Press release

Americans divided on perceptions about personal data privacy control

Trust in government to secure private data, prevent election tampering appears to be on the decline

RSA Conference 2020 – San Francisco – Feb. 24, 2020 – A new study from nCipher Security, an Entrust Datacard company, suggests that 28% of American consumers think they have more control over their personal data than they did a year ago, while 26% feel that they have less control over personal data privacy and security – or no control at all.

"The stakes are getting higher in cybersecurity and data privacy. The California Consumer Privacy Act went into effect in January, giving some people a greater sense of control over their personal data. However, privacy and cybersecurity concerns related to the 2020 election are growing as the primaries begin and November inches closer," said Peter Galvin, chief strategy officer at nCipher Security. "Meanwhile, biometrics like fingerprints and facial recognition make data even more personal. These factors are sounding alarms for consumers, businesses and government over the state of cybersecurity and data privacy."

Control beliefs and trust drivers are variable

Forty-six percent of the more than 1,000 American adults surveyed said they believe they have the same level of control over their personal data as they did a year ago. But 15% said they have no control over what happens with their personal data. And the results of an nCipher survey early last year showed that a fifth of Americans said they don't trust anyone to protect their data.

Forty percent of the new survey group said their trust is higher when they have the ability to delete their data, which is now an option under data privacy laws. Forty-one percent said that when they feel in control of their personal data, they have a greater sense of trust. Nearly half (49%) said they trust that a company is safeguarding their personal data when it uses encryption.

Trust in government's ability to safeguard data appears to be on the decline

Entities enabling online banking and digital payments have taken the lead in the race to build consumer trust. Twenty-seven percent of the survey group said they trust online banking more than they did a year ago. Nearly a quarter (24%) said their trust in digital payments has increased. A fifth of the survey group (20%) trusts online shopping more than they did a year ago.

On the flip side, 30% of the survey group said they actually trust the ability of government to keep their personal data safe less than they did a year ago. And 17% went as far as to say they had no trust at all in government's capacity to safeguard their personal data privacy.

Americans are willing to accept some data risks for consumerism

Previous survey findings suggest that Americans rank safeguarding their private data at about the same level as protecting their families. But Americans are fickle when it comes to just how much risk to their personal data they're willing to incur and for what purpose.

Sixty percent of those surveyed expressed a willingness to accept some risk to personal data security for the convenience of online shopping. More than half of the group said they would assume such risk to enjoy the benefits of online banking (55%) and/or digital payments (54%).

But 47% of survey participants said that the benefits of making tax payments online is not worth putting their data security at risk. More than half (54%) said they are not willing to assume risk to their personal data privacy in exchange for the convenience of online voting.

Voter registration tampering and election interference are concerns

Concerns about election security remain high. One third (33%) of respondents said they are less confident about the state of election security in America this year than they were in 2016.

Heading into a presidential election year, 41% of Americans said they are concerned about tampering with voter registration information. More than a third are worried about election interference from a U.S. government official or political parties (38%) or other countries (37%). Thirty-seven percent said that the systems used for voting are antiquated and not secure.

When asked about their preference between paper ballots and electronic voting machines, 35% voted for paper ballots, and 30% selected electronic voting machines with paper backup records. Just 30% of Americans chose the electronic voting machine as their answer.

Survey results indicate that 24% said they would trust duplicate electronic and paper ballots to keep voting secure. Twenty-seven percent said using security questions to verify voter identities would enhance security. A fair share picked biometric approaches like fingerprint voter verification (46%) and/or facial recognition voter verification (29%). About a third said encrypted ballots (31%) and/or encrypted voter registration data (33%) are the answer.

Making the digital world more trustworthy is the better approach, but passwords are challenging

“Strong data security in the form of encryption can help build – or rebuild – trust in businesses and in the technologies and services people use to access and share data and interact with one another,” explained Galvin. “Citizens can play their part in cybersecurity and personal data privacy by keeping a lookout for scams such as phishing and practicing good password hygiene.”

However, 78% of the survey group said they have had to change their password because they forgot it on at least a few occasions. Only 9% said they had never changed a password for that reason. More than a quarter (28%) admitted to using the same passwords for work and personal logins, which increases risk. In addition, 74% of the survey group said it is somewhat, very or just plain frustrating when they have to log in to applications at work multiple times a day.

About nCipher Security

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business-critical information and applications. Today’s fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new

compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business-critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com

Follow us on LinkedIn, Twitter, Facebook and Instagram – search nCipherSecurity.

###

For more information please contact:

nCipher Security
Liz Harris liz.harris@ncipher.com +44 7973 973648