Deloitte.

Privacy for sale – To the highest bidder

In today's "always-on" digital world, consumers have developed an interesting habit when it comes to sharing private data about themselves. Consumers are often quite willing to share their private data in exchange of receiving incentives, or simply as a matter of convenience when surfing online for products and services or using social media channels. This is despite the frequency of highly publicized breaches, cyber hacks and surveillance scandals.

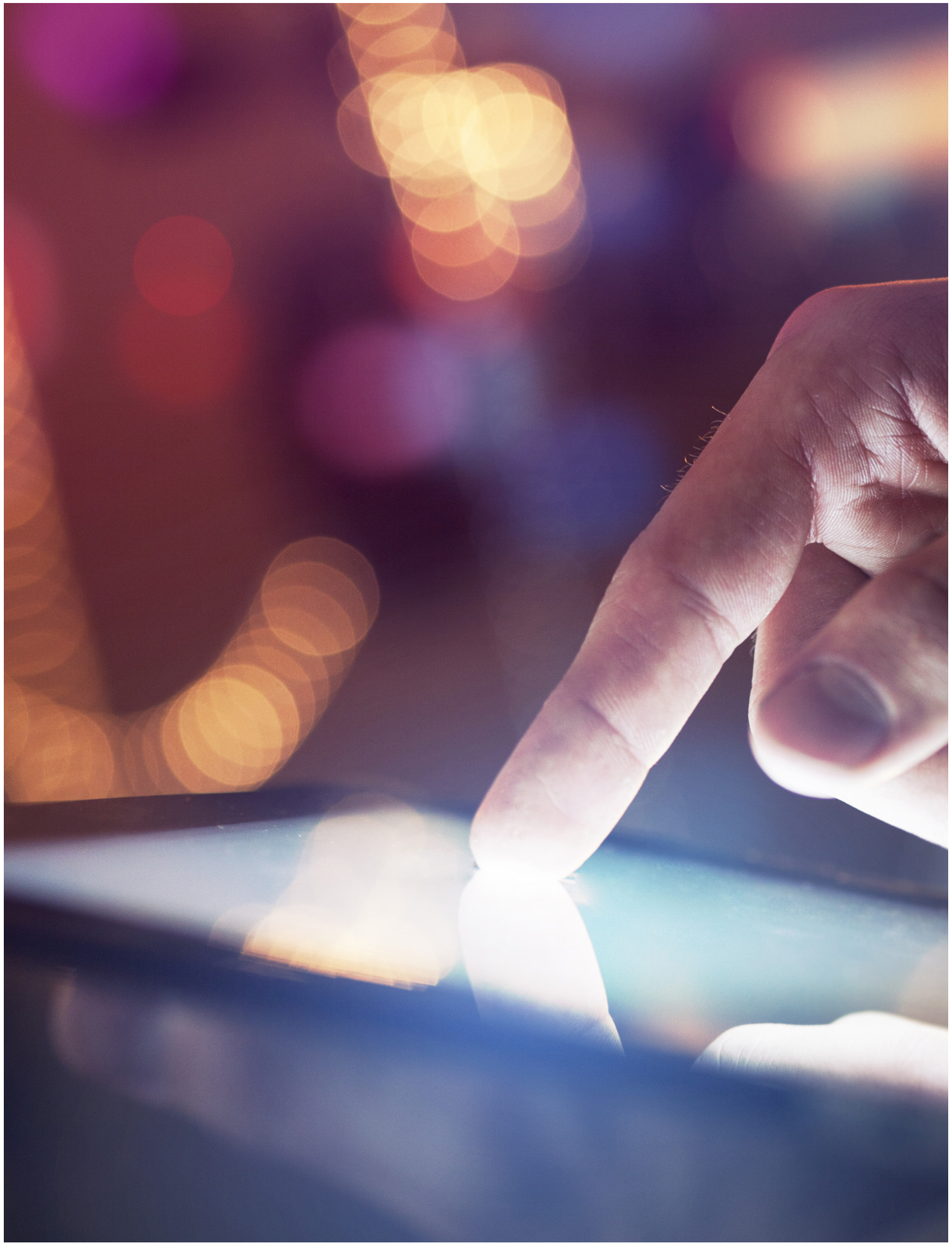
Legal use may not be ethical

While data protection and privacy laws exist to protect customer privacy, these rules can't keep pace with technology and evolving cyber threats.

Every jurisdiction has a different approach to implementing and interpreting its own set of privacy rules which often vary by country, and in many cases only provide a baseline for consent, permitted uses or disclosures and a right of recourse in the event of a breach.

"With big data comes big responsibility, and organizations not only need to do the right thing, they need to show their customers that they are doing it."

Pam Snively
Chief Data & Trust Officer | TELUS



Navigating the grey zones

Privacy laws may not always neatly align with cultural norms, values and expectations which can amplify the need for a global standard for ethical and sustainable data protection practices in our data saturated world.

As a result, companies often find themselves navigating "grey zones", left to their own devices when it comes to defining what it means to be "ethical" and "responsible" in their data use. Ultimately it's not about what you can or cannot do with the data within the confines of the law, it's what companies "should" do.

To better understand this ethical threshold—and the potential consequences for breaching it—Deloitte conducted a global survey of approximately 6,000 individuals across six different countries—namely, Canada, Chile, Germany, Japan, UK and US—to gain insights into how citizens view and value data privacy.

Deloitte conducted a global survey of approximately 6,000 individuals across six different countries—namely, Canada, Chile, Germany, Japan, UK and US.

Unethical behaviour is punished

The results revealed that most consumers didn't pay much attention to how their information was collected and used by companies and governments, because they simply *trusted* that their data was being used in a manner that aligned with their ethical expectations.

Although these expectations varied depending on where the consumer lived or the type of industry we asked about, the response to a perceived breach of consumer trust was virtually universal: **86% of respondents said they would be very or fairly likely to sever ties with an organization if the entity (irrespective of sector) used data unethically**.[1] This has both business and reputational implications if you measure the cost of a privacy breach against the cost of a customer acquisition—which can range from five to 25 times more than retaining an existing customer.[2]

Yet walking this ethical tightrope doesn't have to be a challenging task if businesses and government take a proactive approach to data privacy. This requires considering customer expectations upfront when it comes to using their data – an increasing trend called "privacy by design" and "privacy by default". This simply means baking in privacy considerations into Big Data initiatives by being transparent and open about secondary data uses and making responsible choices to respect and protect the personal information and data organizations are entrusted with.

Breach of trust can be measured in loss of business

The majority of respondents admitted that, on a day-to-day basis, data privacy was not top-of-mind. On average, 53% said they were not very familiar with regulations surrounding data privacy, and 20% said they were not familiar at all.[3] A brand's privacy policy was one of the lowest purchase drivers (1%), and only 5% believed data privacy should be among their federal government's top priorities over the next four years.[4]

Despite this, 80% of respondents believed corporations and governments have an ethical responsibility with respect to the data they collect from the public.[5] And, in Canada at least, there's an inherent trust that companies are upholding these ethical obligations—particularly those that are in highly regulated industries such as banks (80%), healthcare (79%) and insurance (69%).[6] Break that trust, and 90% of Canadian respondents said they would sever ties with an organization if it was revealed that the company used data unethically.[7]

This apparent Catch-22—where customers are unwilling to define their data and privacy expectations or conduct their own due diligence, but are nevertheless willing to punish companies that they perceive to be unethical—puts businesses in a difficult position. The loss of customers can have enormous consequences—including long-term brand and reputational damage, increased customer acquisition costs, reduced revenue growth and higher operational costs. Add in the growing prevalence of privacy breaches in today's data-centric business environment, and the possibility of having perceived unethical behaviour leaked to the public is on the rise.

In the face of this new reality, organizations hoping to maintain their customer base—and effectively navigate the next inevitable data breach—must ensure that their data and privacy frameworks are not only compliant and secure, but ethical as well. This is particularly critical as the advent of newer, smarter technologies, and the proliferation of digital channels, give organizations unprecedented access to vast amounts of consumer data—including traditional data (culled from online and mobile transactions); non-traditional data (collected through such things as sensors, wearables and smart devices); and unstructured data (email, text messages and secondary sources such as photos and social sites).

About the survey

In the summer and fall of 2016, Deloitte—with the help of a research provider—interviewed approximately 1,000 individuals in each of six different countries (Canada, Chile, Germany, Japan, UK and US). In each country, targets were set by age/gender and region such that the responses were nationally representative of the general population 16 years of age and older.

The survey was designed to uncover consumers' views of data and privacy, and explored a wide variety of topics, including: consumer familiarity with data privacy legislation and associated legal responsibilities; depth of understanding surrounding the concept of Big Data; and the impact of data and privacy views on purchasing behaviours. The survey also explored how consumer trust differs according to industry (automotive, insurance, healthcare, retail, telecom, banking, government and technology), as well as how consumer comfort levels were impacted by different data and privacy-related scenarios.

Figure 1. Familiarity with legal regulations

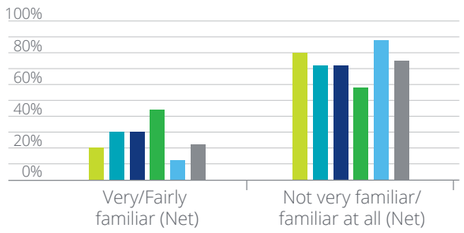
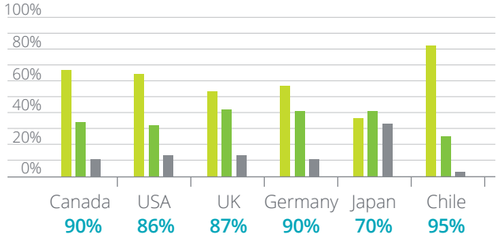


Figure 2. Impact of misuse of customer data

In each of the six countries, there is a significant penalty to be paid by companies that use customer data contrary to ways in which customers have agreed to. Japanese respondents, are once again, slightly more forgiving in this instance.



Results from our survey reveal the term “ethical” means different things to different people.

What do customers care about?

Devising an ethical guideline to govern corporate data collection and use is a complicated task—particularly because results from our survey reveal the term “ethical” means different things to different people. Given the indifference exhibited by most consumers, simply providing a detailed and accurate privacy policy isn’t sufficient—as only 55% of respondents said they ever read privacy policies before making online purchases.[8]

Despite this, our survey showed certain geographical markets and age groups shared common ethical views—and similar expectations surrounding the management of data. It’s also interesting to note that consumers’ comfort levels changed depending on the scenario in which they provided their data. This suggests consumer views on data and privacy aren’t completely reliant on the individual—and there may, in fact, be common patterns to uncover.

Not all channels are created equal

In general, consumers were most comfortable providing personal data in-store—with 57% saying they’d prefer this option over telephonic data collection, and 41% saying they’d prefer in-person over online.[9] Just over 42%[10] said they provided information in-store always or most of the time, even though 45%[11] believed it was not beneficial to them.

Although less willing to divulge personal information online, more than 83% said they often or sometimes buy products or services online.[12] And while many rarely or never read online privacy policies, they still checked the box and agreed to them—with 67% saying they somewhat trusted the privacy policies they agreed to, and 24% saying they completely trusted them.[13]

These behaviours seem to indicate that, while customers aren’t completely comfortable giving their personal information away, they’re reluctantly willing to do so if it allows them to transact conveniently—even if there’s no other perceived benefit.

Data must be stored domestically

Consumers were adamant about where their data is stored. Of the Canadians surveyed, 72% said they would be uncomfortable if their data was stored on a server outside of their home country.[14] The same percentage of Canadian respondents said not even added incentives, such as a 25% discount on a product or service, would alleviate this discomfort.[15] This strong response—which was held relatively equally across all six countries—indicates that most consumers expect the organizations they do business with to store their data domestically, regardless of what is outlined in the organizations’ privacy policies.

A moving target

Consumer expectations of personal privacy, and their willingness to impart personal information, are shaped by a number of different factors—including cultural norms, political climate and history—and therefore take on different meanings across geographic locales, generations and even industries.

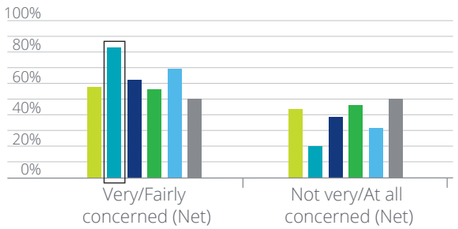
For example, Americans tend to be more distrustful of their government than other countries when it comes to the collection, storage and use of their data. Canadians are most likely to place trust in their government. Japanese respondents, on the other hand, are more concerned than most with businesses collecting, storing and using their data (see Figure 3).[16]

These discrepancies illustrate that different markets and demographics have different opinions of “unethical behaviour”, which is something to be wary of—particularly when expanding into new markets.

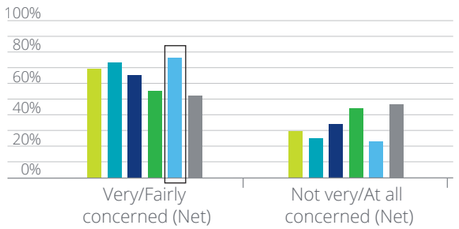
Figure 3. Data collection, storage and use—Government & company

Americans appear to be more concerned than others with government collecting, storing or using their data; while Japanese respondents are slightly more concerned than others with companies doing the same.

Government Collected



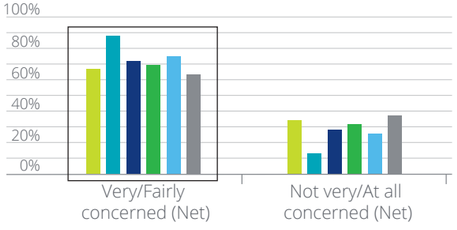
Company Collected



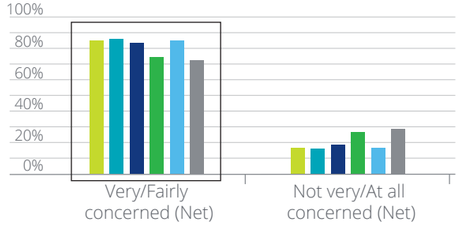
Government Stored

Company Stored

Government Used



Company Used



Value exchange

While most consumers were generally uncomfortable—but nevertheless willing—to share their personal information, that discomfort was alleviated if they were offered something in return for their efforts.

Our survey presented respondents with 10 different scenarios, each of which offered a reward in exchange for personal information. In the majority of cases, respondents were much more comfortable giving their information away—and much more open to ethically questionable practices—if there was a financial or social benefit.

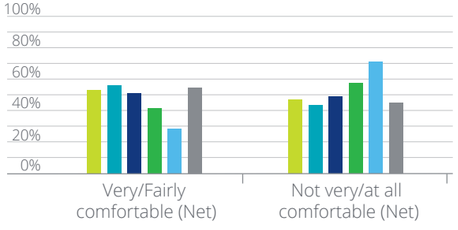
For example, when it came to collecting data to benefit the social good, most consumers were on board. Globally about half of respondents said they were very/fairly comfortable with the government using location data from mobile phones to help locate people in arrears for child support payments,[17] and 61% were willing to divulge their health history to help find a cure for deadly diseases.[18] 64% were even comfortable with police using court orders to unlock and access cellular phones of suspected (but not yet convicted) criminals.[19]

Additionally, ethical standards were loosened when some form of financial gain was involved. Consumers in most countries were okay with companies accessing their personal information if it meant they received something in return—such as free coupons from a preferred brand (57%),[20] movie/TV show suggestions from their video streaming service (57%),[21] or notifications of retailer deals/offers from a search engine, if the retailer in question was the subject of a search (55%).[22]

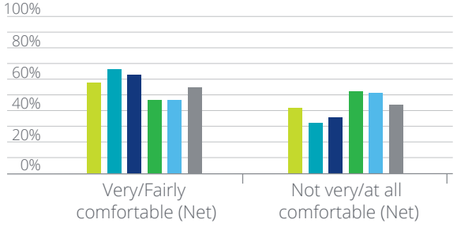
Figure 4. Data provision scenarios

Americans appear more comfortable, on average, with providing more personal data in order to receive a personal benefit. Germans and Japanese, on the other hand, are more likely to be guarded.

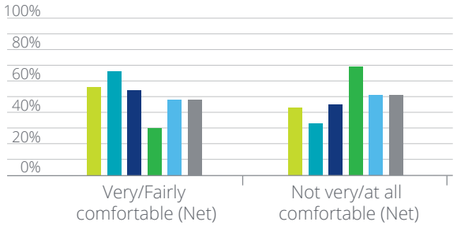
Government uses location data from mobile phones to help locate individuals who are in arrears for child support payments in order to enforce payment

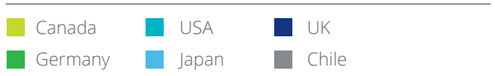


A video streaming service suggests movies/TV shows that might interest you based on previous viewing habits

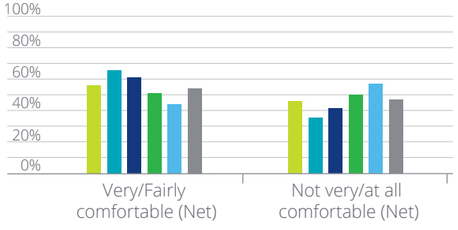


An energy company provides its customer data to a company specializing in data analytics in order to help improve overall efficiency of customer service

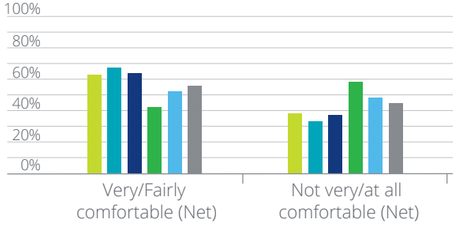




A search engine automatically suggests deals/offers on retailers as you enter them



A brand of cookies automatically sends coupons to people who have bought their brand in the past month



When it came to collecting data to benefit the social good, most consumers were on board

50% said they were very/fairly comfortable with the government using location data from mobile phones to help locate people in arrears for child support payments

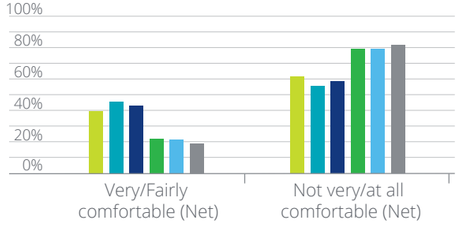
61% were willing to divulge their health history to help find a cure for deadly diseases

64% were comfortable with police using court orders to unlock and access cellular phones of suspected criminals

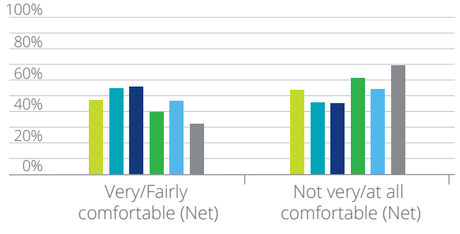
Data provision scenarios

There is an interesting perceptual difference across Canada, the US and the UK, compared to Germany, Chile and Japan in terms of many of the scenarios assessed.

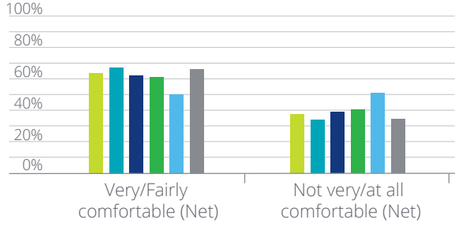
The company you work for monitors the websites you visit on company computers/phones



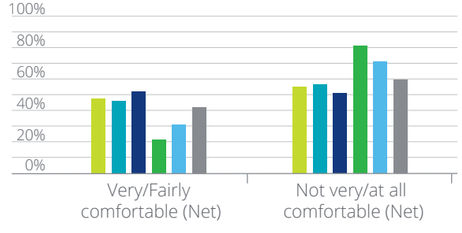
An internet content provider free content shows advertisements between content



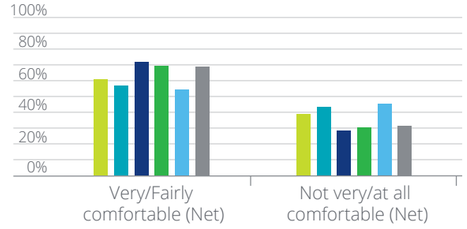
Your health history is used in a clinical research study that is aimed at finding a cure for deadly diseases



Your cellular monitors your call history in order to provide you a discounted rate on frequently called numbers



Police use court orders to unlock and access cellular phones of suspected criminals



Consumers in most countries were okay with companies accessing their personal information if it meant they received something in return

57% free coupons from a preferred brand

57% movie/TV show suggestions from their video streaming service

55% notifications of retailer deals/offers from a search engine, if the retailer in question was the subject of a search

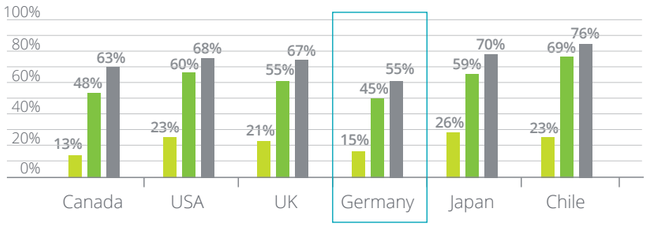
However, the most interesting responses came in regards to a potential personal financial gain. When asked how comfortable respondents would feel if an insurance company monitored their social media feeds to set insurance rates, only 20%, on average, were comfortable with the idea. Yet, if that same insurance company offered a 25% reduction in rates in exchange for social media data access, 56% of respondents said they would be comfortable with providing the information. In a scenario where consumers received a 50% reduction in rates, over 67% of respondents said they would be comfortable.[23]

In almost all the value exchange scenarios, German respondents were the least comfortable with providing their personal information—and only 55% said they would be willing to divulge their social media information in exchange for a 50% insurance rate reduction. Chile was generally on the other end of the spectrum, with 76% of respondents saying they would be comfortable providing information in exchange for a 50% reduction in insurance rates. This again highlights the cultural perceptions at play when it comes to how data is used for mass marketing, and how global brands need to tailor their campaigns to suit a local audience.

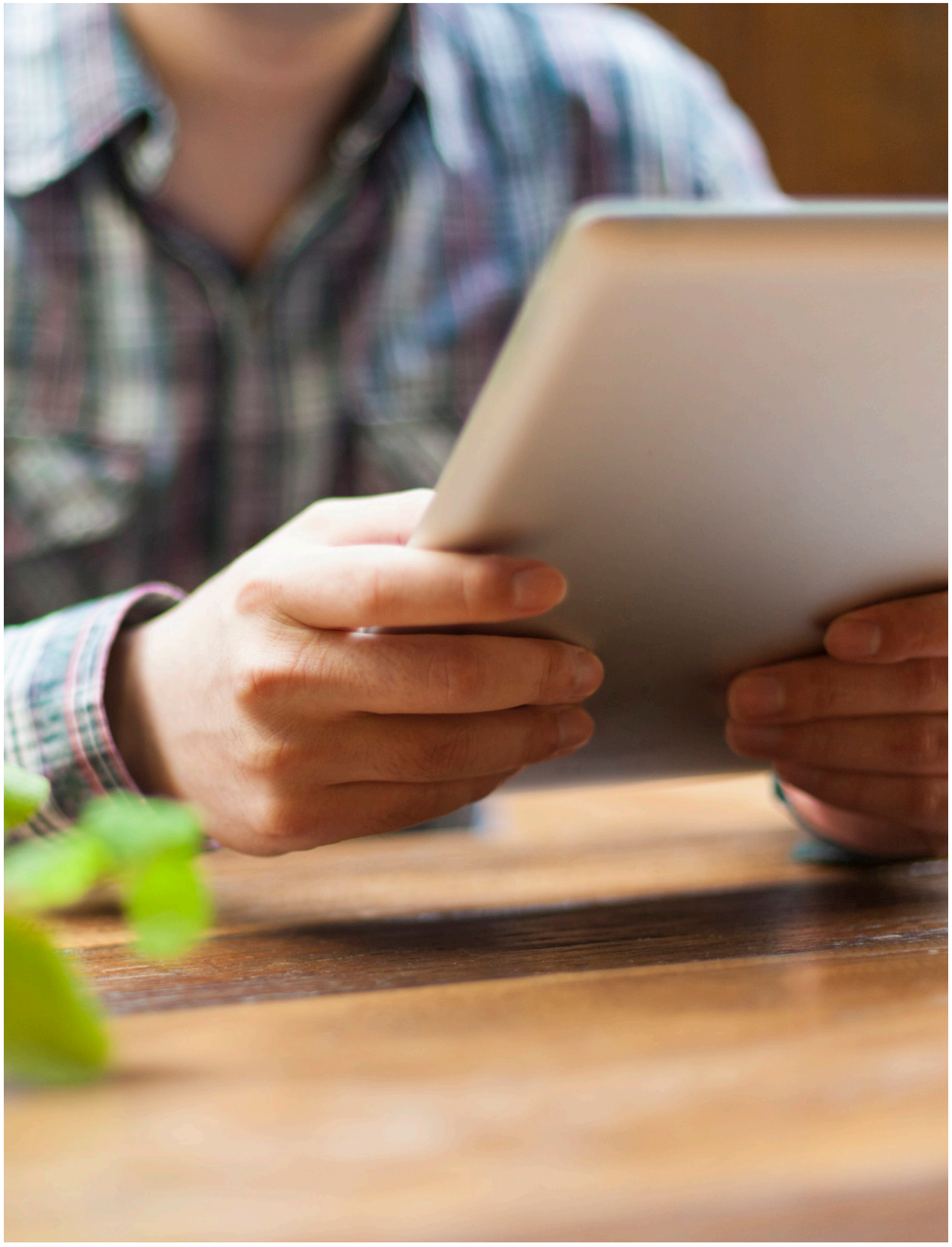
Figure 5: Insurance company scenario—with incentives

Regaldless of nationality, all respondents are willing to offer increased accsses to one's personal life for increased financial benefit. Not surprisingly, Germans have the lowest willingness overall even at a substantial rate reduction.

An insurance company monitors your social media feeds/platforms in order to help set your insurance rates: Would your level of comfort become more positive if reduced rates by an average of 25%/50%



Base scenario
25% reduction
50% reduction



Could vs. should

In today's increasingly global business environment, the sheer quantity of available data is escalating, increasing the danger of data misuse. To effectively mitigate the risk of breaching stakeholder trust, organizations must devise a strong ethical construct to ensure employees are using data in a responsible manner.

"With big data comes big responsibility," states Pam Snively, "and organizations not only need to do the right thing, they need to show their customers that they are doing it." This involves articulating the organization's principles, beliefs and values and using them to create a well-defined ethical guideline with respect to data privacy. It also involves keeping the ethical position of their target market in mind—and adjusting their data collection and use in ways that honour these nuanced social behaviours.

Ultimately, by creating and promoting a company-wide culture that treats consumer data with integrity—and enforcing it with appropriate policies and procedures—savvy organizations will not only be able to preserve their customers' trust, they will also have the confidence to connect with those customers in new and innovative ways.

"Earning and maintaining the trust of customers is foundational to any business, which is why it's vitally important to protect their privacy and treat their data with respect. Canadians shouldn't be expected to blindly trust organizations, so there must be demonstrable governance processes to show that respecting customers' privacy is a top priority."

Pam Snively
Chief Data & Trust Officer | TELUS

Endnotes

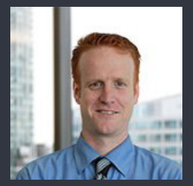
1. Question: If you found out that an organization that you had actively provided data to was using data in a way that was contrary to the usage that you agreed to, how likely would you be to sever your relationship with that organization?
2. Harvard Business Review, October 29, 2014. "The Value of Keeping the Right Customers," by Amy Gallo. Accessed at https://hbr.org/2014/10/the-value-of-keeping-the-right-customers on February 27, 2017.
3. Question: Overall, how familiar are you with laws and regulations in <country name> regarding data collection from the public and how that data is used?
4. Question: Importance in making decision about which brand of product you purchased; Important priorities for Federal Government in next 4 years.
5. Do you believe that government and companies have an ethical responsibility with respect to the data they collect from the public?
6. Question: To what extent do you trust each of the following types of organizations to use your information in an ethical way?
7. Question: How often do you read privacy policies online?
8. Question: How often do you read privacy policies online?
9. What differences do you feel there is between providing data in person versus providing data over the phone or online?
10. How often do you provide information in-store?
11. What is your opinion of the personal information provided in-store?
12. Which of the following statements best describes how often you currently buy products/services online?
13. To what extent do you trust the privacy policies you agree to?
14. How comfortable would you be with data that you have provided to a company being stored on a server outside of <insert country>
15. Would you be more comfortable with this scenario if there was a financial benefit offered to you, such as a 25% off your next purchase/service?
16. Generally speaking, how concerned are you about how your personal information is collected, stored and used by each of the following organizations? Government/Company – Collected, Stored, Used.
17. Question: Please indicate how comfortable you would be with the activities described in the scenario overall: Government uses location data from mobile phones to help locate individuals who are in arrears for child support payments in order to enforce payment.
18. Question: Please indicate how comfortable you would be with the activities described in the scenario overall: Your health history is used in a clinical research study that is aimed at finding a cure for deadly diseases.
19. Question: Please indicate how comfortable you would be with the activities described in the scenario overall: Police use court orders to unlock and access cellular phones of suspected criminals.
20. Question: Please indicate how comfortable you would be with the activities described in the scenario overall: A brand of cookies automatically sends coupons to people who have bought their brand in the past month.
21. Question: Please indicate how comfortable you would be with the activities described in the scenario overall: A video streaming service suggests movies/TV shows that might interest you based on previous viewing habits.
22. Question: Please indicate how comfortable you would be with the activities described in the scenario overall: A search engine automatically suggests deals/offers on retailers as you enter them.
23. Question: For each of the above scenarios, please indicate how comfortable you would be with the activities described in the scenario overall.

Contact

For more information about how to implement governance structure around the ethical use of data, please contact:

Anthony Viel
Managing Partner | Financial Advisory

anviel@deloitte.ca
416-452-8341



John MacLeod
Manager | Financial Advisory | Analytics

jmacleod@deloitte.ca
416-643-8438

Acknowledgements

Tamara Dinelle
National Marketing Lead | Analytics

tdinelle@deloitte.ca

Swathi Sadagopan
Analyst | Financial Advisory | Analytics

ssadagopan@deloitte.ca

Notes

Notes

Deloitte.