The societal context of social media

MARK 360

WEEK 5

Overview

- The creepy factor – do people care about online privacy?
- The legal context – Privacy
- The legal context - SPAM

THE CREEPY FACTOR – DO PEOPLE CARE ABOUT ONLINE PRIVACY?

“When something online is free, you’re not the customer, you’re the product.”

Variously attributed to Bruce Schneier (October 2010) and Douglas Rushkoff (September 2011)

Data mining

- Data mining means that it isn't just individual customer data that is the issue

- Jennifer Golbeck: The curly fry conundrum: Why social media "likes" say more than you might think (TEDx 2014) 10 minute video

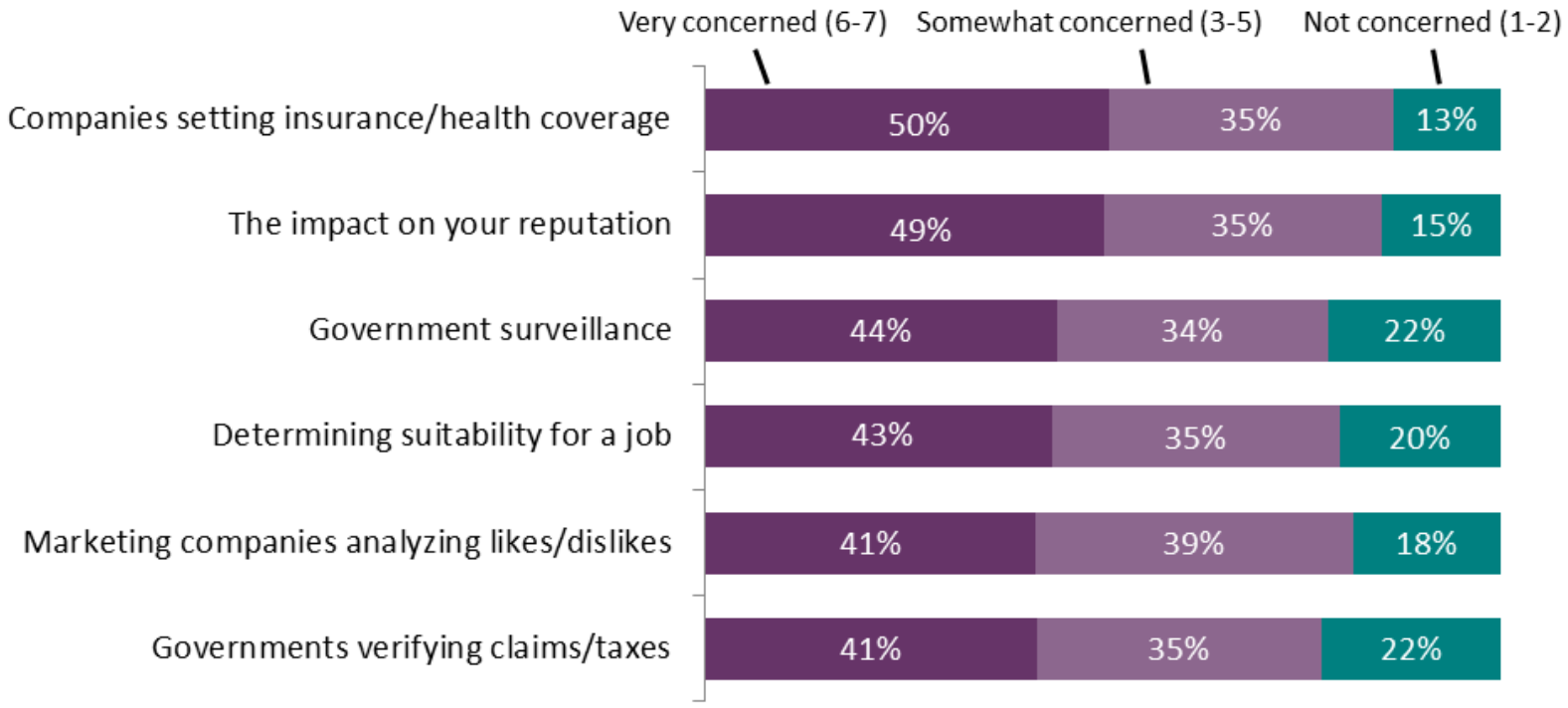
How concerned are people about online privacy?

- Survey of Canadians on Privacy-Related Issues (Privacy Commissioner 2014)
  - The poll found that nine in 10 Canadians were concerned about privacy. One in three (34%) said they were *extremely* concerned – up significantly from 25 percent in 2012.
  - "they are concerned about many privacy issues, for example, data breaches, identity theft, digital privacy and warrantless access to personal data held by telecommunications companies"
  - A significant majority (78%) expressed concern about how personal information about them online might be used in the context of government surveillance.

Implications for marketers of privacy concerns

- The poll Survey of Canadians on Privacy-Related Issues (Privacy Commissioner 2014) showed how people are changing behaviour
- Almost eight in 10 people surveyed (78%) have become less willing to share their personal information with organizations
- More than three-quarters (77%) had refused to provide an organization with their personal information at one point in time.
- 72 percent adjust settings to limit info sharing (compared to 40% in 2011);
- 75 percent have decided not to install an app because of concerns re. the personal information requested (compared to 55% in 2011); and
- 58 percent have turned off location tracking because of privacy concerns (compared to 38% in 2012.)
- Eight in 10 (81%) are more likely to choose to do business with a company specifically because it has a good reputation for privacy practices.

Concern about How Online Personal Information Might be Used



Q: When you think about the information available about you online, please tell me how concerned you are about each of the following?

Base: Internet users; n=1,272
DK/NR=2%

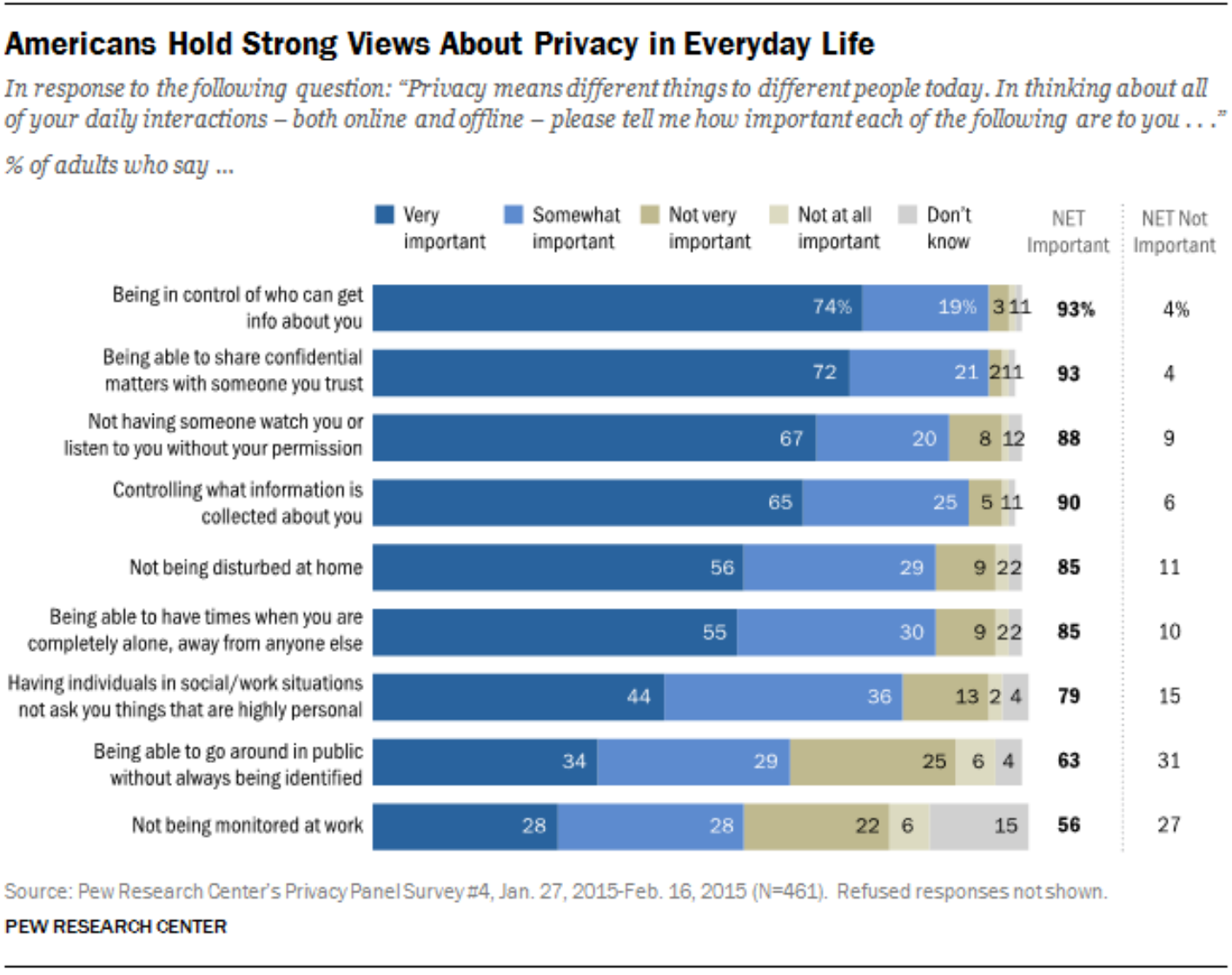
Phoenix SPI for OPC; November 2014

https://www.priv.gc.ca/information/por-rop/2015/por_2014_12_e.asp#fig4

2013 survey data re privacy from Pew

- Anonymity, Privacy, and Security Online – Pew Internet (September 2013)
- Security concerns continue to rise
- 86% of internet users have taken steps online to remove or mask their digital footprints
- 55% of internet users have taken steps to avoid observation by specific people, organizations, or the government.

Research from May 2015 shows privacy still a big deal



The “creepy” factor in social listening

- Jay Baer discusses the double edged sword of social listening
  - Short video
- “42% of consumers expect brands to respond to positive comments in social, but 43% say social listening invades privacy” from Social Listening V. Digital Privacy (JD Power)

What about marketing ethics and online privacy?

- The evolution of default privacy settings on Facebook over time (2005 – 2010)
- Not just what users do *on* Facebook. *Like* buttons on 3rd party websites have always been tracked, but now that data will also be sold to advertisers
- Facebook's "emotional contagion" research – "Facebook is learning the hard way that with great data comes great responsibility"
- How to control Facebook Ad Tracking

LEGAL PROTECTION OF ONLINE PRIVACY / SPAM PREVENTION

Legal Protection of Internet Privacy

- A major concern of Internet users is that their personal data is used only for the purpose it was provided
- Legislation in Canada
  - PIPEDA (*Personal Information Protection and Electronic Documents Act)*
  - All businesses and other organizations had to comply by Jan 1, 2004
  - Covers the "Collection, use or disclosure of personal information by organizations in the course of commercial activity."
- Note this is federal legislation – there is also provincial-level privacy legislation

Privacy requirements

- Information about an identifiable individual
  - Name, address, gender, age, ID numbers
  - Sensitive information (religion, union affiliations, sexual orientation, medical records etc)
- Identify purpose for which info is being collected
- Knowledge and consent of individual is required
- Use only for the purpose for which it was collected
- Keep it secure
- Make public your policies and practices about how private information is deal with

Privacy Policies

- Organizations carry out this legal requirement by providing information in privacy policies
- Policy must address information collected automatically from (for example) log files and cookies, as well as personal information actively provided by the user
  - Example: Instagram's Privacy Policy
- Privacy with respect to mobile devices and now wearables must also be incorporated into policy and practice for organizations

What about SPAM in social media?

- CASL (Canada's Anti-Spam Legislation)
  - Passed December 2010 (after many years in development)
  - Sections covering "commercial electronic messages" came into force July 1, 2014
  - January 15, 2015, sections of the Act related to the unsolicited installation of computer programs or software come into force.
- This is very comprehensive and stringent legislation
- Penalties: up to $1,000,000 per violation for individuals and up to $10,000,000 for corporations
- Private rights of action after 1 July 2017 – ie. recipients can sue

http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html

CASL prohibits (amongst other things…)

- The sending of **commercial electronic messages** without the recipient's consent (permission), including messages to email addresses and social networking accounts, and text messages sent to a cell phone

http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html

What is a “commercial electronic message”?

- A commercial electronic message (CEM) is defined as
  - a digital message sent to any electronic address (i.e. email address, social media account, text message)
  - that promotes or advertises a product, person, event, investment, or business.
- So if there is any commercial activity tied to the message it would be considered a CEM under CASL.
- This applies to **individual messages** as well as bulk messages (very different from typical anti-spam legislation)

http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html

What's an electronic address?

- "A typical advertisement placed on a website or blog post would not be captured."
- "Whether communication using social media fits the definition of "electronic address," must be determined on a case-by-case basis, depending upon, for example, how the specific social media platform in question functions and is used."
  - "For example, a Facebook wall post would not be captured."
  - "However, messages sent to other users using a social media messaging system (e.g., Facebook messaging and LinkedIn messaging, Twitter DM), would qualify as sending messages to "electronic addresses."
  - "Websites, blogs and micro-blogging would typically not be considered to be electronic addresses."

http://www.mondaq.com/canada/x/319300/Social+Media/Canadas+AntiSpam+Law+And+Social+Media+Marketers+Advised+To+Proceed+With+Caution

Consent is really important

- You can legally send CEMs only with the full CONSENT of the recipient
  - Express consent: Direct, positive opt-in (absolutely no pre-checked boxes) - remains in force until the customer opts out
  - Implied consent – exists where there is a previous business relationship – BUT expires after 2 years – then Express consent is needed to continue sending messages
- Consent difficult to get on social media – a Like or Follow does not (according to the Competition Bureau) imply consent

A Quick Guide to Understanding Canada's Anti-Spam Law and Social Media Compliance (2015)

So how does this apply to social media?

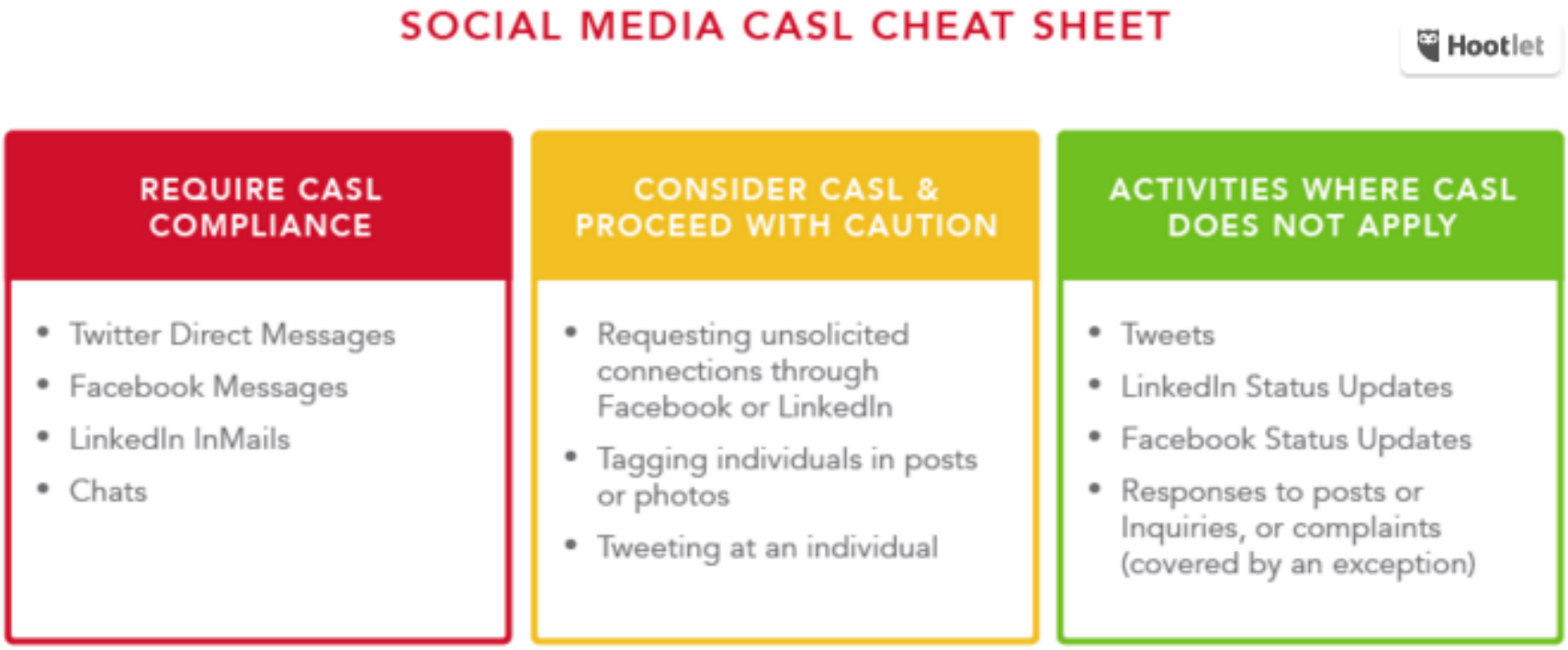
- CASL covers messages that are:
  - **direct** – ask yourself how is this message getting to someone?
  - and **commercial** in nature, that is: "encourage[s] participation in a commercial activity"
- A DM on Twitter saying "thanks for the follow" would be ok
- What would **not** be ok: a DM, @username mention or @username reply to a customer who had complained on twitter offering an apology and a discount on next purchase

www.clickz.com/clickz/column/2348625/casl-s-impact-on-email-marketers?

Impacts on social listening

- Training social media teams on how to engage with consumers will become even more important
- Current social listening tools will still be ok but the consent requirements when dealing with inquiries, quotes or complaints will need to be understood
- Messages will need to be tailored in a non-commercial way Eg "We are sorry to hear you had a bad experience, can you contact our support team email with more details?“
- If CEMs are sent through social media, then they must comply with CASL (i.e. identify the sender, obtain consent and provide an unsubscribe mechanism).

www.clickz.com/clickz/column/2348625/casl-s-impact-on-email-marketers?



A Quick Guide to Understanding Canada's Anti-Spam Law and Social Media Compliance (2015)

THE REPUTATION ECONOMY AND PRIVACY

Social media and the social economy

- Online reputation dashboard
  - "Real time stream of who has trusted you when and why"
- The currency of the new economy is trust. TED talk on collaborative consumption by Rachel Botsman (20 minute video)
- Implications of "reputation as a currency"?