Big data, personalization and market manipulation

IAPP Canada Privacy Symposium

Toronto, May 9, 2014
Éloïse Gratton, Partner and Co-chair, Privacy
Plan of presentation

PART 1: Data protection laws challenged in light of Big Data
- A) Individuals in control of their personal information
- B) Definition of “personal information”

PART 2: Marketing and Market Manipulation
- A) Disclosure and subjective harm
- B) Use and objective harm
- C) Problematic business models: manipulation
PART 1:
Are data protection laws adapted to issues triggered by Big Data?
What is privacy?
First Wave: “Right to be Let Alone”

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.”

Second Wave:  
“Right for Respect for Private and Family Life”

“Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security (…)”


“Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people”

Third Wave: “Control over Personal Information”

RESOLUTION (73) 22

ON THE PROTECTION OF THE PRIVACY OF INDIVIDUALS
VIS-A-VIS ELECTRONIC DATA BANKS IN THE PRIVATE SECTOR

(Adopted by the Committee of Ministers on 26 September 1973
at the 224th meeting of the Ministers’ Deputies)

The Committee of Ministers,

Considering that the aim of the Council of Europe is to achieve a greater
unity between its member States;

Conscious of the already widespread and constantly increasing use of elec-
tronic data processing systems for records of personal data on individuals;

Recognising that, in order to prevent abuses in the storing, processing and
dissemination of personal information by means of electronic data banks in the private
sector, legislative measures may have to be taken in order to protect individuals;

Considering that it is urgent, pending the possible elaboration of an inter-
national agreement, at once to take steps to prevent further divergencies between the
laws of member States in this field;

Having regard to Resolution No. 3 on the protection of privacy in view of the
increasing compilation of personal data into computers, adopted by the seventh
Conference of European Ministers of Justice,

Recommends the governments of member States:

(a) to take all steps which they consider necessary to give effect to the principles
Fourth Wave?

• Increase in Volume of Information
• New Types of Information and Data Collection Tools
• Aggregation and Correlation of Data + Extensive Data-mining Capabilities
• Convergence in Technologies
• New Business Models (Customization and Sponsored Services)
What is Big Data?

More information + more sophisticated technology =

more knowledge and business opportunities and privacy concerns
A) Privacy as individuals in “control” of their personal information

(notice & choice model)
Inadequacy of Privacy Policies as a Means to Communicate Choices
Current policies are broad on the “uses” made with personal information
“How we use information we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads. (…)

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. (…) When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.”
High Volume of Privacy Policies are Not Read
British internet users need 31 hours a year to read online privacy policies

13 August 2013

- Website privacy policies take, on average, 25 minutes to read;
- 10% decline in the number of people aware companies collect and use their data;
- Generations Y and Z most prolific in data generation, but least likely to understand implications of their digital footprint;
- Cookie crumbles for Privacy and Electronic Communications Regulation.

New research from Deloitte has found it would take British internet users 31 hours to wade through the privacy policies of all the websites they visited in a year.

**Data Nation 2013: Balancing growth and responsibility** considered Great Britain’s attitudes to data collection and use by private and public sector organisations. The research revealed that, on average, it would take 25 minutes to read a website’s privacy policy in full. And, although 35% of people are fully aware that their data is collected and used, this represents a drop of 10% from 2012, revealing that more should be done to educate internet users on what’s happening with their data and why.

The survey, conducted by Ipsos MORI on behalf of Deloitte, shows that people are still not confident in the way that companies collect, use, handle and share data. Just 38% believe companies will keep their data safe, while only 22% are confident their details won’t be sold on to other organisations.

Despite generations ‘Y’ and ‘Z’ being the most prolific generators of data, particularly through social media, they are the least likely to understand the consequences of the digital trails they leave behind. Nearly one-third (28%) of these generations perceive that companies have little or no information about them, or simply don’t know how much data is collected. This compares with 19% for generation ‘X’ and 14% of baby boomers.
Dynamic Aspect of Privacy Policies and Business Models
Facebook’s Eroding Privacy Policy: A Timeline

Since its incorporation just over five years ago, Facebook has undergone a remarkable transformation. When it started, it was a private space for communication with a group of your choice. Soon, it transformed into a platform where much of your information is public by default. Today, it has become a platform where you have no choice but to make certain information public, and this public information may be shared by Facebook with its partner websites and used to target ads.

To help illustrate Facebook’s shift away from privacy, we have highlighted some excerpts from Facebook’s privacy policies over the years. Watch closely as your privacy disappears, one small change at a time!

Facebook Privacy Policy circa 2005:

No personal information that you submit to Thefacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings.

Facebook Privacy Policy circa 2006:

We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your school, your specified local area, and other reasonable community limitations that we tell you about.

Facebook Privacy Policy circa 2007:

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.

Facebook Privacy Policy circa November 2009:

Facebook is designed to make it easy for you to share your information with anyone you want. You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings. You should review the default privacy settings and change them if necessary to reflect your preferences.
Does the “notice and choice” model still make sense?
Implied or deemed consent as a solution?
Reasonable-ness test

PIPEDA: Under s. 5(3) an organization may collect, use or disclose personal information “only for purposes that a reasonable person would consider appropriate in the circumstances.”

Alberta or the B.C. DPL: In meeting its responsibilities under the DPL, an organization must act “in a reasonable manner”, and must develop and follow policies and practices “that are reasonable for the organization” to meet its obligations. The golden standard is as follows: “what a reasonable person would consider appropriate in the circumstances”.

Directive 95/46/EC states that “any processing of personal data must be lawful and fair to the individuals concerned”.

When is a data collection activity "reasonable"?
B) The definition of “personal information”
Definition of “personal information”

- **Canada:**
  - QC: “Any information which relates to a natural person and allows that person to be identified.”
  - PIPEDA: “Information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.”
  - CB: “information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information; »
  - AL: “information about an identifiable individual” (vs. personal employee information)

- **EC Directive 1995:** “Any information relating to an identified or identifiable natural person” which is “one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”
over-reaching definition
Speeches

The benefits of a broad interpretation of the definition of personal information

Remarks at the Canadian Bar Association’s Access and Privacy Symposium Dinner

September 14, 2012
Ottawa, Ontario

Address by Jennifer Stoddart
Privacy Commissioner of Canada

(Check against delivery)

Introduction

Good evening everyone. All in all, today’s digital economy, and our digital society for that matter, is marked by many players holding a growing wealth of personal information.

And in a world increasingly marked by businesses finding new ways of using personal information along with large scale data breaches, personal information is being put at greater and greater risk.

In this world, our Office stands as a privacy guardian. And in setting out to fulfill PIPEDA’s stated purpose, I sometimes look to the words of Theodore Roosevelt for both inspiration and resolve. He famously once said, "speak softly and carry a big stick." But, given the tools currently bequeathed unto me by law, I'm left to "speak softly and carry a big, banana cream pie."

I mean, as it stands, we do hold some leverage to deter bad privacy practices such as when we make findings public, but this comes only after the fact.
Publicly available information is still personal information

- Some laws (PIPEDA, BC, AL) have exceptions for publicly available information (e.g., information that the individual has voluntarily given which can be found in lists such as "directories") Ex: PIPEDA, Regulations Specifying Publicly Available Information (SOR/2001-7)

- Information will still be personal information even if it is publicly available within the meaning of the regulations, and is exempt from applicable consent requirements. Englander v. TELUS Communications Inc., 2004 FCA 387 (CanLII)

- QC: there is only an exception if the information is "public" under the applicable laws
Ex: Status of IP addresses

“So, unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side.”

(individuals which) “by their own actions, have encouraged indiscreet revelations about which they complain later on, cannot avail themselves of the right to privacy.”

SUPREME COURT OF CANADA


DATE: 20131115

Docket: 34890

S.C.R. 733
under-reaching definition
“Taking a broad, contextual view of the definition of personal information, the OPC will generally consider information collected for the purpose of OBA to be personal information, given: the fact that the purpose behind collecting information is to create profiles of individuals that in turn permit the serving of targeted ads; the powerful means available for gathering and analyzing disparate bits of data and the serious possibility of identifying affected individuals; and the potentially highly personalized nature of the resulting advertising.”

“(…) and any information allowing a natural person to be singled out and treated differently”

Article 29 Working Party, Opinion 08/2012 providing further input on data protection reform discussions, October 5, 2012, p. 5.
uncertain definition
Directive 95/46/CE defines personal data as:
"any information concerning an identified or identifiable person (...)

Paragraph (26) of the Directive 95/46/CE:
"Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (...)."
Information will be about an “identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.

- *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII).

(This case arose under the *Access to Information Act, R.S., 1985, c. A-1* that incorporates the definition of “personal information” from the *Privacy Act, R.S.C. 1985, c. P-21*, which is virtually identical to the definition of “personal information” in PIPEDA.)
Case Study

- **Facts:**
  - EU company is about to transfer to a U.S. pharmaceutical company *key-coded* clinical trial data (the names of the trial participants have been removed and replaced by codes).
  - EU company has to determine if the information is anonymized or whether it is considered “personal information”, in which case additional legal requirements may apply to the transfer.

- **Question:**
  - Is the information transferred *personal information*?
  - Should *illegal means* be taken into account when determining whether the anonymized information should still be considered as personal?
Are IP addresses *personal information*?

- April 2007: Cour d'appel de Paris – NO
- May 2007: Cour d'appel de Paris – NO
- July 2007: Press release from CNIL – YES
- May 2008: Cour d’appel Rennes – YES
- January 2009: Cour de cassation – NO
- June 2009: Tribunal de grande instance Paris – YES
- February 2010, *Cyrille S. c. Sacem* - Cour d'appel de Paris – NO
What are the solutions?


Data protection is broader than privacy

“(…) we believe that data protection goes further than the protection of privacy in its narrowest sense: it serves to protect many interests of the data subject, of which his privacy is only one.”

- U.K. Lindop Report dating back to 1978 (para. 21.26)

“On the one hand, it has to be considered that the concept of private and family life is a wide one, as the European Court on Human Rights has made clear. On the other hand, the rules on protection of personal data go beyond the protection of the broad concept of the right to respect for private and family life.(…)”

PART 2:
Marketing and Market Manipulation
Retweeted by Eloise Gratton

Daniel Barth-Jones @dbarthjones · Dec 9
Predictive Harm & Due Process: 3 Important #Privacy Law papers to read as a set: papers.ssrn.com/sol3/papers.cf... from @eloisegratton (3/3)

Retweeted by Eloise Gratton

Daniel Barth-Jones @dbarthjones · Dec 9
Predictive Harm & Due Process: 3 important #Privacy Law papers to Read as a set: papers.ssrn.com/sol3/papers.cf... from @katecrawford @Lawgeek (2/3)

Retweeted by Eloise Gratton

Daniel Barth-Jones @dbarthjones · Dec 9
Predictive Harm & Due Process: 3 important #Privacy Law Scholars to Read as a set: papers.ssrn.com/sol3/papers.cf... from @DANIELLECITRON (1/3)
Technological Due Process

Danielle Keats Citron

If Personal Information is Privacy’s Gatekeeper, then Risk of Harm is the Key: A proposed method for determining what counts as personal information.

Abstract

In the late nineties, with the development of automated data banks and the growing use of computers in the private and public sector, privacy was conceptualized as having individuals “in control over their personal information” (Weiss, 1997). The principles of Fair Information Practices were elaborated during this period and have been incorporated into data protection laws (“DPIs”) adopted in various jurisdictions around the world ever since. These DPIs protect personal information, which is defined similarly in various DPIs (such as in Europe and Canada) as “information relating to an identifiable individual”. In the U.S., information is accorded special recognition through a series of sectoral privacy statutes focused on protecting “personally identifiable information” (or PI), a notion close to personal information. Going back to the early seventies, we can note that identical or very similar definitions of personal information were already used in DPIs, illustrating that this definition of personal information dates back to this period.

In recent years, with the Internet and the circulation of new types of information, the efficiency of this definition may be challenged. Recent technological developments are triggering the emergence of new identification tools allowing for easier identification of individuals. Data mining techniques and capabilities are reaching new levels of sophistication. In the era of Big Data, because it is now possible to interpret almost any data as personal information (even data can in one way or another be related to some individual) the question arises as to how much information should be considered as personal information.

In section 1, I elaborate on how a literal interpretation of the definition of personal information is no longer workable. In light of this, I present the proposed method for determining what constitutes personal information, under which the ultimate purpose behind DPIs should be taken into account. I then demonstrate that the ultimate purpose of DPIs was to protect individuals against a risk of harms triggered by organizations collecting, using, and disclosing their...
DPL: risk of harm decision tree

**Disclosure** (subjective harm)
- Information “identifiable”
  - Identifiable
  - Available
  - Intimate nature

**Use** (objective harm)
- Information “identifiable”
  - Impact on individual (negative)
    - Accurate
    - Relevant
A) Disclosure and **subjective** harm
“(…) the notion of privacy has a substantial emotive content in that many of the things which we feel the need to preserve from the curiosity of our fellows are feelings, beliefs or matters of conduct which are themselves irrational.”

1972, the Scottish Justice Committee.
Subjective harm and disclosure of information

- Warren and Brandeis in their article about privacy and the right to be let alone, referred to the disclosure of private facts in new press, contending that privacy involved “injury to the feelings.” (1890)

- William L. Prosser discusses how the common law recognizes a tort of privacy invasion in cases where there has been a “[p]ublic disclosure of embarrassing private facts about the plaintiff”. (1960)

- Ryan Calo suggests that many of the harms we associate with a person seeing us, such as “embarrassment, chilling effects or a loss of solitude”, flow from the mere belief that one is being observed. (2011)

- *Jones v. Tsige* 2012 ONCA 3, the Court of Appeal for Ontario hinted that there was a subjective component to an invasion of privacy, assimilated to “distress, humiliation or anguish”. (2012)
DPL: risk of harm decision tree (disclosure)

disclosure
(subjective harm) → information “identifiable” → available → identifiable

intimate nature
Disclosure of information and business practices or models
A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.; Saul Hansell contributed reporting for this article.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list.
Google settles privacy complaint with FTC over Buzz social networking launch

By Cecilia Kang, Published: March 30, 2011  E-mail the writer

The Federal Trade Commission said Wednesday that Google agreed to settle a complaint that it violated its own privacy promises to consumers when it rolled out its Buzz social networking application.

The settlement requires Google to adopt a comprehensive privacy program and to submit to an independent privacy audit every two years for the next two decades. This is the first time the FTC has required a company to implement such a program.
Personalized advertising
How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you
How cyber shame scams are playing on our privacy fears and scaling up

Christine Dobby | March 29, 2014 7:00 AM ET
More from Christine Dobby | @christinedobby
Note2be avec vous !
Malgré tous ceux qui lui veulent du mal, note2be poursuit sa route. Chaque jour vous êtes des milliers à vous connecter et le nombre de professeurs notés ne cesse de croître.
Le site compte aujourd'hui plus de 165 000 inscrits !

Dernières news

<table>
<thead>
<tr>
<th>Titre</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note2be aime Facebook</td>
<td>il y a 3 ans</td>
</tr>
<tr>
<td>Faites savoir à vos contacts que vous notez vos profs. Publiez vos actions sur ...</td>
<td></td>
</tr>
<tr>
<td>Les commentaires sont libres</td>
<td>il y a 3 ans</td>
</tr>
<tr>
<td>Il est désormais possible d'ajouter un commentaire à votre note.</td>
<td></td>
</tr>
<tr>
<td>A vos claviers...</td>
<td></td>
</tr>
<tr>
<td>Bonne rentrée à tous !</td>
<td>il y a 5 ans</td>
</tr>
<tr>
<td>C'est la rentrée pour les élèves mais aussi pour les profs ...</td>
<td></td>
</tr>
<tr>
<td>La justice valide la notation des professeurs sur internet !</td>
<td>il y a 5 ans</td>
</tr>
<tr>
<td>Mardi 23 juin 2009, la Cour de Cassation allemande, a renoncé une décision ...</td>
<td></td>
</tr>
<tr>
<td>C'est les examens pour les profs aussi !</td>
<td>il y a 5 ans</td>
</tr>
<tr>
<td>L'année se termine. C'est le moment des examens et des désaccords...</td>
<td></td>
</tr>
</tbody>
</table>
B) Use and **objective** harm
Objective harm and use of information

- Legal philosopher van den Hoven suggests a certain taxonomy which illustrates the moral reasons for the justification of protection of personal information.

- He posits that we would not want to be “left alone” or to be “private”, but instead we want to prevent others from harming us, treating us unfairly, discriminating against us, or making assumptions about who we are.

Kafka, The Trial
Objective harm and use of information

- Concerns: organizations using the information of individuals in a way which would be detrimental to them.

- On the issue of data protection raised by RFID tags, the Article 29 Working Party noted that:
  - “data relates to an individual if (...) such information is used to determine or influence the way in which that person is treated or evaluated.”

- Types of objective harms: financial or economic harm, discrimination, physical harm.
DPL: risk of harm decision tree (use)

- **use** (objective harm)
- information “identifiable”
- impact on individual (negative)
- accurate
- relevant
Use of information and business practices or models
Explore flu trends - Canada

We've found that certain search terms are good indicators of flu activity. Google Flu Trends uses aggregated Google search data to estimate flu activity. Learn more >

Flu symptoms?
If you have flu-like symptoms, stay home and rest until they are gone. If you get flu-like symptoms and are pregnant, have underlying health problems, or if they get worse, contact your healthcare provider.

Flu symptoms include:
- Almost always: cough, fever
- Common: fatigue, muscle aches, sore throat, headache, decreased appetite, runny nose
- Sometimes: nausea, vomiting, diarrhea

More official info: www.flu.gov

Animated Flu Trends in Google Earth
Download and explore Flu Trends data in Google Earth. Need Google Earth?
Download it here.

Embed this chart
Use this embed code to show this chart on your website.
Dynamic pricing:
an old practice making a come back online...
Dynamic pricing: Case Studies
When does dynamic pricing work?

- Customers must have a difference in their willingness to pay.
- The market must be segmentable.
- Limited potential for arbitrage.
- Cost of segmenting and policing must not exceed revenue increases due to customization.
- Must not breed violations of perceived fairness.
La Commission nationale de l'informatique et des libertés (CNIL) a adressé, vendredi 23 septembre, un "avertissement public" à la société Pages Jaunes, pour avoir constitué, dans des conditions non conformes à la loi, 34 millions de profils d'internaute. Dans un communiqué, le groupe Pages Jaunes affirme "étudier toutes les possibilités de recours" contre cette décision, qui ne s'accompagne pas de sanctions financières.
Marketers Should Take Note of When Women Feel Least Attractive

www.adweek.com

Identifying the right audience is critical for marketers, but pinpointing the right day and time to talk to that audience can be just as important, especially when
Disclosure ratcheting

- Experiments show that it is possible to leverage cognitive bias or otherwise manipulate conditions in order to get subjects to disclose more personal information.
C) Problematic business models involving manipulation
Subliminal advertising and manipulation
RECOMMENDATION 509 (1968)[1]

on human rights and modern scientific and technological developments

The Assembly,

1. Considering that member States under the Statute of the Council of Europe accept the principle of the enjoyment by all persons within their jurisdiction of human rights and fundamental freedoms;

2. Having regard to the serious dangers for the rights of the individual inherent in certain aspects of modern scientific and technological development;

3. Believing that newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights;

4. Considering that the law in the majority of the member States does not provide adequate protection against such threats to the right of privacy, and that there is in consequence danger of violation of Article 8 of the Convention on Human Rights;

5. Noting that some member States of the Council of Europe are planning to revise their legislation on this subject and that it would be desirable for any such reform to tend towards a greater harmonisation of the law;

6. Considering that it would be useful to make a detailed study of the legal problems arising in connection with the right to privacy and its violation by modern technical devices, with special reference to the European Convention on Human Rights;
Subliminal message in presidential campaign

Dirty rats leave Gore a subliminal message
It was only visible for a thirtieth of a second but here's proof the gloves are really off
Special report: the US elections

Julian Borger in Washington
The Guardian, Wednesday 13 September 2000 01.18 BST

The increasingly accident-prone Bush presidential campaign was accused of dirty tricks yesterday, after it was discovered that the word "rats" appeared subliminally in a Republican political broadcast targeting Democratic health care proposals.
The offending word, in large white capital letters, flashes against a black background for a thirtieth of a second as a woman narrator criticises Vice President Al Gore's plan for government funding of prescriptions for pensioners.

George W Bush ridiculed as "bizarre and weird" accusations that his campaign was trying to use such underhand techniques to discredit his opponent. Yesterday, however, he announced that the $2.5m (£1.3m) advertising campaign would be withdrawn.
Subliminal advertising or manipulation
Subliminal advertising
Facial similarity manipulation
Let's face it: Researchers say voters swayed by candidates who share their looks

Made up your mind who to vote for?

Maybe it's because you like the looks of the candidate. Or maybe it's because the candidate looks a little like you, even if you don't realize it.

In a paper slated to be published in the December issue of Public Opinion Quarterly, Jeremy Bailenson, an assistant professor of communication, and Shanto Iyengar, the Harry and Norman Chandler Professor in Communication, say that people are subconsciously swayed by candidates who share their facial features.

"The field of political science has been dominated by the main idea that voters are rational and that voters base their decisions on substance and issues and policy," Bailenson said. "We wanted to say, Well, how much of our decisions are actually based on superficial qualities?"

The answer: More than they expected.

In three experiments, the researchers and their graduate students worked with cheap, easy-to-use computer software to morph pictures of about 500 test subjects with photos of politicians. And they kept coming up with the same results: For the would-be voters who weren't very familiar with the candidates or in perfect lockstep with their positions or political parties, the facial similarity was enough to clinch their votes.

Social scientists have long known that people are more inclined to be friendly and helpful to those who obviously look like them. But what surprised Bailenson and Iyengar was that nobody swayed by one of the morphed photos could tell they were looking at a blended image.

"The big finding No. 1 is that when we do this, no one has any conscious, explicit idea that it's going on," Bailenson said. "The second big
Figure 3. An example of two subjects from Experiment Two, one morphed with Clinton and one morphed with Granholm. Participants saw one of the morphed images in the right panel.
Vance Packard (The Hidden Persuaders, 1957) acknowledges that the marketers of the late 1950s were “mostly decent, likeable people” who “want to control us just a little bit”; they might be appalled, he suggests, by the technologies and techniques of the future.

“when you are manipulating, where do you stop? Who is to fix the point at which manipulative attempts become socially undesirable?”

Thank you!

Eloïse Gratton
+514 987-5093
eloise.gratton@mcmillan.ca