Cyber Security Post Equifax: Perceptions and Priorities from Massachusetts Residents

December 2017

A MA Public Opinion Report produced by Mass Insight Global Partnerships and BW Research Partnership for the Advanced Cyber Security Center

Table of Contents

1 CYBER SECURITY POST EQUIFAX

1.1 INTRODUCTION

In light of the recent Equifax cyber security breach and the ever-increasing need to protect digital assets in today's computerized economy, the Advanced Cyber Security Center asked Mass Insight and BW Research to conduct a survey of Massachusetts residents and a report to better understand public opinion on consumer and privacy matters and cyber security related to the Internet.

This study is built upon an online survey produced by Opinion Dynamics Corporation of 450 Massachusetts residents 18 years or older. Mass Insight and Opinion Dynamics had conducted earlier surveys in 2000, 2001 and 2015 on these issues which provide a basis for tracking changes in public responses. The objectives in this survey were to assess residents' perception of the cyber security landscape regarding:

- The Internet and electronic records;
- Personal data privacy concerns;
- National standards and the role of the federal government;
- Changes in behavior due to cyber-crime and cyber security incidents.

The key themes that emerged from the research findings include;

- ***People believe the Federal government should set tougher standards for managing and protecting electronic records.***

Policy and regulation currently lag behind a wave of cyber threats that continuously evolves and adapts. While the exact solutions might be complex, Massachusetts residents are clearly voicing concerns that the federal government should set stronger standards for technology and data companies to protect personal data. The ever-expanding world of digital interconnectivity brings significant benefits for consumers. However, with these advantages comes a shared responsibility to protect personal data, for consumers to carefully monitor what personal data they provide and for companies to protect consumer data they hold from cyber security threats. Massachusetts consumers are deeply concerned about the privacy of their personal data and believe the federal government should play a stronger role in assuring their data is protected.

- ***Most Massachusetts residents say they are unlikely to continue to do business with an organization that suffers a breach involving personal data.***

Still, despite widespread coverage of the Equifax cyber security breach, many residents accept the damage caused by breaches as merely a cost of using the Internet.

- ***Massachusetts residents believe that benefits of the Internet and its myriad of uses are greater than the threats associated with privacy and cyber-crimes.***

While this study focuses on the privacy concerns and possible costs of having information stored electronically, approximately two out of three residents believe the benefits of the Internet and its myriads applications provide a greater value than the potential threats to privacy from cyber-related crimes.

1.2 KEY FINDINGS

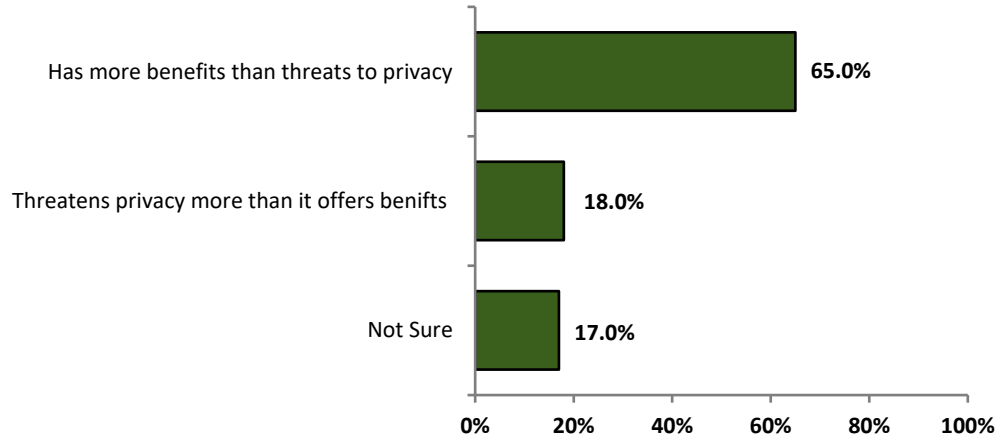
Based upon primary survey research, the research team identified the following key themes and findings.

1.2.1 Despite Concern, Residents Are Unaware of or Believe They Were Not Impacted by Breaches and Say the Internet and Electronic Records Benefits Outweigh Risks

Most residents believe they were unaffected by the recent Equifax breach. Only 22 percent of residents believe that their personal credit information has been affected by the breach, while 49 percent say that their personal credit information has not been affected. Thirty percent of residents were not sure if their personal credit information has been affected.

Overall, the Internet provides residents with more perceived benefits than the potential privacy costs posed by cyber security threats according to the survey. Sixty-five percent of Massachusetts residents hold the opinion that the Internet benefits outweigh threats to privacy, up from 56% in 2000, while only 18 percent believe that Internet usage and electronic record threaten privacy more than they offer benefits.

Figure 1: Resident Survey – Benefits vs Costs of Internet and Electronic Records



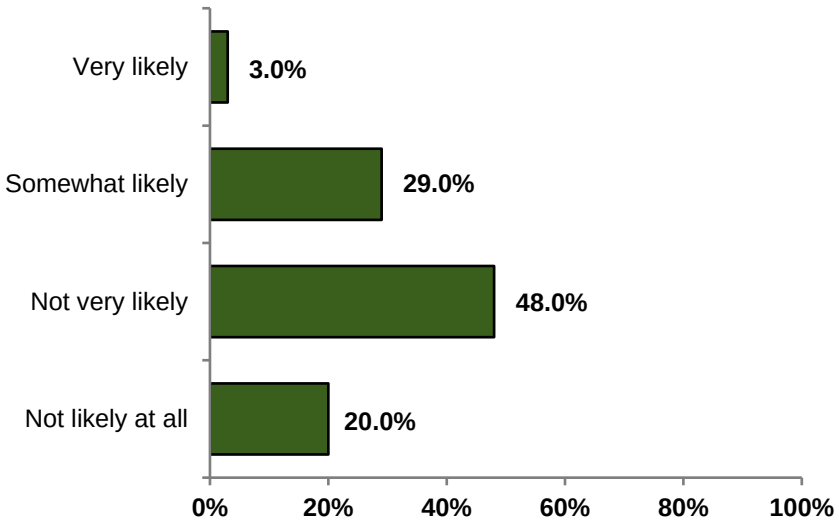
Interestingly from an ideological standpoint, 71 percent of "conservative" residents and 75 percent of "liberal" residents agree that internet usage and electronic records benefits outweigh threats to privacy, exhibiting an emerging cyber consensus amongst traditionally opposing groups. Household income is an indicator of whether or not individuals are more likely to find the benefits greater than threats to privacy. The majority of residents making more than $60,000 of income (72 percent) believe that the Internet provides more benefits than threats to privacy. Residents making less than $60,000 of income project more uncertainty with only 57 percent believing that internet usage and electronic records provide more benefits than threats to privacy.

On a related issue, residents agree that the benefits of electronic medical records outweigh threats of unauthorized use. Seventy-eight percent of residents say that computerized medical records should be encouraged because this digital form is more easily accessible to doctors when traveling and may permit more effective treatment; only 22 percent of residents believe that computerized medical records are vulnerable to unauthorized people and should be discouraged. Support has increased from 47% in 2000 when we asked the same question.

1.2.2 Consumers Report Deep Reservations Regarding Firms that Suffer Breaches

The majority of respondent's report that they are not likely to continue to do business with an organization that suffers a security breach and releases personal data, with 48 percent and 20 percent responding that continued business is "not very likely" and "not likely at all", respectively. However even after the Equifax security breach, 29 percent of resident's state that they are still "somewhat likely" to continue doing business with an organization that suffers a security breach.

Figure 2: Resident Survey – Likelihood of Continued Business with Organization That Suffers Cyber Security Breach



Free credit reports provide potential hazards to personal data security. Sixty-three percent of Massachusetts residents respond that they have received a free credit report and did not detect identity fraud in the process. Only 6 percent state that they have detected identity fraud in the past.

Early monitoring and rapid preventative action are important techniques to protect personal credit information. Thirty-four percent of residents report that they have enrolled in a credit monitoring program. Additionally, 18 percent of residents said that they have put a freeze on credit reports at reporting agencies when there was suspicion that the security of their personal credit information was compromised. Nearly half of residents respond that they have not taken action to protect personal credit information.

1.2.3 As Residents' Use of the Internet Continues to Increase, Real Concerns About Data Privacy and Protections for Consumers Grow

Not surprisingly, people report dramatically increased internet usage since 2000 and even 2015, for a variety of uses.

Figure 3: Resident Survey – Frequency of Connecting to the Internet More Than Once a Day

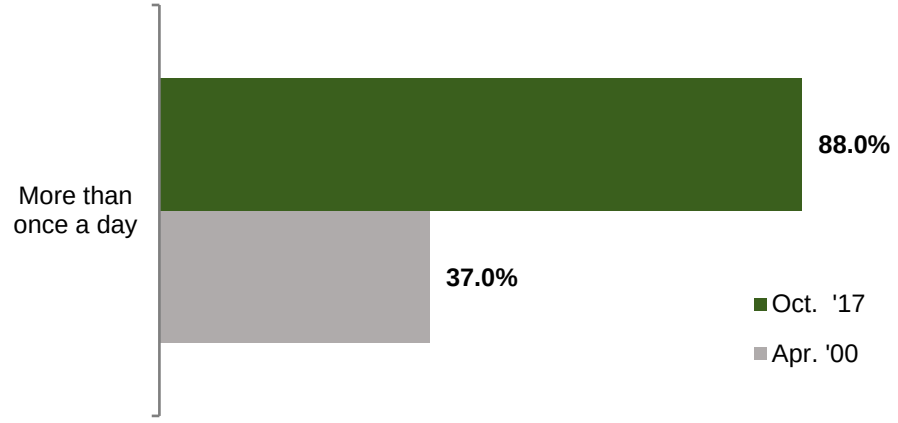
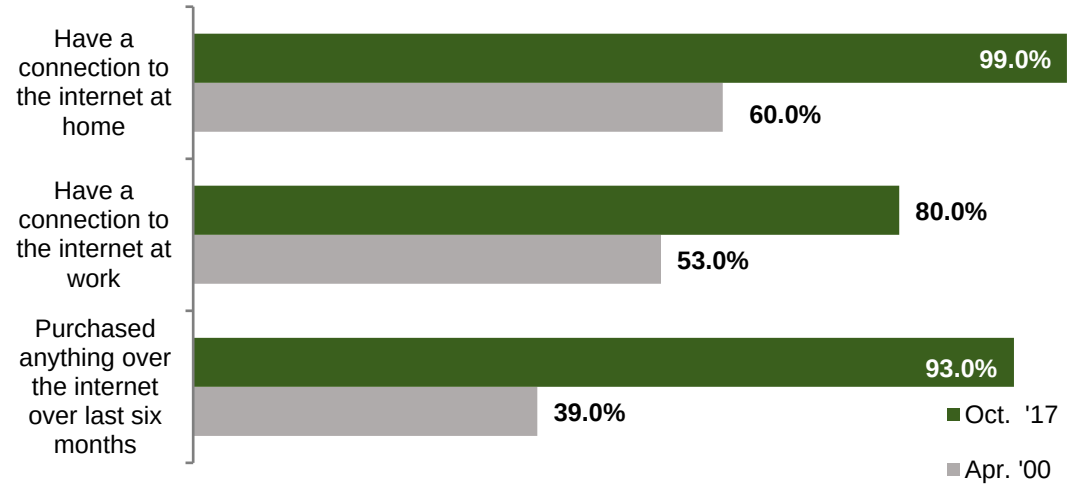
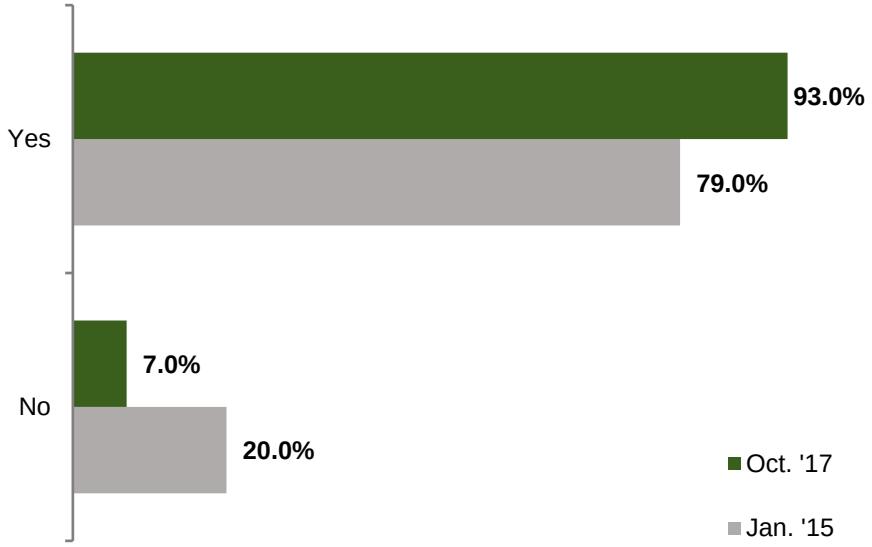


Figure 4: Resident Survey – Internet Usage Present vs. Past – 2017 versus 2000



When asked about the level of concern regarding the privacy of their personal information, 53% percent of residents overall report that this is a "major concern" and with 36 percent saying it is "a concern" or 89% overall. About 80% indicated concerns in 2000 and 2001, with 75% in 2015.

Figure 5: Resident Survey – Purchases Made on the Internet Over the Last Six Months – 2017 versus 2015

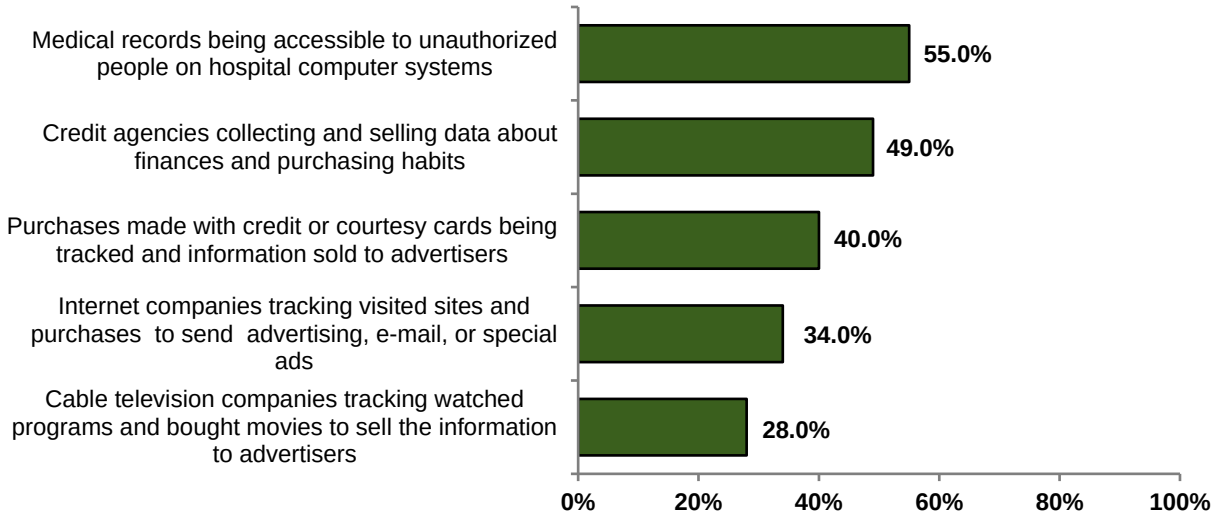


Residents were also asked for their thoughts on a number of specific cyber privacy issues and their level of concern. In general, they are more comfortable with targeted marketing based on tracking of their Internet or movie purchases and most concerned with medical privacy and their financial and credit data being shared without their permission. For all of these privacy concerns, older residents are more likely to be "extremely concerned" than younger residents.

- Despite the seventy-eight percent of residents now saying that computerized medical records should be encouraged, unauthorized use of their medical records leads the list of specific areas of concern, with fifty-five percent of residents "extremely concerned."
- After medical records, credit information is of most concern, with forty-nine percent of residents saying they are "extremely concerned" that credit agencies are collecting and selling data about their finances and purchasing habits.
- Forty percent of residents are "extremely concerned" that purchases made with credit or courtesy cards are being tracked and information sold to advertisers.

- Thirty-four percent of residents are “extremely concerned” that internet companies are tracking sites and purchases to send advertising, e-mail, or special ads.
- Twenty-eight percent of residents are “extremely concerned” cable television companies are tracking programs being watched and movies being bought to sell the information to advertisers.

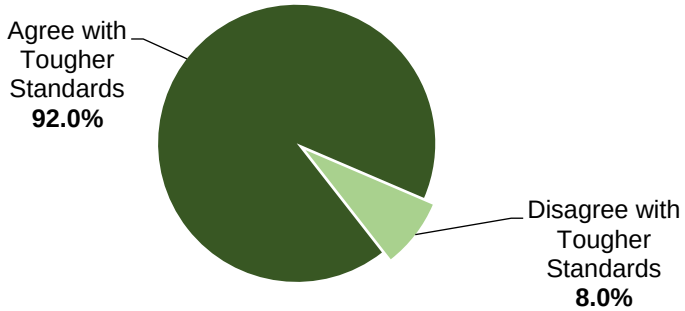
Figure 6: Resident Survey – Privacy Concern Cases (“Extremely Concerned”)



1.2.4 Massachusetts Residents Want Tougher Federal Standards

Residents overwhelmingly believe that the federal government should set tougher standards for technology and data companies to protect the personal data of American consumers with nine out of every ten residents in support. This level of support is consistent regardless of gender, age, education, or political affiliation.

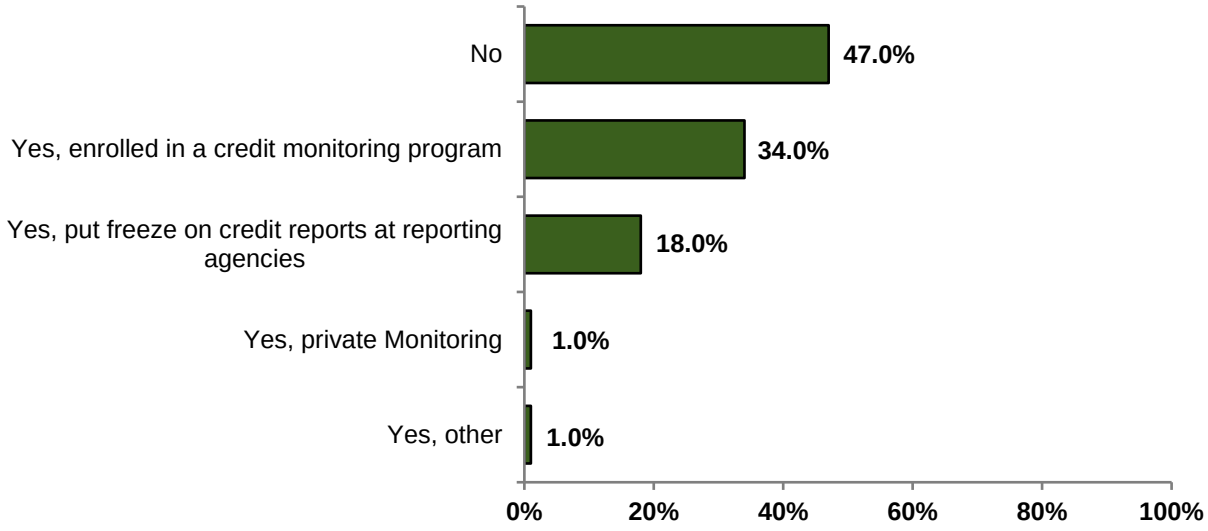
Figure 7: Resident Survey – Tougher Standards for Technology and Data Companies



1.2.5 Consumers Believe They Can Protect Their Own Data, Yet Few Actually Do

Eighty-seven percent of residents believe that they can control the security of their personal data "very well" or "somewhat well" if given the proper tools. However, when asked what steps they have taken to protect personal credit information, 47 percent of residents state that they have never taken any steps. While confidence in their ability to control the security of personal data seems to be high given the right tools, many residents have not yet taken steps to do so.

Figure 8: Resident Survey – Steps Taken To Protect Personal Credit Information



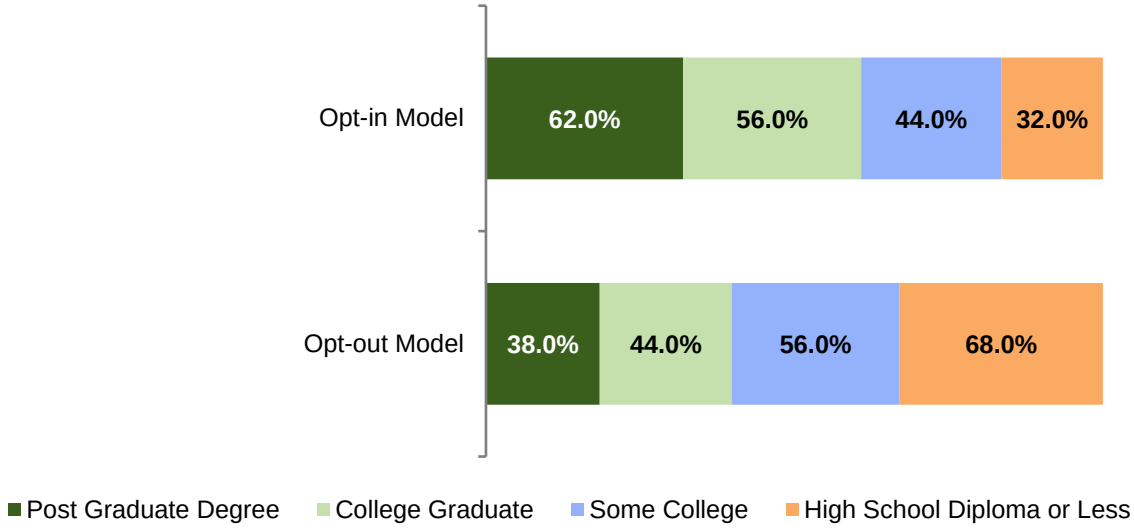
1.2.6 Online Consumers Are Unsure of How Their Data Should Be Collected

There are two basic consumer consent models that companies use when collecting consumer data, commonly referred to as the "opt-in" and "opt-out" models. The opt-in model does not collect consumer data unless consumers actively choose to authorize the use of the data, while the opt-out model collects consumers' data unless they actively choose not to authorize it. Residents are generally split on which model better ensures protection of personal data, with 48 percent believing the opt-out model is better for consumers and 52 percent believing the opt-in model is better.

Residents with higher levels of education are more inclined to favor the opt-in model with 62% of post graduate degree holding residents favoring it.

Sixty-eight percent of residents with a high school degree or less believe that the opt-out model is best for consumers.

Figure 9: Resident Survey – Consumer Consent Model Preference by Educational Attainment



2 CONCLUSIONS

The overwhelming majority of Massachusetts residents (92 percent) believe that there needs to be more attention dedicated to cyber security and tougher federal security standards for technology and data companies which collect and store personal data. At the same time, while residents say they are ready to use tools available for security, many have not done so and most seem to lack a foundation of knowledge about what is already happening to their data. Results of this study illustrate important trends and policy issues for the future including:

1. **What precautionary steps are consumers willing to adopt in order to minimize cyber threats?**

   Consumers appreciate the benefits of the Internet and at the same time would like to see improved and tougher standards for technology and data companies. But many have not yet taken personal precautions to protect their credit information and need better tools and more education to become partners in security. The majority of residents—over six in ten—believe that benefits of the Internet outweigh the potential threats to privacy. For consumers to become partners in securing their data, they need better tools. Nearly half of residents report they have not taken action to protect personal credit information, including enrolling in a credit monitoring program or putting a freeze on credit reports.

2. **Why are close to one third of consumers at least somewhat likely to continue do business with organizations that suffer breaches releasing personal data?**

   Consumers may not fully recognize the damage caused by the Equifax security breach – or conversely, some consumers are realistic about the recurring breaches that plague Internet-based businesses they deal with and willing to accept the risks for the benefits. Again, the public needs a clearer understanding of their risks and choices. While 48 percent and 20 percent of residents would respectively be "not very likely" and "not likely at all" to continue to do business with an organization that suffers a security breach and releases personal data, still 29 percent of residents are "somewhat likely" to continue doing business with an organization that suffers a security breach.

3. **Where should the cyber security agenda focus?**

   "Market me with purchasing choices based on my data, but don't sell my financial data without my permission or put my health records at risk." Consumers appear more comfortable with the benefits of targeted marketing using their purchasing data; medical data vulnerability and financial data being sold without their permission are their greatest concerns. Residents "extremely concerned" with cyber privacy cases drops off from vulnerable medical records (55 percent) and credit agencies selling data about personal finances (49 percent) to tracking of credit card purchases (40 percent), tracking by Internet companies of purchases (34 percent), and tracking by cable television companies to sell to advertisers (28 percent).

4. **What role should the government play in setting security standards for technology and data companies?**

   Almost all consumers agree that the federal government to set standards for technology and data companies that collect and use personal data. Ninety-two percent of residents believe that the federal government should enact tougher standards for technology and data companies to protect personal data. Solutions, however, will have to engage consumers and companies as partners. Government's role will need to consider how to create incentives for both consumers and companies to play their respective roles.

5. **What is the corporate role to educate consumers about the choices they face in sharing their personal data?**

   Consumers need clearer statements of how their personal data collection is being used and the value and risks that creates for them. Residents are generally split on which data collection models better ensure both value and the protection of personal data with 48 percent believing the opt-out model is better for consumers and 52 percent believing the opt-in is better for consumers. If online personal privacy is important to consumers, which this survey demonstrates it is, companies collecting personal data have a responsibility to provide clear and simple privacy statements and choices for consumers explaining how their data will be shared and why that's valuable for the consumer.