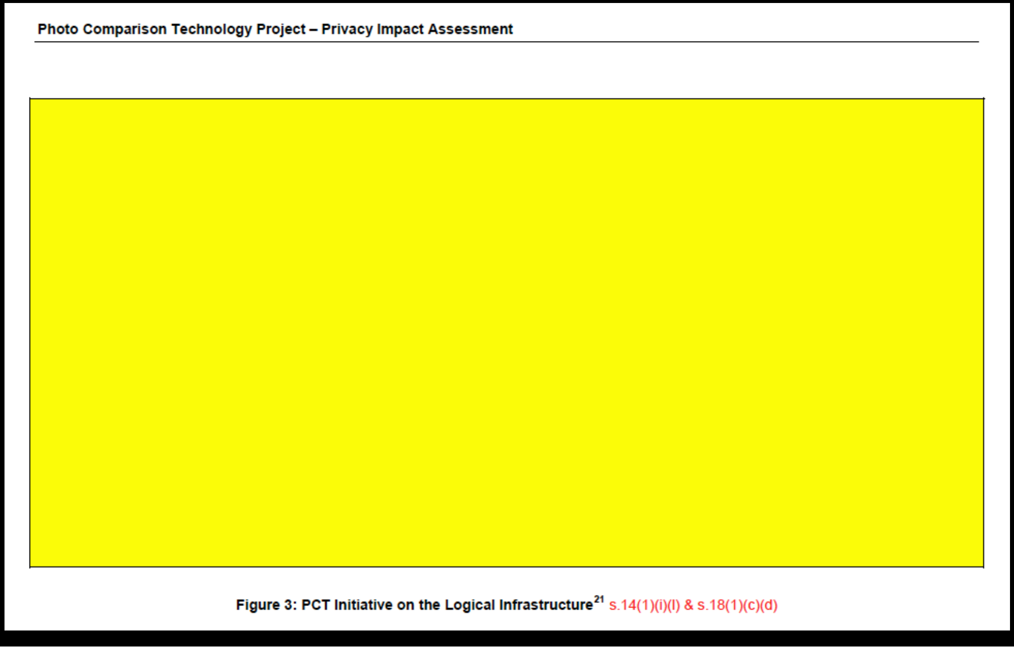


Photo Comparison Technology Project – Privacy Impact Assessment

[redacted]

Figure 3: PCT Initiative on the Logical Infrastructure[21] s.14(1)(i)(l) & s.18(1)(c)(d)

EDL is “botched,” but …

EDLs are flawed as:

- Policy
- Technology
- Governance process

But, Ontario is not alone. Since 9/11, there has been a surge of jurisdictional ID schemes. Most show similar characteristics of:

- Privacy threat, but no good evidence of security gain
- Lack of public disclosure and discussion
- Against much expert and industry advice
- High costs + cost overruns
- Implementation delays

Lessons for ID governance

- Governments can prevail with mis-guided schemes in the absence of strong opposition
  - *Need a civil society capacity for ID politics*

Lessons for ID research & development

- Privacy alone is not an adequate frame
- Mis-match between organization/system and subject perspectives on ID:

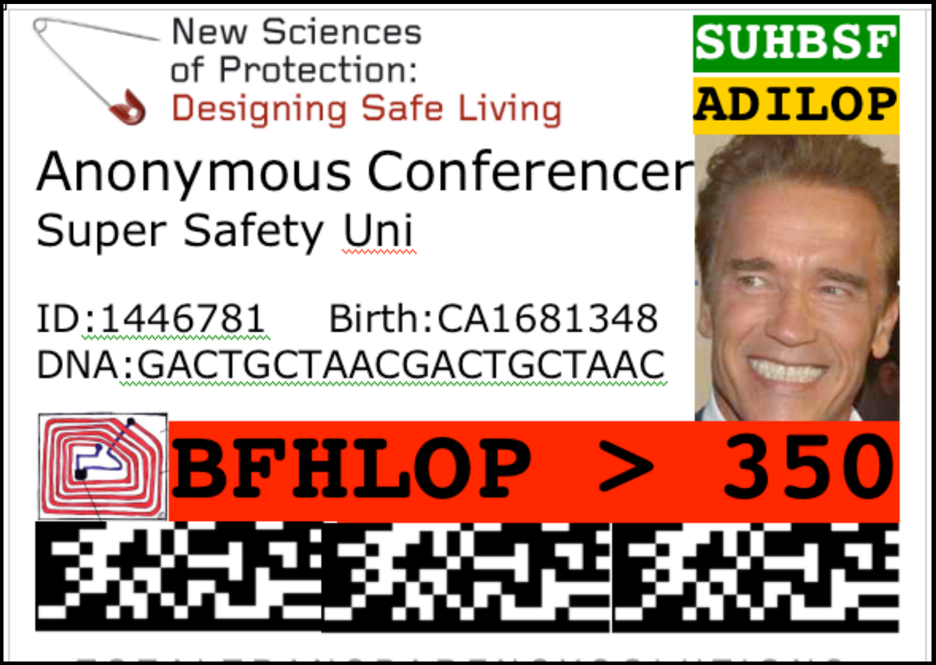
  Organization: "Are you in our databases?"

  i.e. first identify yourself, then we may authorize.

  Person: "Recognize my entitlement. Here is my credential."
- ID subject experiences are ignored

  Need citizen-centric ID technology and policy research and development

Counter design - Mock ID cards



New Sciences
of Protection:
Designing Safe Living

SUHBSF

ADILOP

Anonymous Conferencer
Super Safety Uni

ID:1446781 Birth:CA1681348
DNA:GACTGCTAACGACTGCTAAC

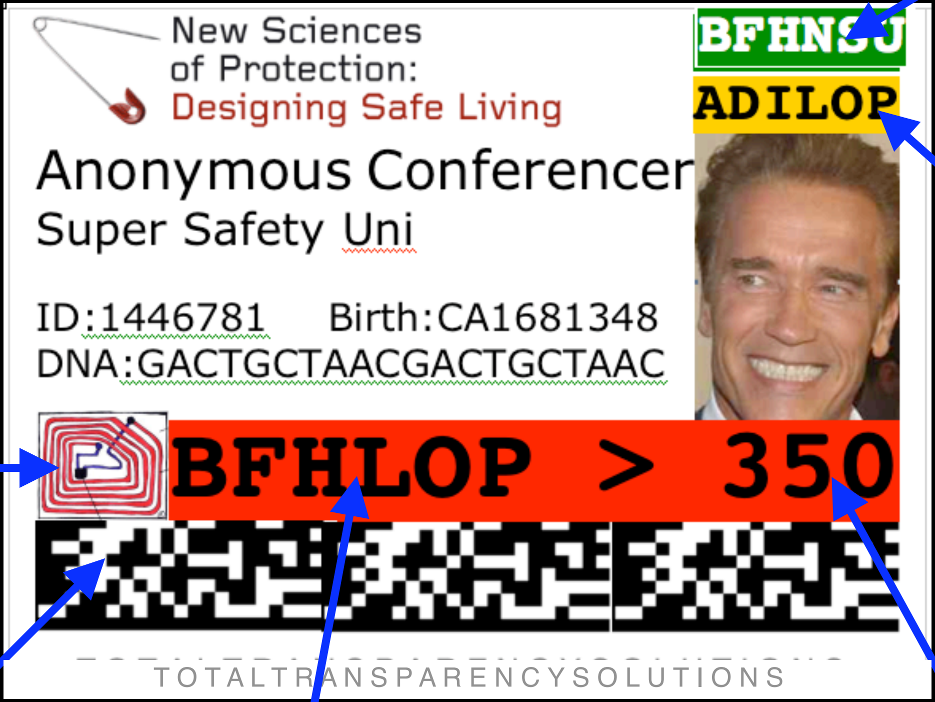
BFHLOP > 350

See: TotalTransparencySolutions.pbworks.com

Prototype of SafeTBioID^{TM} ID card

High Public risk attendee

Biometric samples provided:
B=Blood F=Feces
H=Hair N=Finger Nail S=Saliva
U=Urine



New Sciences of Protection:
Designing Safe Living

BFHNSU

ADILOP

Anonymous Conferencer
Super Safety Uni

ID:1446781 Birth:CA1681348
DNA:GACTGCTAACGACTGCTAAC

BFHLOP > 350

TOTALTRANSPARENCYSOLUTIONS

RFID tag with full personal data for remote wireless reading

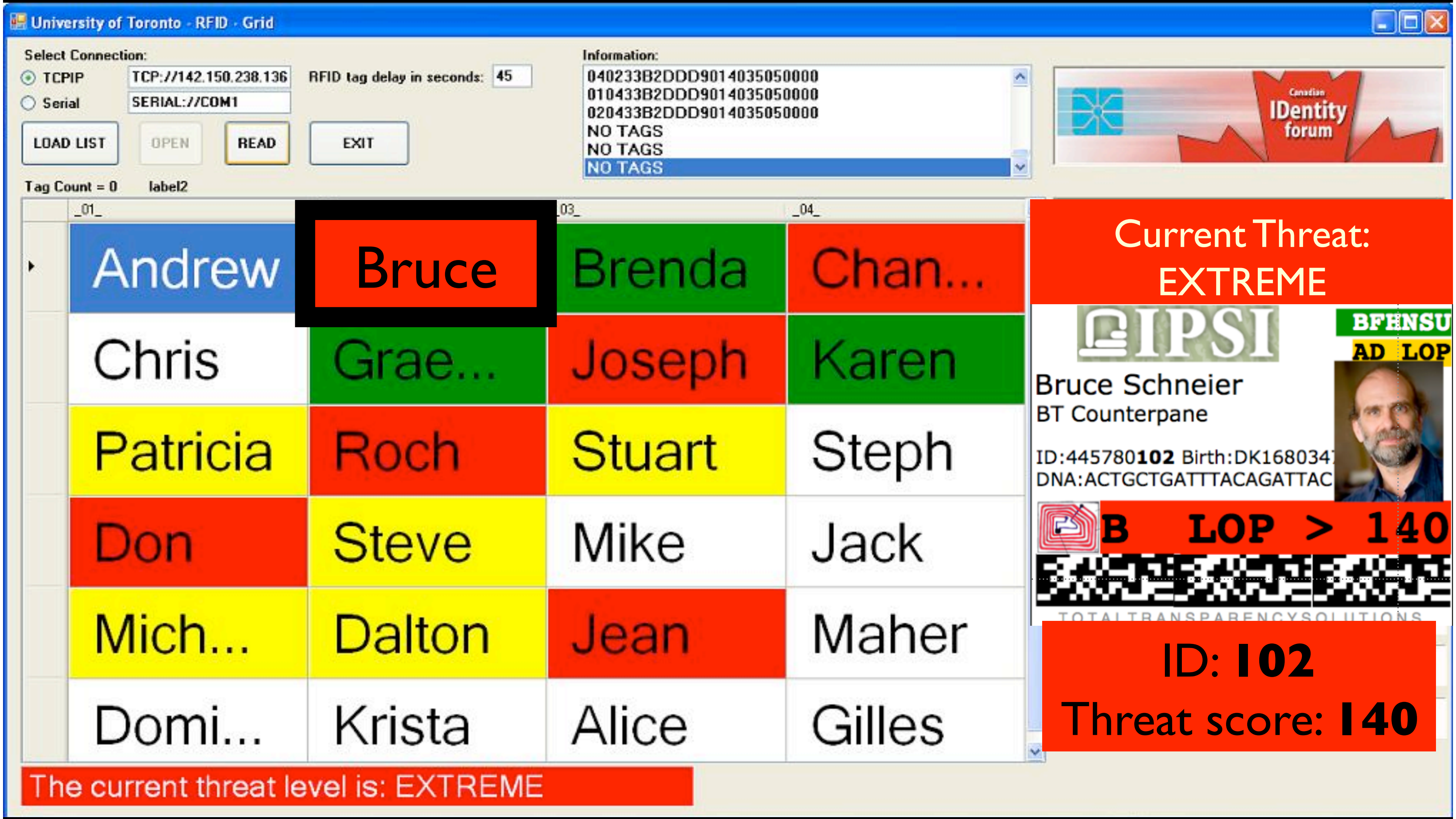
2D barcode with full personal data for remote optical reading

Public risk factors
B=Anti-Social Behaviour
F=Flatulence
H=Hijacking
L=Lung Cancer
O=Overweight
P=Pregnancy

Personal risk factors
A=Athletes Foot
D=Internet Obsessive Disorder
I=Insomnia
L=Lung Cancer
O=Overweight
P=Pregnancy

Public risk score:
0-99=Safe
100-199=**Caution**
200-350=**Watch out!**
350-499=Lock up now

Ironic agitprop RFID demo



University of Toronto - RFID - Grid

Select Connection:

● TCPIP TCP://142.150.238.136

○ Serial SERIAL://COM1

RFID tag delay in seconds: 45

Information:

```
040233B2DDD9014035050000
010433B2DDD9014035050000
020433B2DDD9014035050000
NO TAGS
NO TAGS
NO TAGS
```

Tag Count = 0 label2

_01_		_03_	_04_
Andrew	Bruce	Brenda	Chan...
Chris	Grae...	Joseph	Karen
Patricia	Roch	Stuart	Steph
Don	Steve	Mike	Jack
Mich...	Dalton	Jean	Maher
Domi...	Krista	Alice	Gilles

The current threat level is: EXTREME

Current Threat: EXTREME

Bruce Schneier
BT Counterpane

ID:445780102 Birth:DK168034
DNA:ACTGCTGATTTACAGATTAC

B LOP > 140

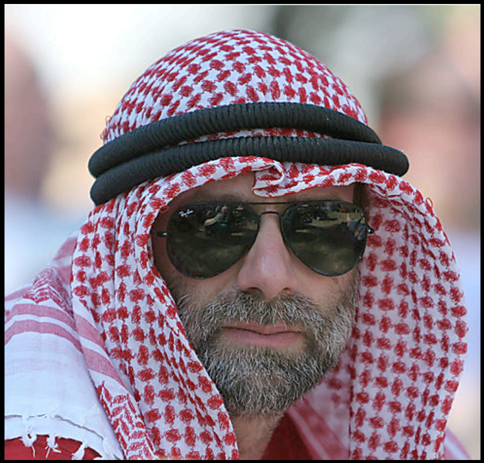
TOTALTRANSPARENCYSOLUTIONS

ID: 102
Threat score: 140

Bruce Schneier

Born: January 15, 1963
Parents: Schneier, Rebecca (b. 1942)
Schneier, Martin (b. 1935)

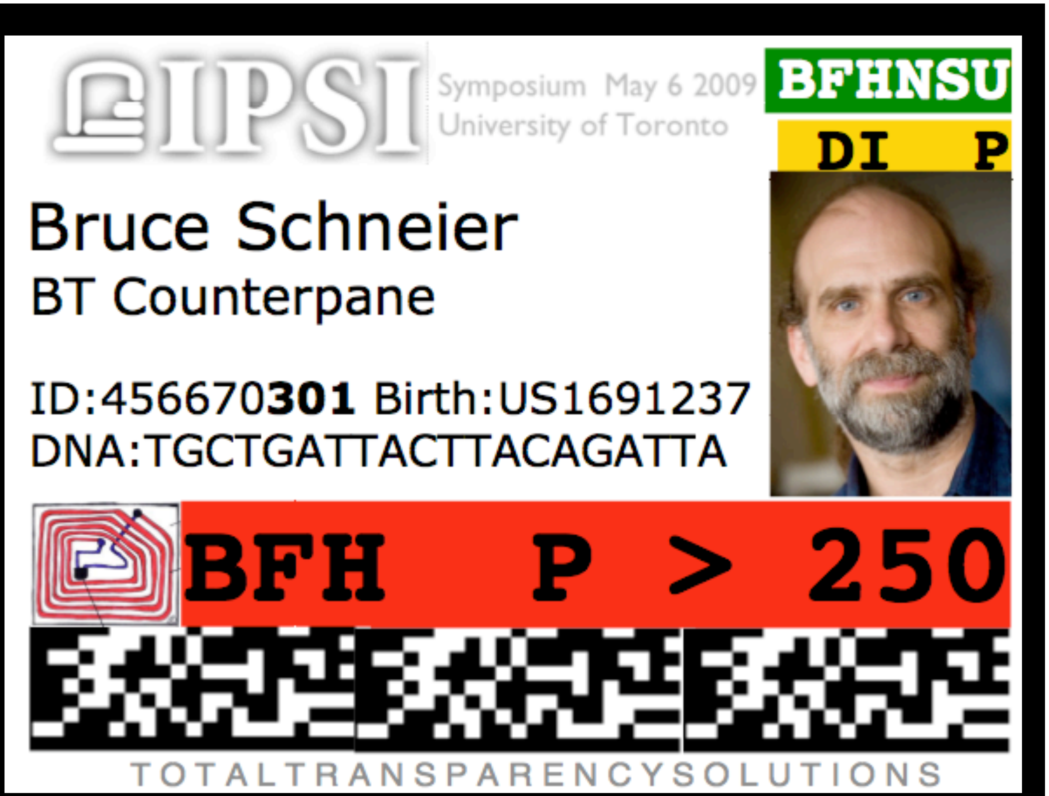
Warning: Known Disguise
Warning: Arab sympathizer?



Warning:
Liberal sympathizer?

2008 Political Donations:

Democratic Congressional Campaign Committee	$1000
Moveon.Org	$1000



IPSI Symposium May 6 2009
University of Toronto

BFHNSU
DI P

Bruce Schneier
BT Counterpane

ID:456670**301** Birth:US1691237
DNA:TGCTGATTACTTACAGATTA

BFH P > 250

TOTALTRANSPARENCYSOLUTIONS

Warning: Itinerant/ Unstable?

Previous addresses:
101 E Minnehaha Pkwy Minneapolis, MN 55419
730 Fair Oaks Ave #1 Oak Park, IL 60302
1300 Army Navy Dr #807 Arlington, VA 22202
7115 North Ave #16 Oak Park, IL 60302
1935 W Pratt Blvd #1 Chicago, IL 60626
1711 Hampshire Green Ln Silver. Sp. MD 20903
17th St #Pvt, Brooklyn, NY
1090 La Avenida St, Mountain View, CA 94043

Performing Identities

An alternative approach

- Identity re-conceptualized
  - as multiple, partial, context-specific, performative
- Policy engagement
  - interact with and learn from policy actors
- Public education
- Subject perspectives
- Ethnographically informed

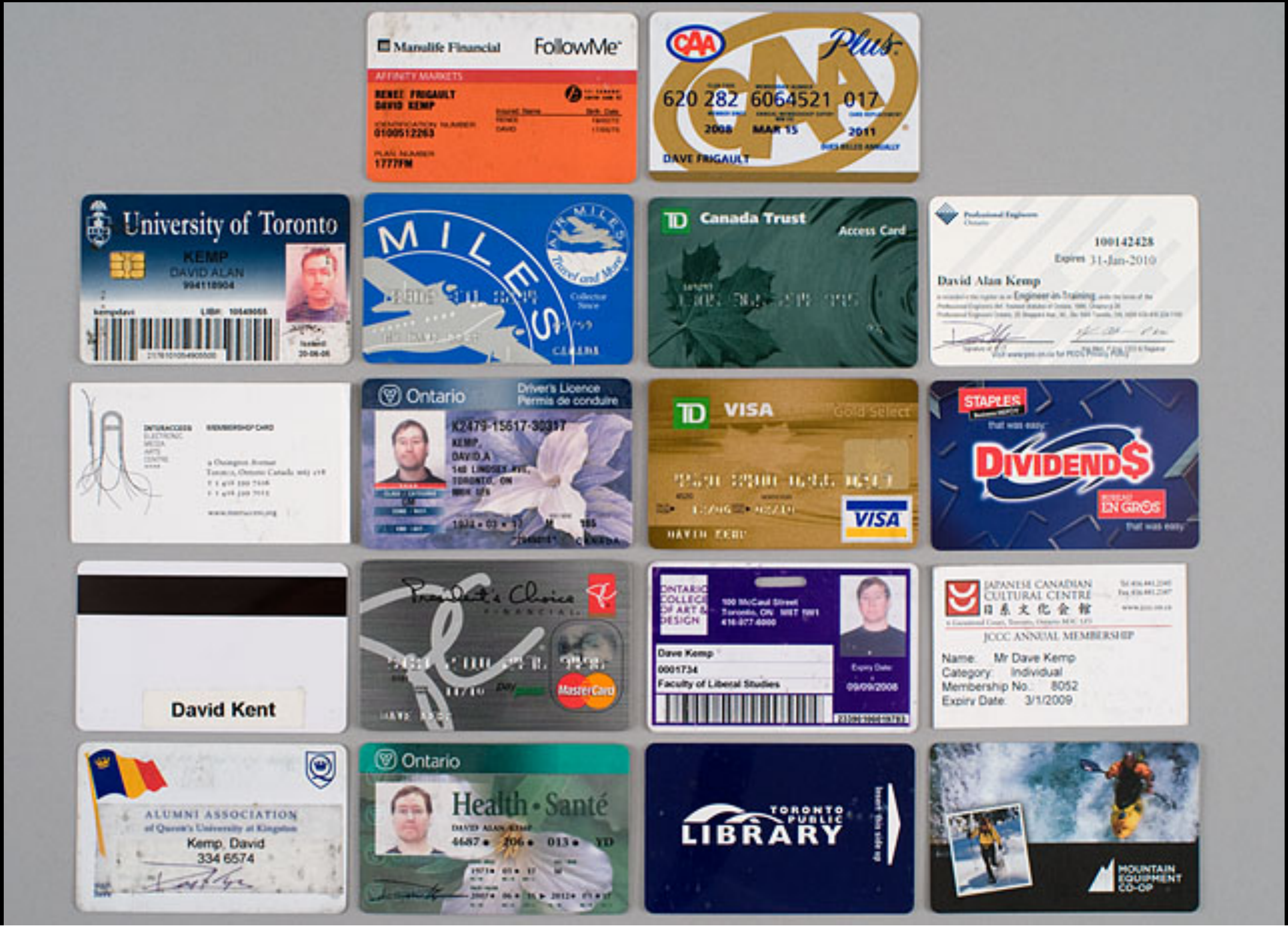
Wallet ethnography

Waiting line recruiting

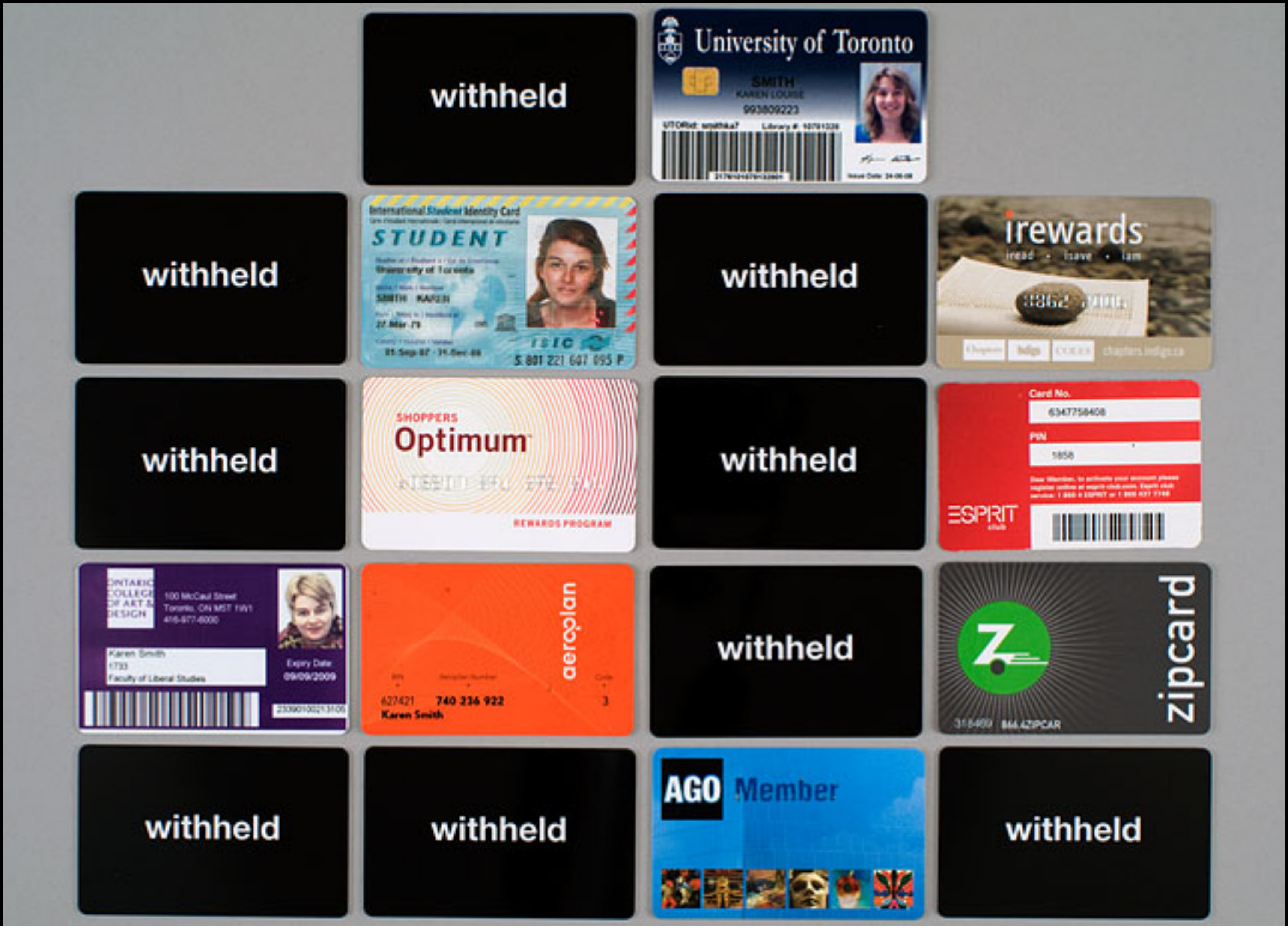
Questions:

- *What ID do you have in your wallet? Please tell us about it.*
- *Do you have an ID story to share?*

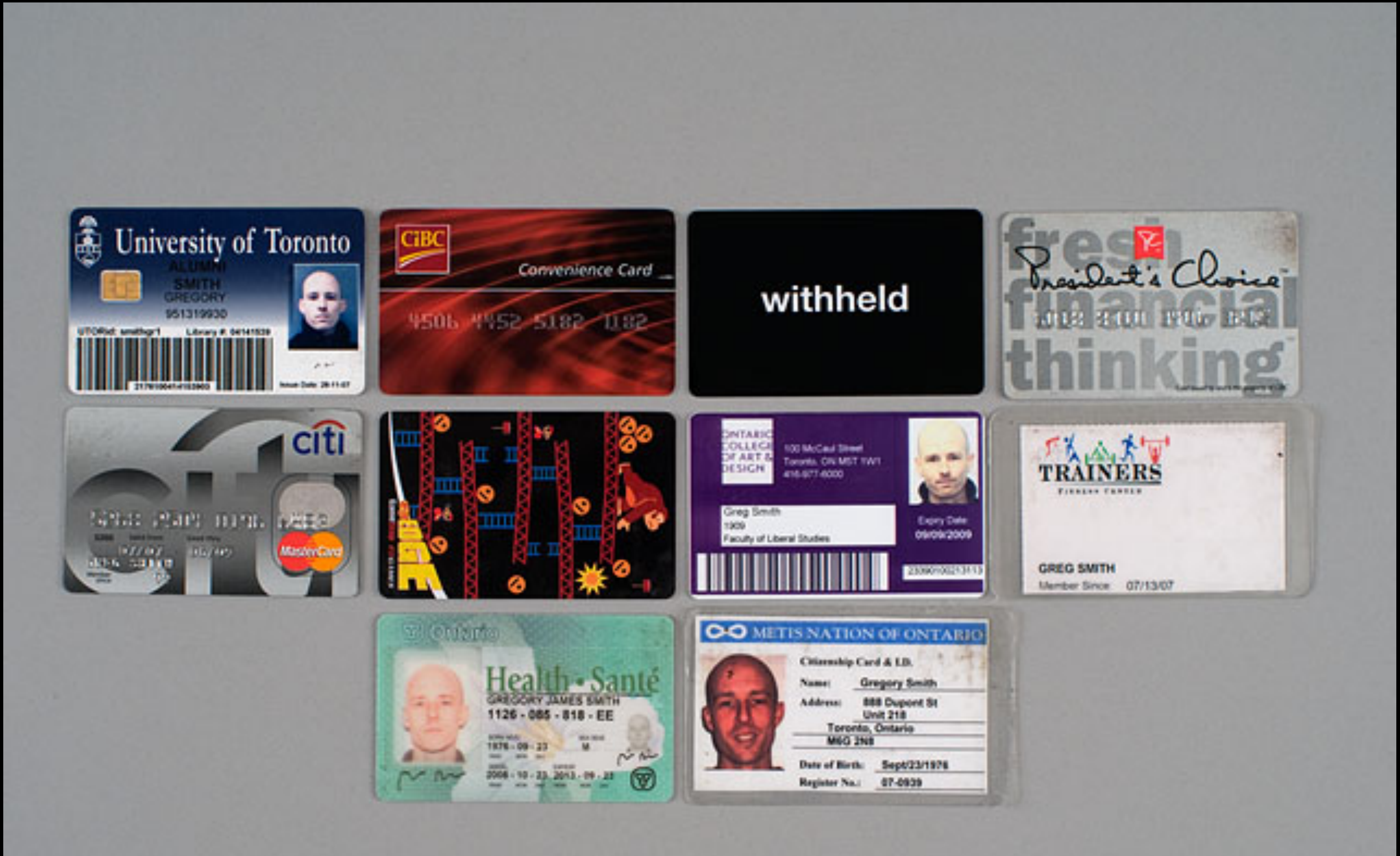
ID we carry - Dave



Karen’s ID


withheld
University of Toronto
SMITH
KAREN LOUISE
withheld
International Student Identity Card
STUDENT
ISIC
withheld
irewards
iread · isave · iam
withheld
SHOPPERS
Optimum
REWARDS PROGRAM
withheld
Card No.
PIN
ESPRIT
ONTARIO COLLEGE OF ART & DESIGN
Karen Smith
Faculty of Liberal Studies
Expiry Date
aeroplan
Karen Smith
withheld
zipcard
withheld
withheld
AGO Member
withheld

Greg’s ID

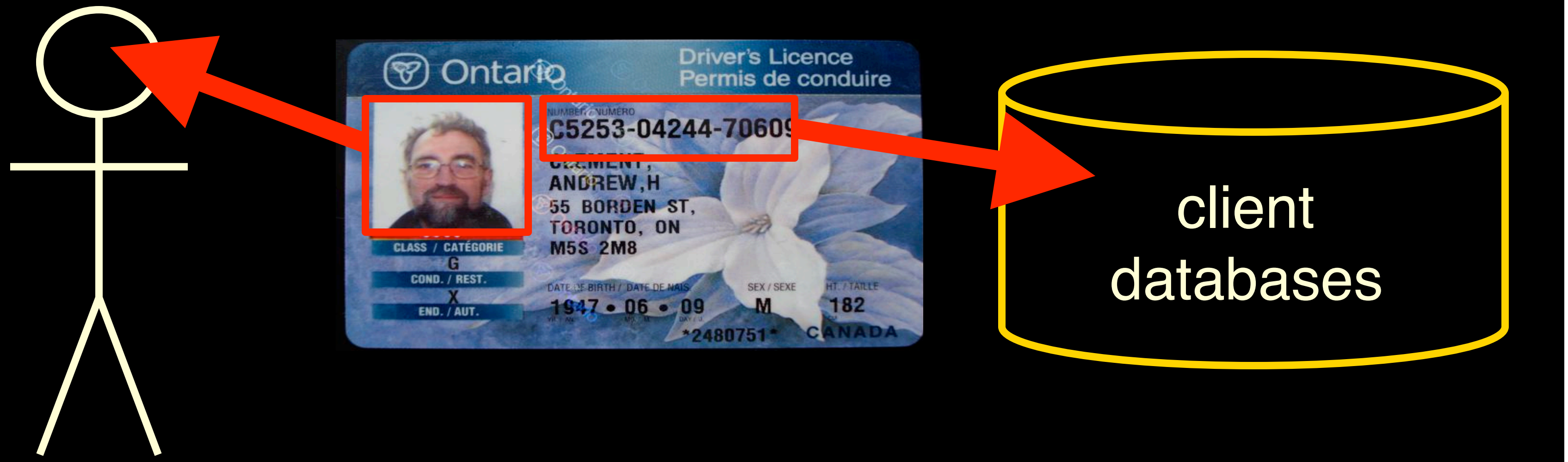


To be shown at the Surveillance Exhibition, Jan – Apr 2010,
Agnes Etherington Art Centre, Queen’s University, Kingston

Alternative ID models - I

Conventional (organizational) model

- ID token as a link between the person and the organizational databases



Ontario

Driver's Licence
Permis de conduire

NUMBER / NUMÉRO
C5253-04244-70609
CLEMENT,
ANDREW,H
55 BORDEN ST,
TORONTO, ON
M5S 2M8

CLASS / CATÉGORIE
G
COND. / REST.
X
END. / AUT.

DATE OF BIRTH / DATE DE NAIS.
1947 • 06 • 09

SEX / SEXE
M

HT. / TAILLE
182

2480751
CANADA

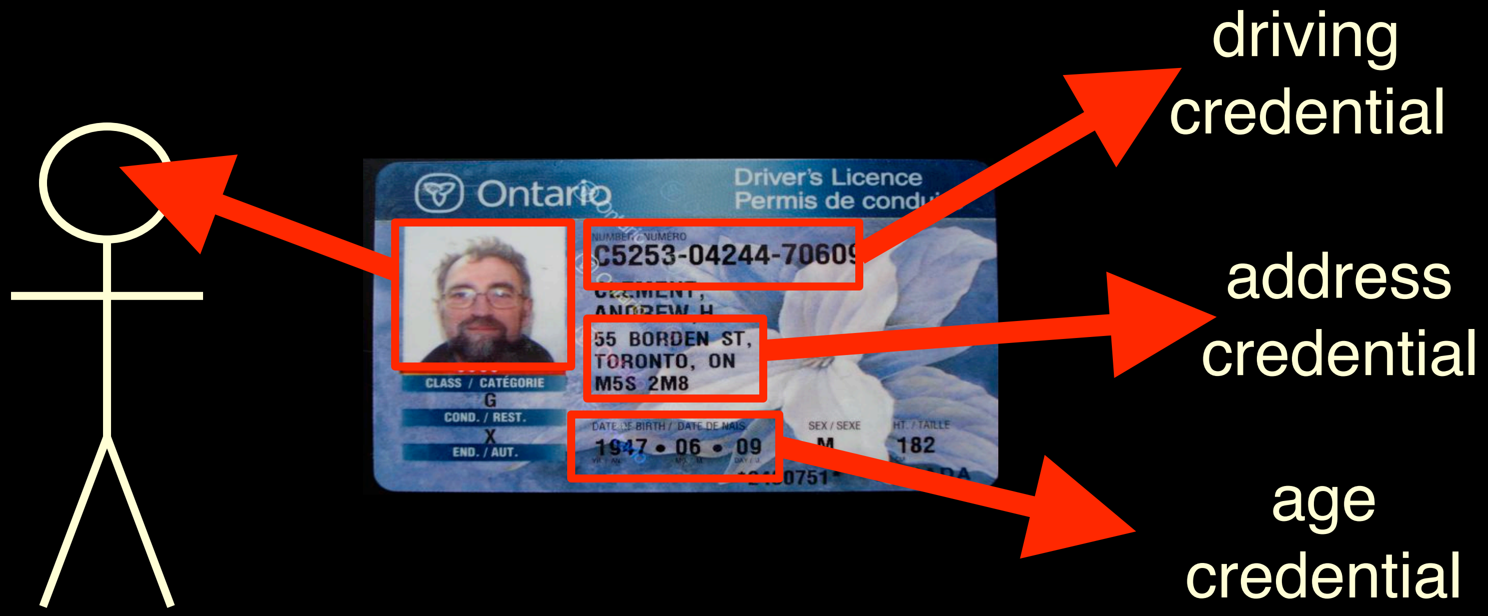
client databases

Involves full identification

Alternative ID models - II

Privacy/identity protective model

- ID token provides recognized credentials



driving credential

address credential

age credential

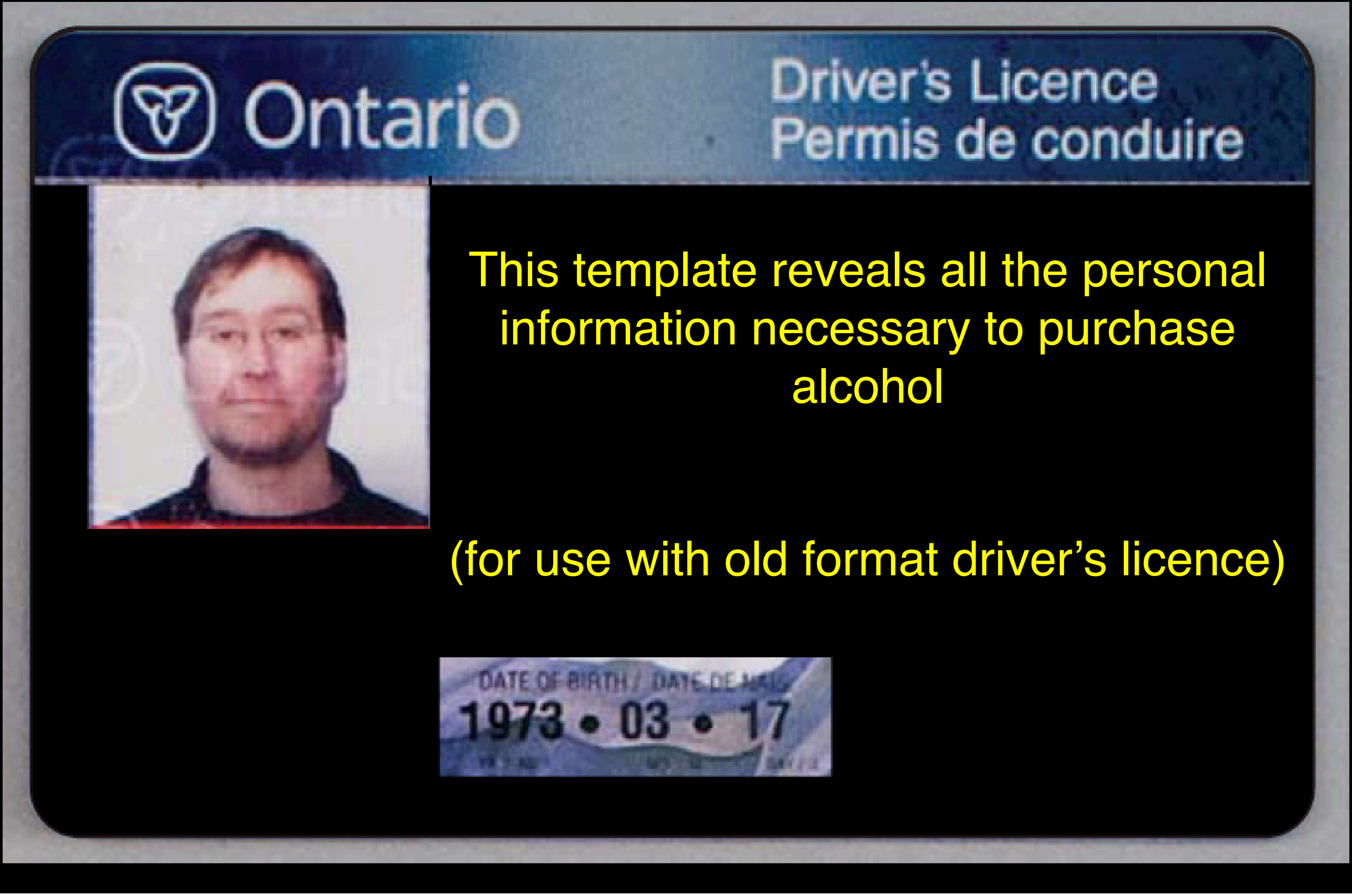
Anonymity and pseudonymities possible

Digital credentials

- Well recognized potential in on-line transactions – see:
  - David Chaum – Anonymous authentication (1980s)
  - Stefan Brands – U-Prove (Credentica > Microsoft)
  - 7 Laws of Identity – Kim Cameron et al

- Can this also work in face-to-face settings?
- A hybrid approach, using digital techniques for both in-person and on-line interactions?

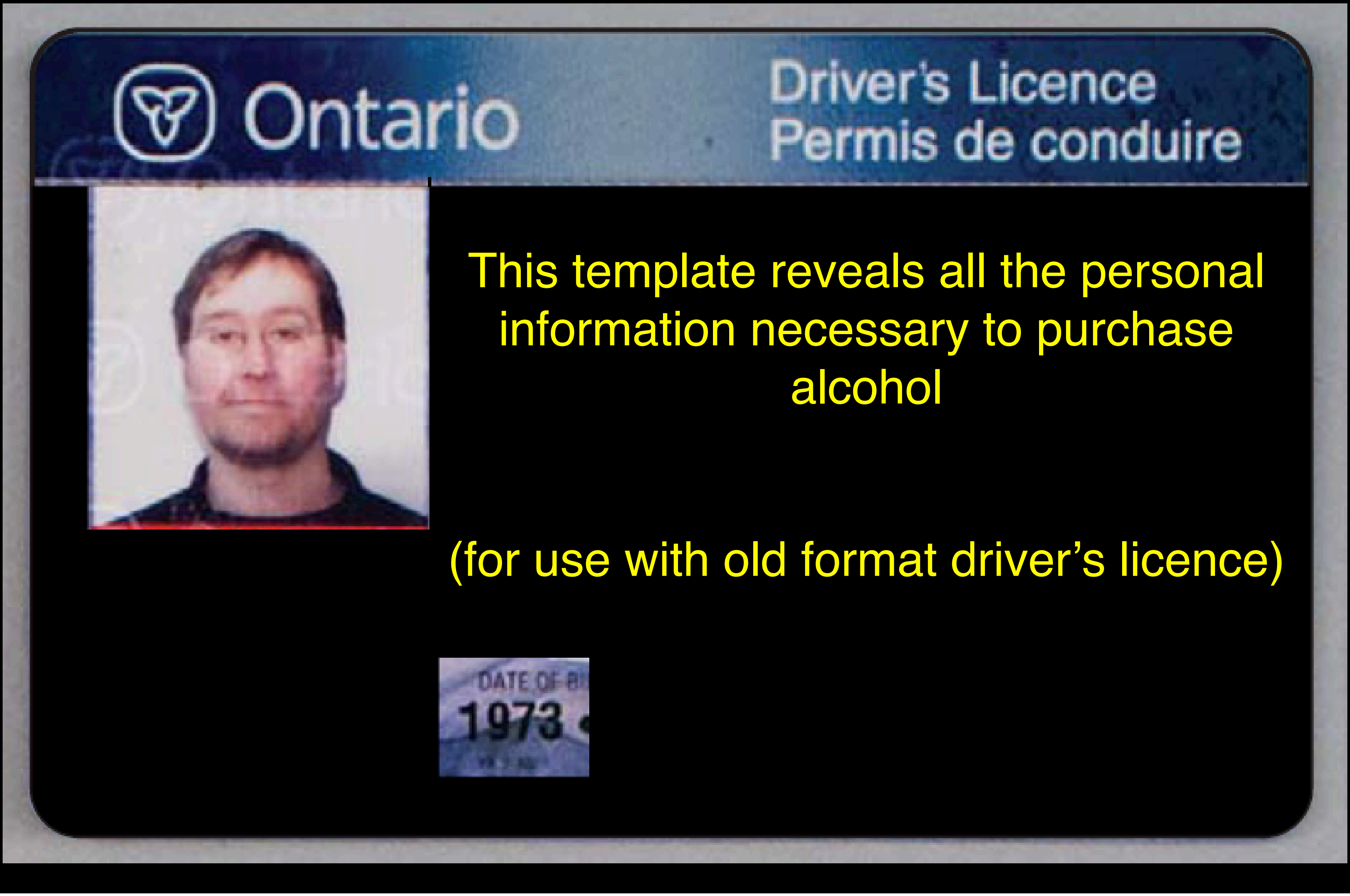
Selectively revealing personal info



This template reveals all the personal information necessary to purchase alcohol

(for use with old format driver's licence)

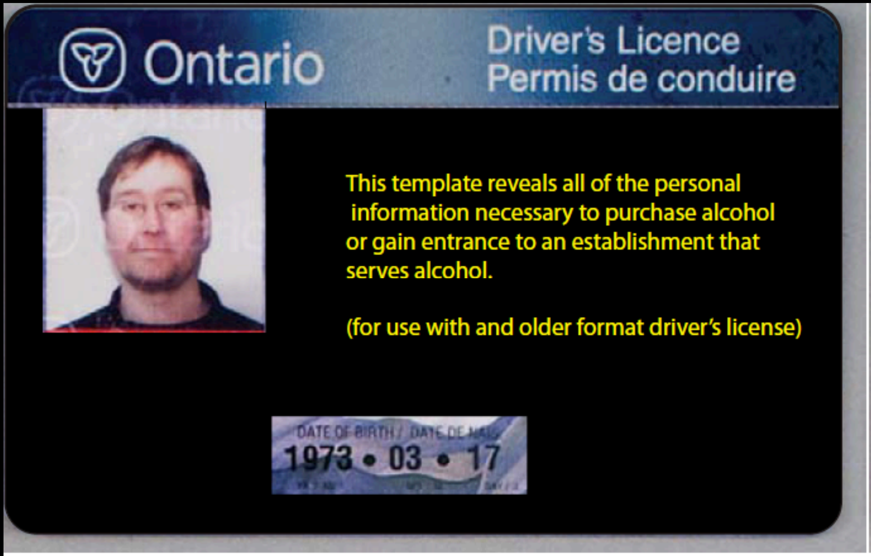
Selectively revealing personal info



This template reveals all the personal information necessary to purchase alcohol

(for use with old format driver's licence)

Selectively revealing personal info



Ontario

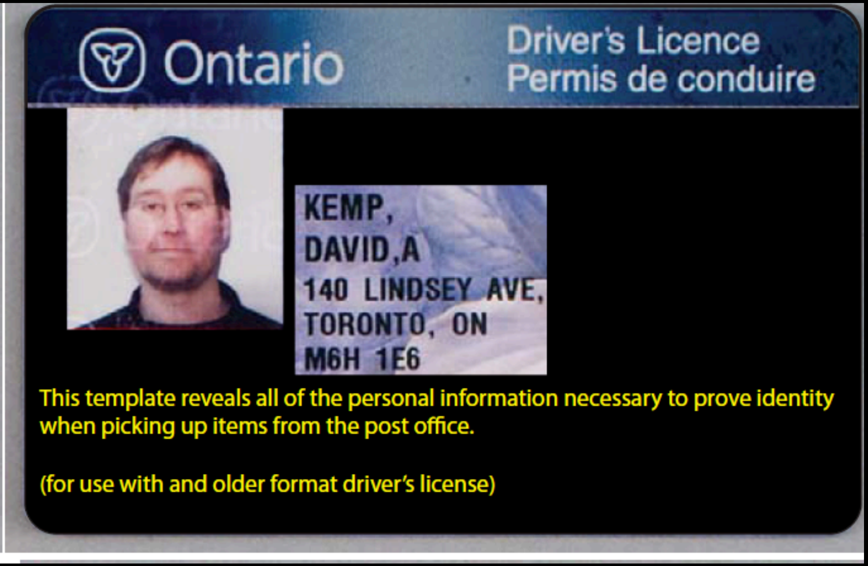
Driver's Licence
Permis de conduire

This template reveals all of the personal information necessary to purchase alcohol or gain entrance to an establishment that serves alcohol.

(for use with and older format driver's license)

DATE OF BIRTH / DATE DE NAIS

1973 • 03 • 17



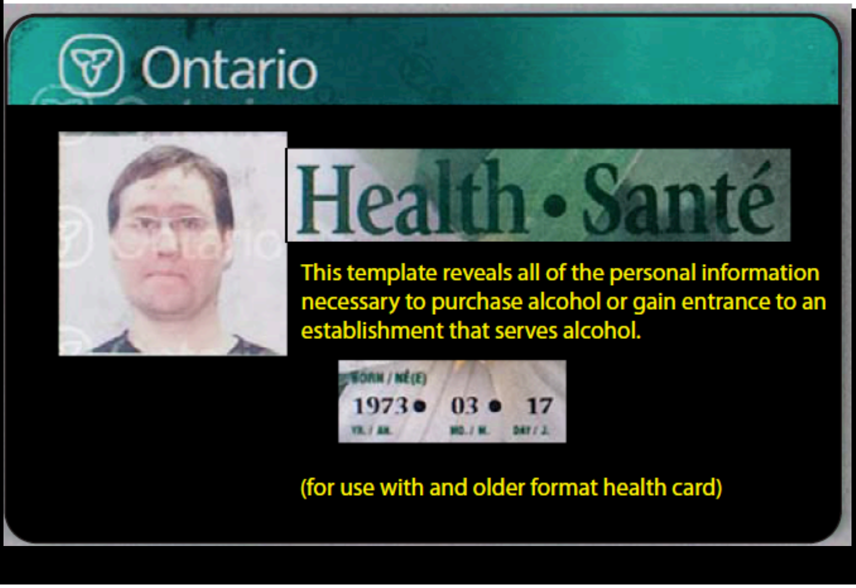
Ontario

Driver's Licence
Permis de conduire

KEMP,
DAVID,A
140 LINDSEY AVE,
TORONTO, ON
M6H 1E6

This template reveals all of the personal information necessary to prove identity when picking up items from the post office.

(for use with and older format driver's license)



Ontario

Health • Santé

This template reveals all of the personal information necessary to purchase alcohol or gain entrance to an establishment that serves alcohol.

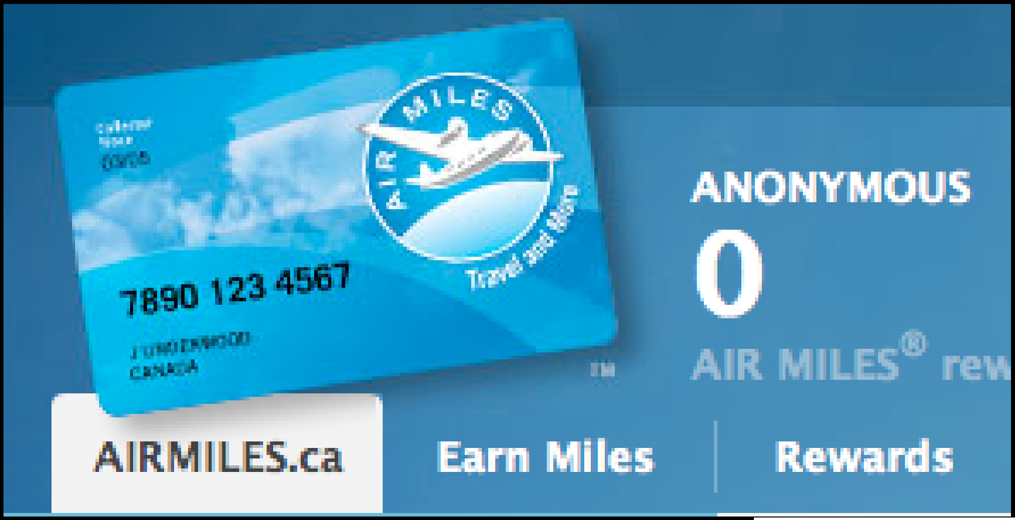
BORN / NÉ(E)

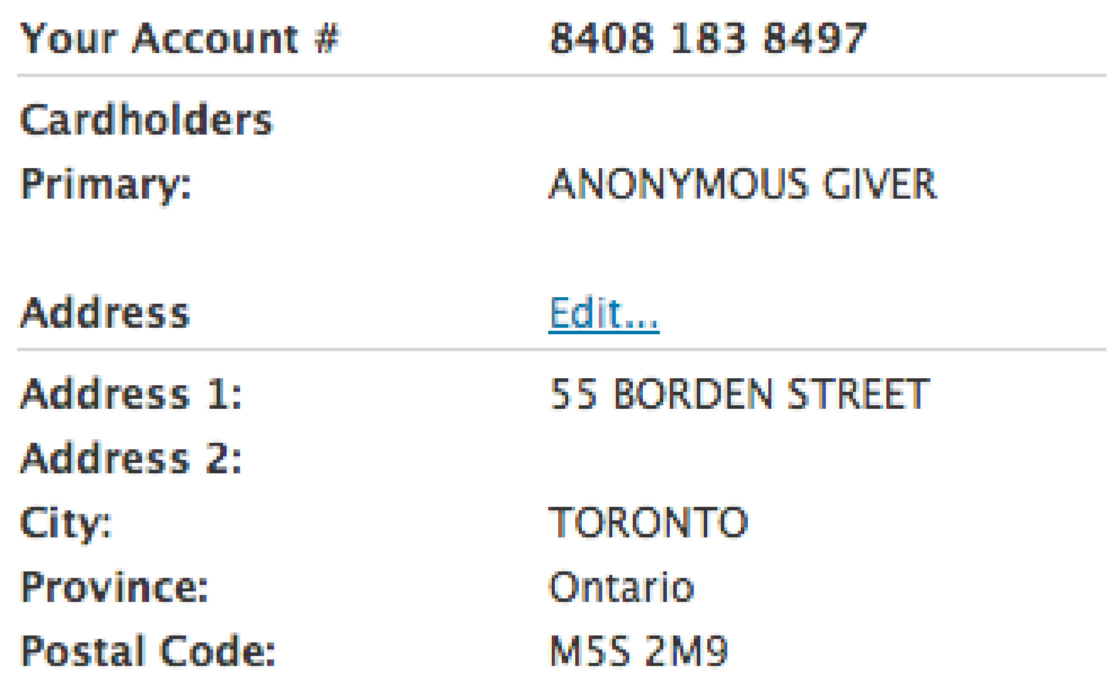
1973 • 03 • 17

YR. / AN. MO. / M. DAY / J.

(for use with and older format health card)

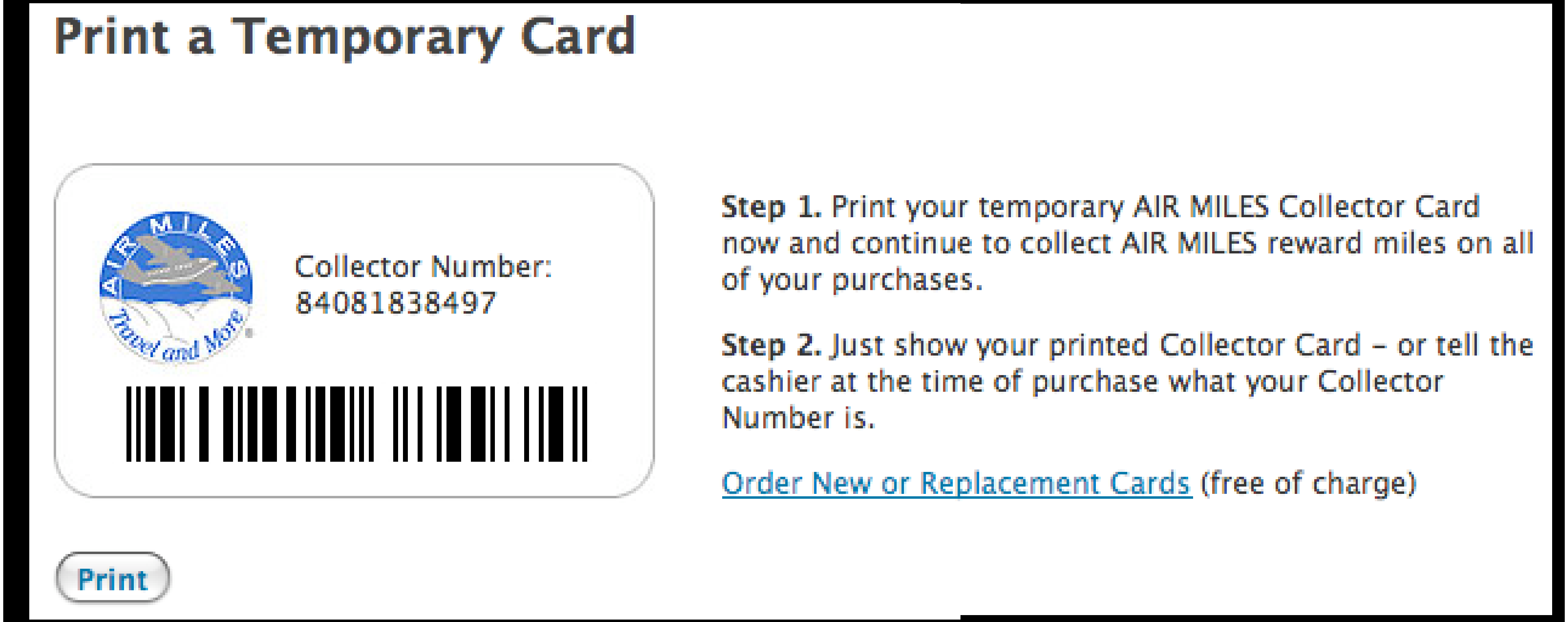
Anonymous “Loyalty”





Your Account #	8408 183 8497
Cardholders	
Primary:	ANONYMOUS GIVER
Address	Edit...
Address 1:	55 BORDEN STREET
Address 2:	
City:	TORONTO
Province:	Ontario
Postal Code:	M5S 2M9

Anonymous “Loyalty”



Print a Temporary Card

Collector Number:
84081838497

Step 1. Print your temporary AIR MILES Collector Card now and continue to collect AIR MILES reward miles on all of your purchases.

Step 2. Just show your printed Collector Card – or tell the cashier at the time of purchase what your Collector Number is.

Order New or Replacement Cards (free of charge)

Upcoming lectures on ID/authentication

Oct 5 – **Kostas Plataniot**is – Professor, ECE, U of Toronto
Introduction to Biometrics for ID and Authentication

Oct 26 – **Roger Clarke** – Principal, Xamax; Visiting Prof, ANU +++
A Sufficiently Rich Model of (Id)entity, Authentication and Authorization

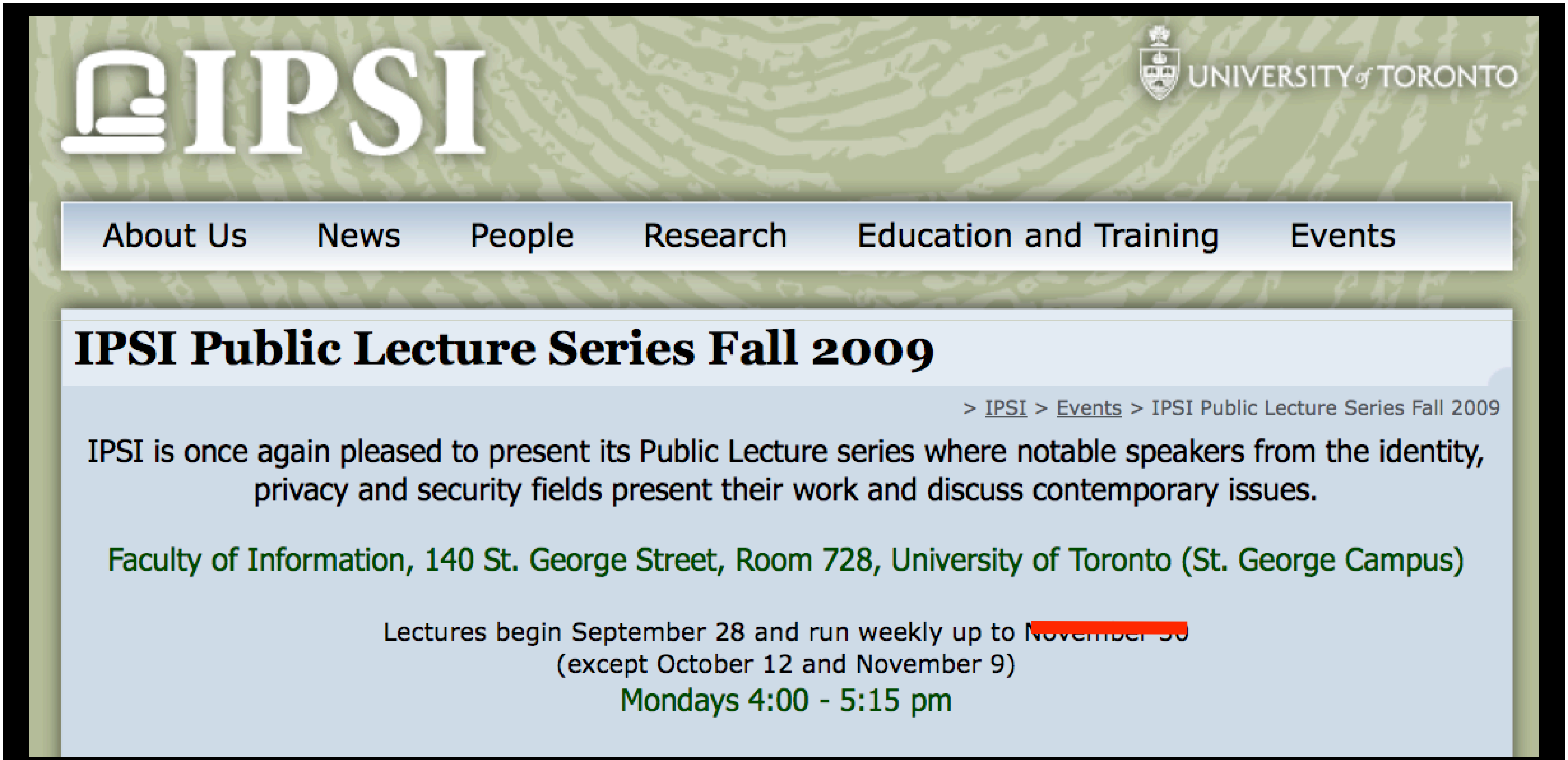
Nov 2 – **David Lyon** – Professor, QRC, Queens University, Sociology
Identifying Citizens: ID Cards as Surveillance

Nov 16 – **Carlisle Adams** – Professor, University of Ottawa
Credential Systems: Promise, Risks and Possible Mitigations

Nov 23 – **Lorrie Cranor** – Program Director, Carnegie Mellon University, CyLab/Engineering and Public Policy/ Institute for Software Research
Usable Privacy and Security

Nov 30 – **Dmitry Gorodnichy** – Senior Research Scientist, Canada Border Services Agency
Recognition in Video

Dec 7– **Ian Kerr** – *Professor, CRC in Ethics, Law and Technology, U Ottawa,*
Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society



IPSI Public Lecture Series Fall 2009

IPSI is once again pleased to present its Public Lecture series where notable speakers from the identity, privacy and security fields present their work and discuss contemporary issues.

Faculty of Information, 140 St. George Street, Room 728, University of Toronto (St. George Campus)

Lectures begin September 28 and run weekly up to ~~November 30~~
(except October 12 and November 9)
Mondays 4:00 - 5:15 pm

Lectures begin September 28 and run weekly up to December 7
(except October 12, 19 and November 9)

+ Student project presentations: December 14

http://www.ipsi.utoronto.ca/events/fall2009.htm