



TO: Interested parties
FROM: Purple Insights
RE: Recent polling results for ACT | The App Association
DATE: April 18, 2016

This memo summarizes results from a survey conducted by Purple Insights on behalf of ACT | The App Association. The survey includes 1,250 interviews of registered voters nationwide between April 11th and 14th, 2016. Respondents were randomly selected from a voter file. Fifty-eight percent (58%) of the interviews were completed with voters on landlines and 42% were completed with voters on their cell phones. The margin of error is +/-2.8%. The margin of error for subgroups is higher.

Key Findings:

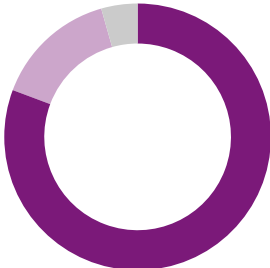
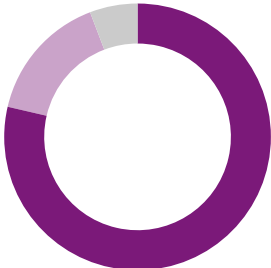
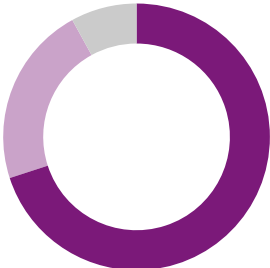
These survey results demonstrate that US voters strongly support robust encryption technology that keeps the information they store on their electronic devices and share online private and secure. More specific findings include:

- By large majorities, US voters recognize the need for strong privacy protections and data encryption to keep their personal information secure.
- Voters are very concerned about their personal information being accessed by cybercriminals and hackers and believe the threat is increasing.
- Few find current security protections adequate so voters believe tech companies need to continually strengthen data encryption.
- Voters worry that if universal encryption “backdoors” are created, it could be misused and make their personal data more vulnerable.
- Voters say they trust technology companies more than the federal government on data security.

Voters recognize the importance of strong privacy protections and data encryption.

By overwhelming numbers (93%), voters believe that it is important to keep information they store on their electronic devices and in mobile apps or share online secure and private. Eighty-four percent (84%), of voters saying it is “very” important. This sentiment is shared across party, with 81% of Democrats, 86% of independents, and 86% of Republicans saying it is “very” important.

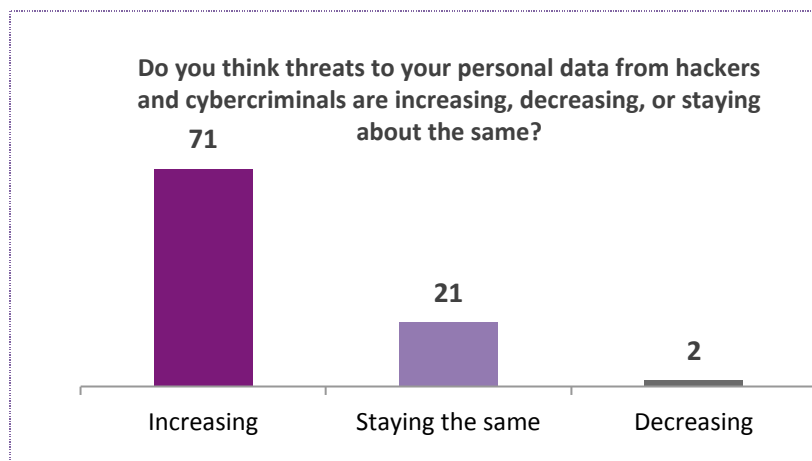
Voters recognize that they store and share more of their information than ever in digital form, both on their devices and online. They see data encryption and security measures as critical to protecting that information from cybercriminals and hackers – and want access to the strongest possible technology to achieve that end.

<p>Now that we share so much more of our personal information online, including photos, messages, and credit cards, it is more important than ever to strengthen how we protect our data.</p>	<p>Consumers should be allowed access to the strongest safeguards available to protect their personal information and security.</p>	<p>Powerful, consumer-focused encryption technology is necessary to ensure that data on my devices and the information that we share with others is secure and protected.</p>
<p>95% Agree 81% Strongly Agree</p>	<p>94% Agree 79% Strongly Agree</p>	<p>92% Agree 70% Strongly Agree</p>
		

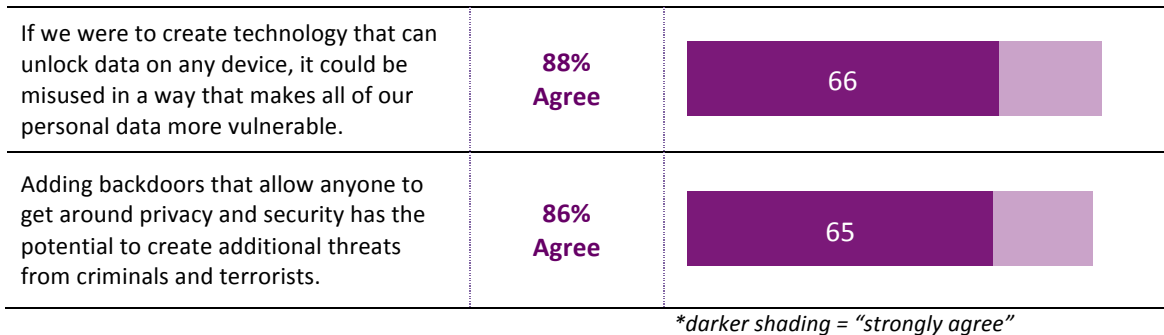
Voters are very concerned that their personal information could be accessed by cybercriminals and hackers, and believe that the threat is increasing.

A large majority (87%) of voters are concerned “that a person or organization they do not trust could gain access to personal and private information” on electronic devices or shared online, with nearly two-thirds (64%) being “very” concerned. The concern doesn’t diminish with age; millennial voters are just as concerned as seniors (84% and 83%, respectively). One in three (33%) say their own personal information has been compromised.

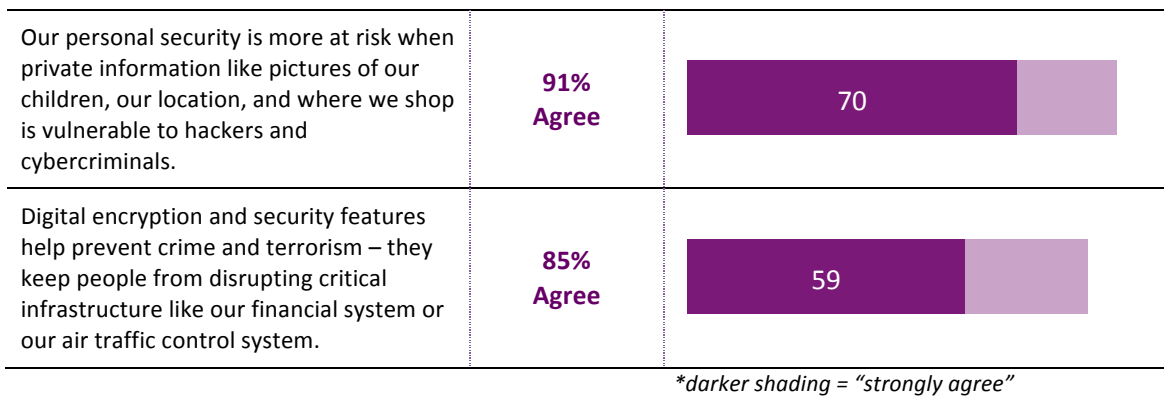
Moreover, they believe that the threat from hackers and cybercriminals is growing. Seven in ten (71%) believe the threat to their personal data from is increasing, while only 2% think it is decreasing, and a fifth (21%) say it’s staying the same. As with other results in this poll, voters across party share in their beliefs about the increasing threats.



Asked about the possibility of creating a “backdoor” to encryption technology that could be used to access any device, voters are very worried about potential misuse.



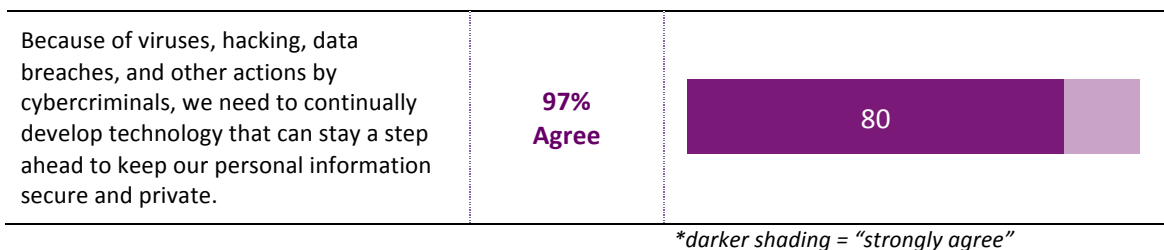
Voters strongly believe encryption helps keep them safer by protecting their personal data from hackers and cybercriminals. They also agree that weaker data encryption could make key infrastructure more vulnerable to crime and terrorism.



Few find current security protections adequate for the evolving threat, so voters believe technology companies need to continually strengthen data encryption.

When voters were asked if technology companies “should continue to build strong, innovation safeguards and strengthen data encryption to keep your information secure” or if “current security protections are adequate,” eight in ten (80%) sided with steps technology companies are making to strengthen encryption to adapt to new threats. Only 13% of voters felt current protections were adequate.

Nearly all voters believe data security has to continually evolve to stay a step ahead of cybercriminals.



Voters say they trust technology companies more than the federal government on data security.

When it comes to protecting personal digital information, voters trust technology companies over the federal government (54% trust technology companies more, 21% trust the federal government more). Importantly, voters across party share this view.

When it comes to protecting the security of the personal information that you store on your electronic devices and in mobile apps and share online, who do you trust more...?

