October 2016

PUBLIC OPINION STRATEGIES

EXECUTIVE SUMMARY

Public Opinion Strategies recently completed a national survey of voters which shows that American voters are increasingly concerned about the privacy of their information in the digital space, and indicate strong support for changes in how notifications of data breaches are provided and companies are affected by these hacks.

Overall, we found that…

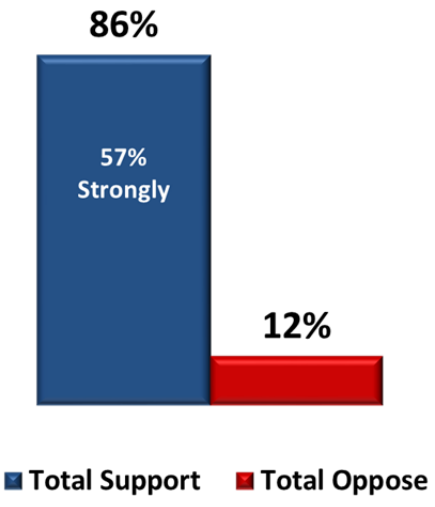
- Nearly half of Americans (45 percent) have been notified that their information could have been affected by a data breach.

- Voters are increasingly concerned about the security of their personal information while shopping on-line. Almost three-quarters (74 percent) say they worry "a lot" or "some" about the security of their personal information while shopping on-line. This is an increase of ten points from September 2014 when a CNBC survey found that 64 percent worry a lot or some about this. Somewhat fewer today worry about personal information security while shopping in person (64 percent).

- The vast majority think data breaches are inevitably going to affect major companies. Seventeen percent say that it is "inevitable," while another 63 percent say it will "probably" happen. Only 16 percent say that data breaches will only happen to companies which are negligent or incompetent in handling this information.

- There is overwhelming support for a single national notification standard, with 86 percent indicating support for this proposal. As we knew from previously held focus groups that many are not familiar with how notifications are required to be handled, we provided a brief explanation of the status quo prior to positing this proposal:

  "Today, there are varying state and local laws with different rules for how a company must legally notify customers of a data breach, based on where a customer lives. Three states have no rules at all. One proposal would create a single, national standard for notifying people of a data breach and holding companies accountable for keeping their customers' data secure."



Support for National Notification Standard:

As one can see, support is significant and intense, with a majority (57 percent) saying they strongly support this change.

Moreover, support extends across the partisan spectrum: 83 percent of Republicans, 77 percent of independents, and 93 percent of Democrats indicate support.

There is even strong support among those who have been notified in the past about a data breach (87 percent).

Moreover, voters side with supporters of such a standard, even after respondents hear rationales both in support and opposed to it. More than two-thirds - 68 percent - side with *"People who support the proposal say that a single standard would ensure customers are notified swiftly and with less confusion than with the current patchwork quilt of state requirements. For example, California's laws are in direct conflict with Massachusetts' law. And in one state a company has 90 days to notify customers, while in others it is significantly less."*

Only 26 percent instead prefer the view of *"People who oppose the proposal say that the peoples' elected state officials have the right to hold companies accountable as they see fit for the protection of their states' citizens. The federal government should not mandate a single, one-size-fits-all standard. That could mean some states end up with laxer requirements on companies than what they desire*."

- In addition, more than four-in-five (84 percent) support reining in investigations and lawsuits by ensuring that we have consumer protection laws that specifically address data privacy, and not allow government regulators and lawyers to rely on older laws. A mere 11 percent oppose this proposal.

  Again, we provided a brief neutral summary of the current situations prior to asking about this reform as follows: *"Currently, actions and lawsuits against companies following data breaches are being based on interpretations of consumer protection laws that were written well before modern technology was in place. One proposal would ensure that we have consumer protection laws that specifically address data privacy, and not allow government regulators and lawyers to rely on older laws*." Again, support is not only significant but also fairly intense as 45 percent say they strongly support only using laws specifically drafted regarding data breaches to apply to these cases.

- Voters say that companies who make investments up-front in cyber-security but still suffer a database breach should not be sued (70 percent). Similarly, three-quarters (75 percent) say that companies which respond afterward by quickly notifying its customers, providing free credit monitoring, and fixing the security problems in its systems also should not be sued.

- In fact, more than two-thirds (69 percent) say that they would "limit class action lawsuits to people who have personally suffered identity theft, fraudulent activity in bank or credit card accounts or other financial harm." Exposure would not constitute harm, therefore.

Bottom Line:

The survey clearly demonstrates overwhelming and consistent support for policies to reform how data breaches are handled in legal proceedings and by government regulators. This support is significant across partisan lines and among all key sub-groups. While American voters are increasingly worried about the security of their personal information, they also feel that most companies will be affected by hackers at some point. They feel that companies who are responsible prior to and following these data breaches should not be sued, and want to limit class action lawsuits to only those who have experienced direct harm, not just exposure.

Methodology: Public Opinion Strategies conducted a phone survey of 800 voters throughout the United States (480 interviews conducted on landlines, 320 on cell phones). The margin of error for this sample at the 95% confidence level would be +3.46%. Interviews were conducted October 7-12, 2016.