Internet Society

The State of User Privacy and Trust Online

Centre for International Governance Innovation

Ipsos

Table of Contents

Executive Summary

Since its inception five years ago, the annual CIGI-Ipsos Global Survey on Internet Security and Trust (the Survey)[1] has provided a global litmus test into user perceptions of the Internet and their security and privacy online. With five years of survey results, the Internet Society and the Centre for International Governance Innovation developed this report to highlight some of the Survey's most important findings and trends.

While user trust in the Internet remains high, with 74% of users saying they trust the Internet in 2019, privacy concerns are even more widespread and continue to grow year to year. Users continue to point to cybercriminals as a major source of distrust and online privacy concerns, but not as their only source of concern. Rather than being seen as improving online security and privacy, many respondents also see governments, social media, and Internet companies as contributors to distrust in the Internet or online privacy concerns.

The Survey also highlights the widely different experiences of Internet users across income and education levels—particularly when faced with online trust challenges. Those with positions of privilege—the rich, well-educated and/or male, are consistently more likely than the less privileged to take actions that can effectively improve their online trust and privacy.

High rates of online privacy concerns and inequalities in digital security and privacy must be addressed. No single stakeholder can tackle these challenges alone. All stakeholders need to take action to improve trust and privacy online.

- Stakeholders should enable, and not restrict, the use of trust and privacy-enhancing tools, such as encryption or virtual private networks (VPNs). They can take steps to foster the development new, affordable and usable tools; use procurement to drive demand for better security and privacy; and improve user understanding of security and privacy tools through digital literacy and capacity building initiatives.
- Stakeholders should create an enabling environment for online privacy and Internet trust by addressing inequalities in education, income and opportunities with targeted solutions such as incorporating cybersecurity literacy into their educational and ICT national strategies.
- Stakeholders should take collaborative actions to mitigate the trust and privacy risks posed by cybercrime and other threats by improving information sharing of threats, incidents, mitigations, and the implementation of norms; and highlighting successes and explaining cybersecurity failures to improve user perceptions of security and privacy online.
- Stakeholders should strengthen online privacy and Internet trust through their own actions, not weaken them. Data collectors and handlers can improve privacy and trust by practicing strong privacy and data handling hygiene; stakeholders can implement cybersecurity best practices to protect themselves and those who rely on their services; and stakeholders can build and maintain systems that make pervasive surveillance harder, not easier.
- Stakeholders should foster more reliable and secure networks by avoiding Internet shutdowns and investing in local and regional ICT infrastructure that improve Internet reliability and security.

1 The CIGI-Ipsos Global Survey on Internet Security and Trust is conducted by Ipsos on behalf of the Centre for International Governance Innovation (CIGI), in partnership with the United Nations Conference on Trade and Development (UNCTAD) and the Internet Society.

Introduction

In recent years, user trust in the Internet has faced considerable obstacles. Major security breaches, such as the Equifax breach, have exposed the personal and financial information of millions.[2] Government surveillance continues to occur, with new AI-based biometrics and IoT devices expanding the gaze of governments into the physical world via the Internet.[3] Fake content (sometimes referred to as "fake news") is increasing in both volume and sophistication, causing polarization, confusion, and political discord.[4] Meanwhile, the advertising-based business model on the World Wide Web continues to push businesses to collect, process, and monetize user data in ways that are unexpected, disorienting, and often unwelcome.[5]

News of surveillance, data breaches, fake news, and other problems seem like a recipe for user distrust in the Internet. Yet, user trust remains resilient, although users seem to have a conflicted view of the Internet. In 2019, a large majority of users across 25 economies—nearly three quarters—trusted the Internet overall, even as nearly eight in ten said they have serious concerns about online privacy.

In the 2019 CIGI-Ipsos Global Survey on Internet Security and Trust ("the Survey"), Internet users point to cybercriminals, Internet companies, other Internet users, and governments as major sources of their distrust in the Internet and concerns about online privacy.

How Internet users react to trust and privacy concerns depends on who they are. Often, when faced with challenges, those with greater privilege (higher income, education, or male) are more likely to take action, either through simple steps or more sophisticated countermeasures, to try to improve their online security and privacy. However, those with less privilege often tend to perform only the most basic of mitigations. Those who are more disadvantaged are also more likely to report doing nothing at all in response to distrust.

This gap between the privileged and less privileged could have very serious consequences for a fair future for the Internet, particularly as the next billion users will come from less developed economies and likely less privileged circumstances.

2 https://www.internetsociety.org/blog/2017/09/post-equifax-need-reconsider-identify-people/
3 https://www.cigionline.org/articles/state-and-surveillance
4 https://www.cigionline.org/articles/beware-fake-news
5 https://www.internetsociety.org/blog/2018/04/larger-facebook-cambridge-analytica-question-really-signed/

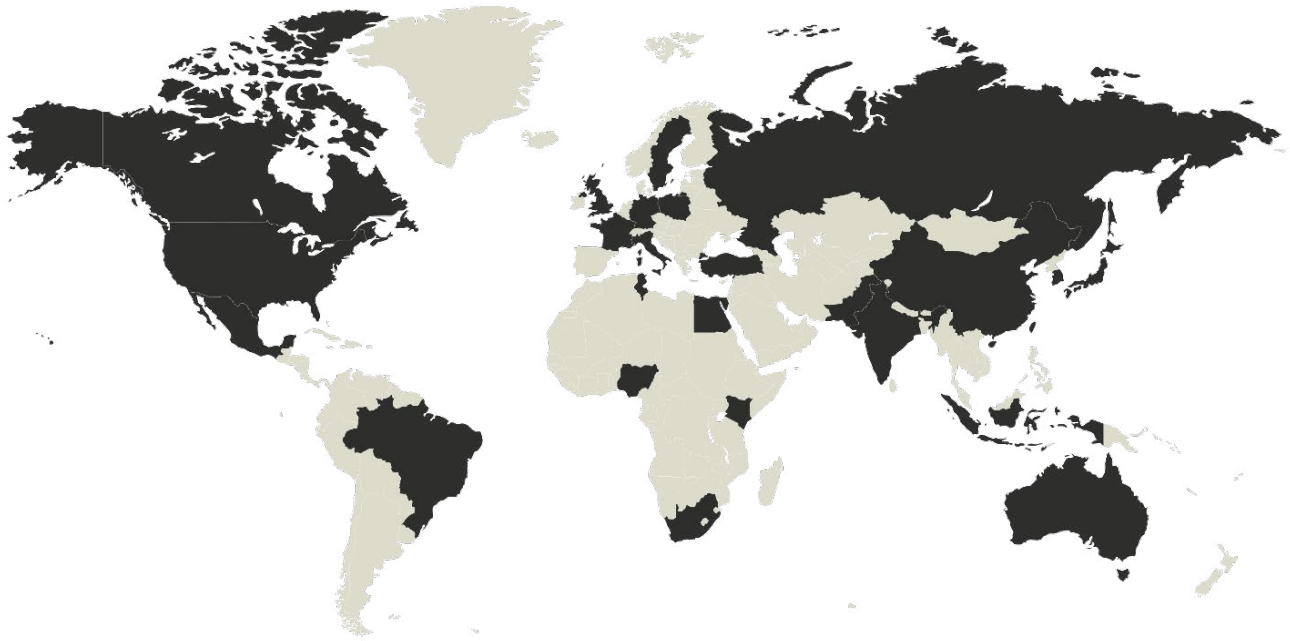


IMAGE CREDIT: CIGI, 2019

About the CIGI-Ipsos Global Survey on Internet Security and Trust

The *CIGI-Ipsos Global Survey on Internet Security and Trust* is currently in its fifth iteration.[6] The Survey is conducted yearly by Ipsos[7] on behalf of the Centre for International Governance Innovation (CIGI),[8] the Internet Society,[9] and the United Nations Conference on Trade and Development (UNCTAD).[10]

The 2019 survey collected the views of more than 25,000 Internet users from 25 economies: Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Russia, South Africa, Republic of Korea, Sweden, Tunisia, Turkey, and the United States.

The 2019 Survey was carried out online and in face-to face interviews between December 21, 2018 and February 10, 2019. Face-to-face Interviews were held in Pakistan, Tunisia, Kenya and Nigeria. Each year, approximately 1,000+ individuals were surveyed in each economy and the results are weighted to match the population in each economy surveyed. As participation in the interviews is voluntary, the respondents were self-selected and it is unlikely that the same individuals were interviewed year to year.

6 https://www.cigionline.org/internet-survey-2019
7 https://www.ipsos.com/en
8 https://www.cigionline.org/about
9 https://www.internetsociety.org/about-internet-society/
10 https://unctad.org/en/Pages/aboutus.aspx

The precision of Ipsos online polls is calculated using a credibility interval. For the 2019 Survey, a poll of 1,000 is accurate to +/- 3.5 percentage points. For the face-to-face interviews, the margin of error is +/-3.1, 19 times out of 20. These margins of error are consistent throughout the five iterations of the Survey.

The Survey also collected demographic information from respondents, allowing for closer analysis, not only the economy level, but also between users of different ages, education levels, household incomes, and genders.

In the US and Canada, respondents were aged 18-64. Respondents in all other economies were aged 16-64. Respondents were also divided into classifications for both household income level and education level. The thresholds for low, medium, and high levels of household income or education varied by economy and were based off of census groupings and categories by Ipsos. For example, in India, respondents with monthly household incomes of between Rs. 25,000 (360 USD) and Rs. 100,000 (1,442 USD) were classified as having medium household income. In China, respondents with monthly household incomes of between 3000 yuan (434 USD) and 7,499 yuan (1085 USD) were classified as medium household income.

User Trust in the Last Three Years

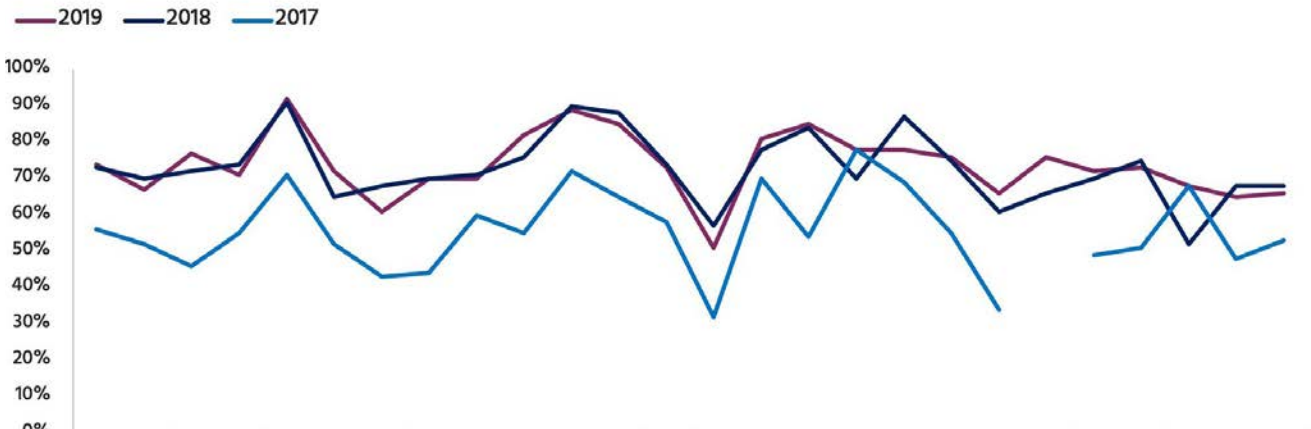
Internet users' trust in the Internet has remained steady over the last two years (2018-2019), although it was significantly lower in the survey released in 2017, the first year that featured a question on how much users trust the Internet overall.

In the 2019 survey, 74% of those responding said they trust the Internet, roughly in line with the 73% who indicated the same in 2018. In 2017, just 56% of respondents said they trusted the Internet.

It is difficult to definitively establish causal associations between world events and the survey results, yet it is worth noting that news reports of mass government surveillance and fake news campaigns, among other things, were fresh in the mind during the 2016 and 2017 timeframe. At the same time, the 2017 survey asked additional questions about censorship and surveillance before asking the question on overall trust. The difference in question sequencing might have also contributed to the lower reported levels of trust in 2017, when compared to the results from more recent years.

User trust is very personal. The word "trust" may mean different things to different people even in the same context. What we consider to be trust is shaped by my factors including our culture, our education, and our experience. The Survey did not ask users how much they trust the Internet to perform in specific ways or to provide a specific user experience. Rather, it asked how much they agree or disagree with the statement "Overall, I trust the Internet." Therefore, the results around user trust should be analyzed with the understanding that differing notions of what it means to trust the Internet are likely to have influenced the results. An example, is highlighted in the final paragraph of section 4 on the degree to which users equate control and predictability with trust. Nonetheless, there is still value in gauging the proportion of respondents within a population who trust the Internet, by whatever their definition, as a rough indicator of positive or negative attitudes towards the Internet.

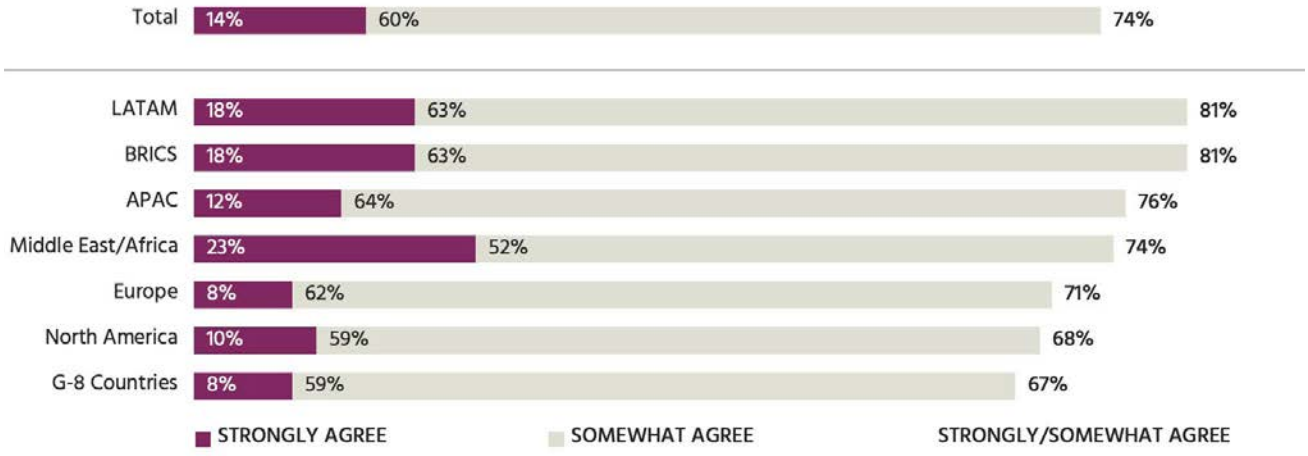
OVERALL, I TRUST THE INTERNET – BY ECONOMY



	TL	AU	BR	CA	CN	EG	FR	DE	GB	HK	IN	ID	IT	JP	KE	MX	NG	PK	PL	KR	RU	ZA	SE	TN	TR	US
2019	74%	67%	77%	71%	92%	72%	61%	70%	70%	82%	89%	85%	73%	51%	81%	85%	78%	78%	76%	66%	76%	72%	73%	68%	65%	66%
2018	73%	70%	72%	74%	91%	65%	68%	70%	71%	76%	90%	88%	74%	57%	78%	84%	70%	87%	75%	61%	66%	70%	75%	52%	68%	68%
2017	56%	52%	46%	55%	71%	52%	43%	44%	60%	55%	72%	65%	58%	32%	70%	54%	78%	69%	55%	34%	n/a	49%	51%	68%	48%	53%

Q6. To what extent do you agree or disagree with the following statement: "Overall, I trust the Internet"
Base: All Respondents 2019 (n=25,229); 2018 (n=24,962); 2017 (n=24,225)

OVERALL, I TRUST THE INTERNET— BY REGIONAL ECONOMY IN 2019



Q6. To what extent do you agree or disagree with the following statement: "Overall, I trust the Internet"
Base: All Respondents 2019 (n=25,229); 2018 (n=24,962); 2017 (n=24,225) BIC (not BRICS)

Online Trust Varies by Economy

The degree of user trust varies significantly by economy.

In 2019, 92% of respondents from China said they trust the Internet, while 89% of those from India and 85% of those from Mexico said the same. While these economies had the highest levels of trust in 2019, Japan had by far lowest, with only 51%. Following Japan for lowest levels of trust in 2019 were France (61%) and Turkey (65%). Slightly less than 70% of respondents in Tunisia, Australia, the United States, and Republic of Korea said they trust the Internet in 2019.

In 2017, just 32% of Japanese survey respondents said they trust the Internet, with that number rising to 57% in 2018, while falling again by 6 points in 2019.

In 2017, only 34% of respondents in the Republic of Korea said they trust the Internet. In 2019, the number rose to 66%.

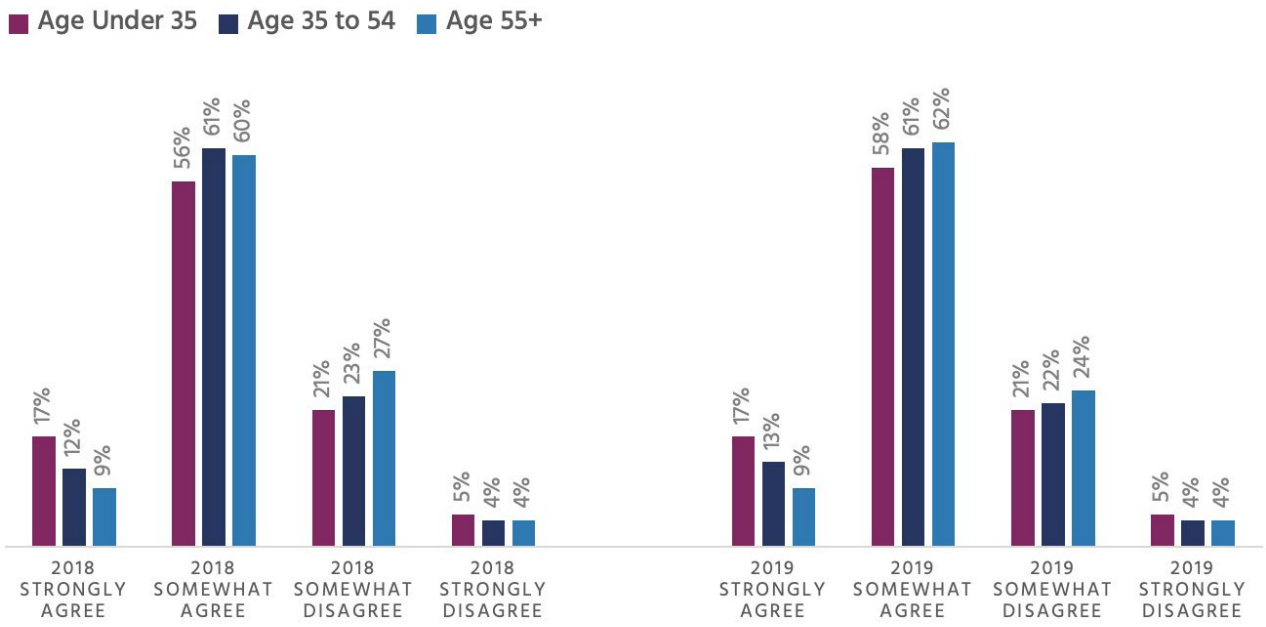
While most economies' numbers were 15 to 20 percentage points lower in 2017, then similar between 2018 and 2019, a couple of economies went against the trend. Pakistan's level of trust stood at 69% in 2017, rose to 87% in 2018 and fell back to 78% in 2019. Meanwhile, Tunisia's numbers went from 68% in 2017 down to 52% in 2018 and then rebounded back to 68% in 2019. Economy-specific events may well be driving this variation and it would be helpful for the local community to examine the reasons why user trust may be fluctuating in this way.

Online Trust Is Higher among Younger Users

While gender, education, and income levels matter somewhat, a key driver of trust in the Internet tends to be age.

Younger people, who are more likely to be "digital natives," strongly trust the Internet at higher rates than older individuals. There is an 8 percentage-point difference between the youngest and the oldest demographic groups in both 2018 and 2019. These results may help to reconcile the perception (whether valid or not) that young people are less concerned with their online privacy or more willing to share personal information online than older generations. These characterizations of youth behavior might be accurate, but it is also possibly a result of higher levels of trust in the Internet, rather than due to a lack of understanding or a general disregard with online privacy.

AGE AND AGREEMENT TO THE STATEMENT "OVERALL, I TRUST THE INTERNET", 2018 AND 2019



A "Trusted" Internet?

Overall, despite concerns about privacy and other issues, user trust in the Internet is high, with nearly three-quarters of the survey respondents in 2018 and 2019 saying they trust the Internet.

Trust varies considerably across economies, and it is difficult to point to reasons why, for example, Chinese users trust the Internet considerably more than those in Japan. This raises interesting questions, particularly around what users view as "trust" and "the Internet." For instance, if users equate trust with a predictable and controlled environment, Chinese users, who engage online on highly centralized and controlled networks and applications, would seem to be more likely to respond that they trust the Internet.

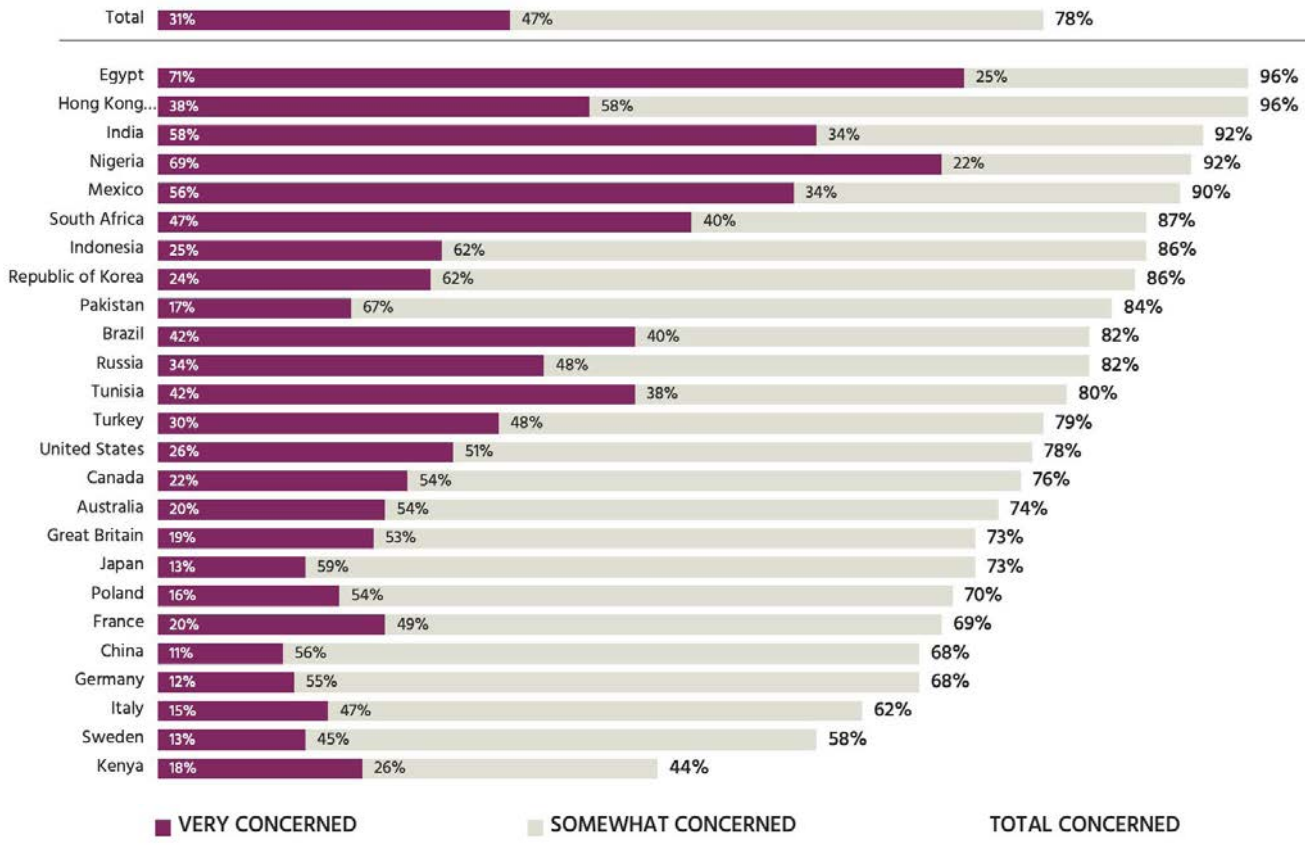
Privacy During the Last Five Years

In 2019, 78% of survey respondents said they were very concerned or somewhat concerned about their online privacy, and 53% said they were much more concerned or somewhat more concerned than they were a year ago.

While more than half of all respondents have expressed more concern about their online privacy in each year of the survey, the rate by which concern has grown has actually slowed since the first survey in 2014-2015. In the 2014 survey (released in 2015), 64% said they were more concerned about their online privacy than a year earlier. That number dipped to 57% in 2016, 55% in 2017, and 52% in 2018, before remaining steady with a a 1% increase in 2019.

Two reasons stand out as potential explanations for this trend. When viewed cumulatively, the rate by which perceptions of privacy worsen might eventually slow, since people could reach a point where they are so concerned about online privacy that they could not perceive themselves as being any more concerned than they already are ("privacy fatigue"). Another explanation could be that the 2014-2015 survey results followed in the wake of Edward Snowden's disclosure of US National Security Agency (NSA) surveillance, which may have prompted widespread concern over government mass surveillance and online privacy.

PRIVACY CONCERNS BY ECONOMY IN 2019



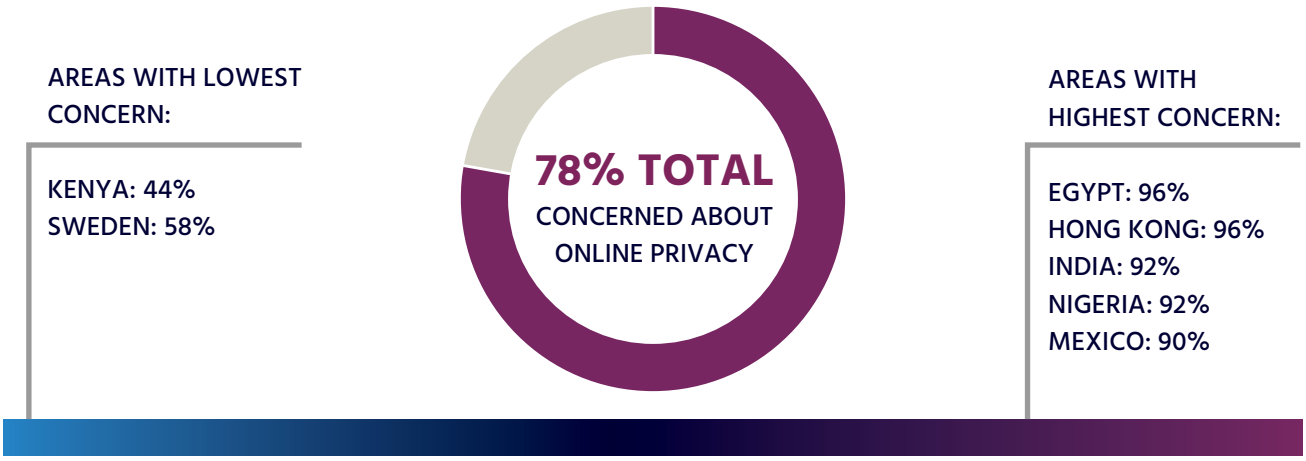
A1. How concerned are you about your online privacy?
Base: 2019 (n=23,854)

Privacy Concerns Vary by Economy

Privacy concerns varied significantly among the 25 economies represented in the 2019 survey. While 78% of all respondents in 2019 were concerned about their online privacy, 90% or more were concerned in Egypt, Hong Kong, India, Nigeria, and Mexico, with more than 85% concerned in South Africa, Indonesia, and South Korea.

On the other end of the spectrum, 58% of respondents from Sweden and 44% from Kenya were somewhat or very concerned about their online privacy in 2019.

Similarly, while 53% of all respondents said they were more concerned about their online privacy than they were a year ago, 82% of Nigerian respondents said they were. About three-quarters of respondents from Egypt and India also said they were more concerned about online privacy compared to a year ago.



Does GDPR Feel Like Better Privacy?

Overall, those surveyed from European Union economies were 14 percentage points less concerned about privacy in 2019 than the respondents from the other economies surveyed. Similarly, the proportion of respondents in European economies who were more concerned about privacy than last year fell from 50% to 40% since the 2016 survey. By contrast, the rate by which privacy concerns worsened in non-EU economies remained relatively flat, dropping only from 59% to 57% since the 2016 survey. Similarly, when asked how aware they are of their country's data protection and privacy rules, 50% of respondents from EU economies said they were at least somewhat aware. In contrast, only 41% of respondents from non-EU economies in 2019 said they were at least somewhat aware of their country's data protection and privacy rules. While other factors may have influence, the results could suggest that the EU General Data Protection Regulation (GDPR), which was passed into law shortly after the 2016 survey, has had a reassuring effect on user perceptions of online privacy.

Privacy Concerns Vary by Demographic Groups

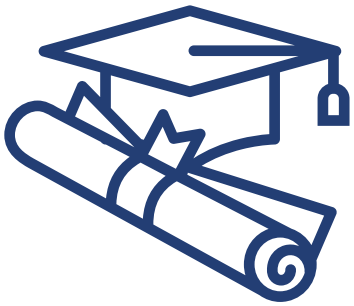
Meanwhile, within the various economies in the sample, higher income and education levels were tied to greater online privacy concerns.

Higher income respondents are more concerned, but lower income respondents showed greater increase in concern.

Across all those surveyed, 80% of high-income respondents were at least somewhat concerned about their online privacy in 2019, compared to 74% in the lowest income bracket. Yet, lower-income respondents' concerns about privacy are growing at a faster rate. Their online privacy concerns, compared to a year earlier, grew faster than those with high incomes in the 2017, 2018, and 2019 surveys, although the difference was small in the most recent survey.

Highly educated respondents are more concerned than less educated respondents.

Breaking the results down by education level yielded similar results. 83% of highly educated respondents were at least somewhat concerned about their online privacy in the latest survey, compared to just 72% of respondents with low education levels. Highly educated respondents also had a higher level of concern than the year earlier in the last three years, as compared to people with lower education levels.



Male and female respondents differ slightly when asked if their concerns about privacy are growing.

In 2019, 54% of female respondents said they were more concerned about their online privacy than they were a year ago, compared to 52% of males. However, each year, the percentage of females more concerned about their privacy from a year ago was slightly higher than the percentage of males. Therefore, concern about privacy is growing faster among females than it is among males, although the gap each year is small.

A Shifting Privacy Landscape

While overall trust in the Internet remains high, users are concerned about their online privacy, and that concern appears to be growing. The rate of growth has slowed during the last couple of years, but this must be understood in the context that 31% of respondents are already very concerned about their online privacy.

As with the results on trust, privacy concerns differ significantly among the economies surveyed, with high levels of concern in parts of Latin America, Asia, and Africa. They also vary significantly across demographic groups. Although concern was higher among those with higher incomes, concern is growing faster among those in lower-income brackets.

In the 21st century, many online services have become "free," and are instead funded by the monetization of user data. An argument is often made that these services improve access and innovation by allowing those with lower incomes to exchange their data for services. However, rapidly increasing privacy concerns among lower income users, closely illustrates the problems with this "Faustian Bargain."[11] Users might be willing to trade data for services now, but privacy-related warning signs sit on the horizon.

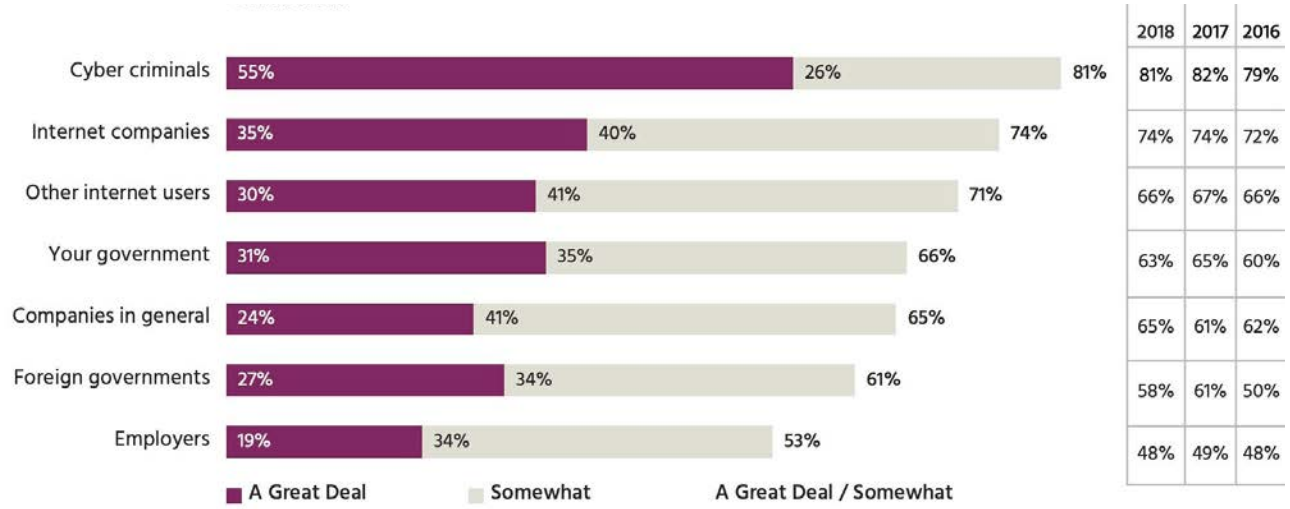
Given such high privacy concerns, it is not surprising that more economies have, or are pursuing, privacy legislation. Given the divide between respondents from EU and non-EU economies on privacy concerns since 2016, privacy legislation may cause positive perceptual changes among users' perceptions of their privacy online.

11 https://www.britannica.com/topic/Faustian-bargain

Contributors to Privacy Concerns and Internet Distrust

While the Survey could not have covered all of the sources of distrust in the Internet and online privacy concerns, the Survey identifies several concerns users have about the Internet. Across multiple years of surveys, many of the respondents said that cybercriminals, governments, and social media hurt both their level of trust and their privacy. Users also indicated that aspects of the Internet itself, including its perceived insecurity and degrees of outside control, contribute to their distrust in the Internet.

ACTORS CONTRIBUTING TO ONLINE PRIVACY CONCERNS IN 2019



2018	2017	2016
81%	82%	79%
74%	74%	72%
66%	67%	66%
63%	65%	60%
65%	61%	62%
58%	61%	50%
48%	49%	48%

Q2. To what extent have the following sources contributed to your being more concerned than last year about your online privacy? Base: A Great Deal / Somewhat More Concerned About Online Privacy 2016 (n=13,867); 2017 (n=12,468); 2018 (n=12,956); 2019 (n=25,229)

Cyber Criminals

Among those that distrust the Internet, 81% in 2019 strongly agreed or somewhat agreed that cybercriminals contributed, by far the highest of any contributor to distrust.

Cybercriminals are consistently seen as sources of worry year over year. In 2018, for example, 80% of respondents who do distrust the Internet said the same. However, this sentiment varies across age groups, with younger respondents less likely to point to cybercriminals as a source of their distrust. When looking at the sources of distrust, 87% of the 2019 survey respondents age 55 and up identified cybercriminals, compared to 77% of those age 35 and younger.

As for a source of their privacy concerns, 81% of respondents who expressed a growing concern in 2019 said cybercriminals contributed.

Governments

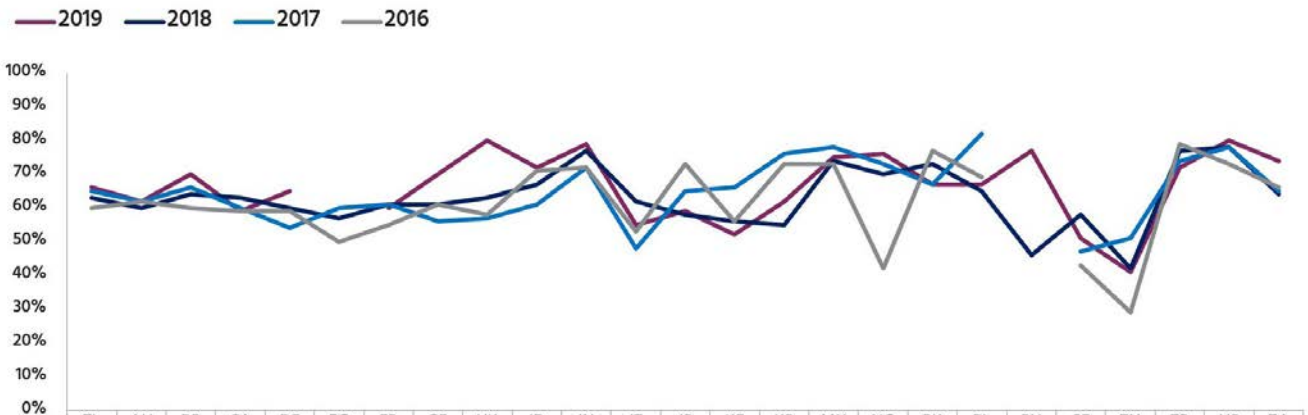
A solid majority of Internet users across the globe point to governments, both foreign and their own, as negatively impacting both their trust in the Internet and their privacy.

Among respondents who distrusted the Internet in 2019, 61% identified foreign governments and 66% identified their own governments as a source of distrust.

Concern varied among economies, but a staggering 86% of respondents in the United States who distrust the Internet said their own government contributes to their distrust in 2019. More than three-quarters of respondents who distrust the Internet in Great Britain, Mexico, South Africa, and Canada also said their governments contribute to distrust in 2019. Less of half from Tunisia and Japan suggested their own government contributes to their distrust in the Internet.

In 2019, 66% pointed to their own governments as a cause of their growing privacy concerns, and 61% blamed other governments. Majorities in 23 of 24 economies[12] saw their own governments as contributors to their growing privacy concerns, about eight in ten of those in Hong Kong, the United States, India, Russia, and Nigeria. The outlier was Tunisia, with only 41% saying their own government contributes to their growing privacy concerns.

PRIVACY CONCERN DUE TO OWN GOVERNMENT



	TL	AU	BR	CA	DE	EG	FR	GB	HK	ID	IN	IT	JP	KE	KR	MX	NG	PK	PL	RU	SE	TN	TR	US	ZA
2019	66%	62%	70%	59%	65%	n/a	60%	70%	80%	72%	79%	55%	59%	52%	62%	75%	76%	67%	67%	77%	51%	41%	72%	80%	74%
2018	63%	60%	64%	63%	60%	57%	61%	61%	63%	67%	77%	62%	58%	56%	55%	74%	70%	73%	65%	46%	58%	42%	77%	78%	64%
2017	65%	62%	66%	60%	54%	60%	61%	56%	57%	61%	72%	48%	65%	66%	76%	78%	73%	67%	82%	n/a	47%	51%	74%	78%	65%
2016	60%	62%	60%	59%	59%	50%	55%	61%	58%	71%	72%	53%	73%	56%	73%	73%	42%	77%	69%	n/a	43%	29%	79%	73%	66%

Q2. To what extent have the following sources contributed to your being more concerned than last year about your online privacy? [Your Government] Base: A Great Deal / Somewhat More Concerned About Online Privacy 2016 (n=13,867); 2017 (n=12,468); 2018 (n=12,468); 2019 (n=12,899) NOT ASKED IN EGYPT & CHINA

12 This question was not asked in China.

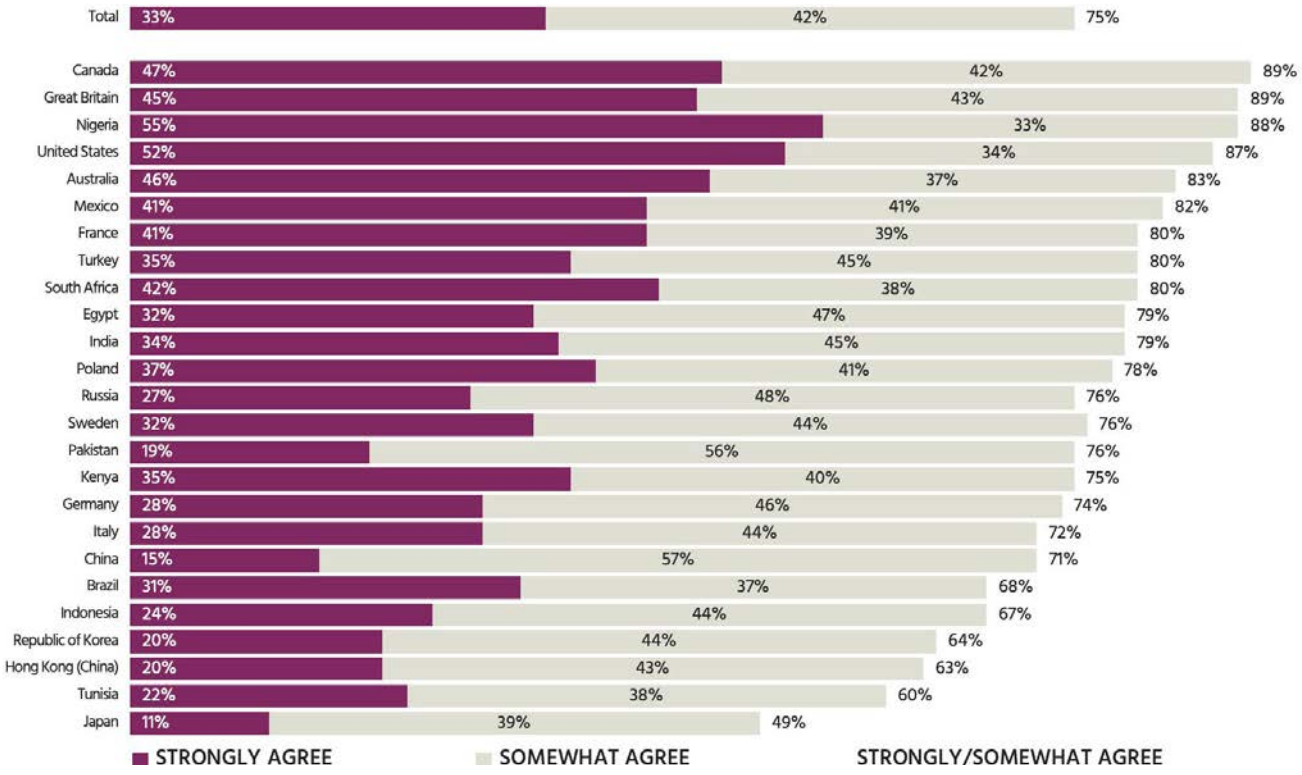
Social Media and Internet Companies

Despite their ubiquity, Internet users have serious reservations about social media. 75% of respondents who distrust the Internet in 2019 pointed to social media as a major contributor to their distrust and, since 2017, Internet companies have been cited by nearly three-quarters of users as a source of their growing privacy concerns.

This perception varied across age groups, however, with 81% of those age 55 and up identifying social media companies as a source of distrust, compared to 72% of those age 35 and younger.

When asked about the impact of social media overall, nearly six in ten respondents in 2019 say it has increased their ease of communication and their access to information. However, nearly half say social media has negatively impacted their personal privacy, and more than four in ten say social media has aided polarization in politics and foreign meddling in politics.

SOCIAL MEDIA COMPANIES AS A SOURCE OF INTERNET DISTRUST IN 2019 BY ECONOMY



Q7. To what extent do the following contribute to your distrust in the Internet? Base: All Respondents who do not completely trust the Internet 2019 (n=6608); 2018 (n=6778)

Other Internet Users

71% of respondents with growing privacy concerns cited other Internet users as a contributing factor. This number was relatively flat until this year, when it jumped by five percentage points. Female respondents were more likely than male respondents to cite other Internet users as a contributing a great deal to their online privacy concerns.

2019 Highlight: Algorithms

Many users suspect algorithms used in different contexts are biased, with less than half of survey respondents saying they are confident that the algorithms used in online daily life are unbiased. SSocial media news feed algorithms, predictive policing, job application screenings, credit score calculations, and risk assessments used in judicial decisions received particularly low scores, with fewer than 40% of respondents expressing confidence in their results.

The most common reasons for a lack of confidence in the unbiasedness of algorithms included a lack of transparency, a perception that they are exploitative by design, and an absence of a human element in the decision-making.

2019 Highlight: Fake News

The 2019 survey looked at fake news for the first time, and many people pointed to social media as a major cause of the problem. Two-thirds of those responding said they have seen fake news on Facebook, with just slightly less saying they have seen it on social media in general. By comparison, just over half said they have seen fake news on television, 44% in print media, and 41% on a blog. Just four in ten said they've seen fake news on Twitter.

In four economies, Republic of Korea, Germany, Russia, and Japan, less than half of respondents reporting seeing fake news on Facebook. Just 14% of Japanese respondents said they have seen fake news on the social media site, but then, 56% of the Japanese participants said they don't use the platform, by far the largest percentage of non-users in any economy.

Twitter, by contrast, still has a large number of non-users in several economies, contributing to its lower fake news results. More than 40% of Internet users in 13 of the 25 economies surveyed, including the United States, Great Britain, Germany, and Hong Kong, said they do not use Twitter. Mainstream media scores lower in reported fake news than Facebook and general social media, with 45% of respondents saying they have seen fake news there. However, more than six in 10 survey participants in Egypt, Turkey, and Russia said they have seen fake news in the mainstream media.

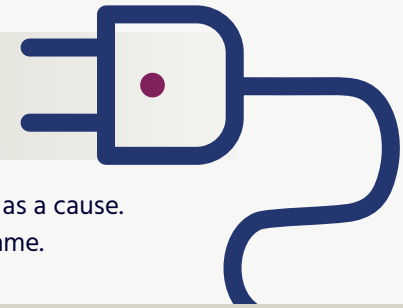
Meanwhile, 44% of the survey respondents admit to being duped by fake news at least sometimes.

Features of an Untrustworthy Internet

Users who distrust the Internet pointed to a number of perceptions of the Internet as sources of distrust. Among these, security rises to the top.

Overall, 62% of those who distrust the Internet in 2019 noted that a lack of Internet security was a contributing factor. Interestingly, these concerns vary significantly by the age of respondents.

Those less than 55 years of age were much less likely to point to a lack of security as a cause of distrust compared to those who are older than 55.



Reliability is consistently another major source of concern.

In 2019, 37% of respondents who distrusted the Internet cited the unreliably of the Internet as a cause. In 2018 and 2017, 38% and 40% respectively of those who distrusted the Internet said the same.

There is also a consistent divide between those who desire more control, and those who desire less control, on the Internet.

In 2019, 39% of respondents who distrust the Internet indicated that the Internet being too uncontrolled was a primary reason.

In 2019, 25% also indicated that they distrusted the Internet because it was too controlled by foreign governments and 20% because it was too controlled by their own government.

In 2018, the divide was similar. Concerns around their own government and foreign government control were higher at 27% and 26% respectively. 36% of respondents who distrusted the Internet in 2018 indicated that the Internet being too uncontrolled was a primary reason for distrust.

While "the Internet is too uncontrolled" was not an option in the 2017 survey, respondents who distrust the Internet pointed to foreign governments as a source of distrust at the same rates as in the 2018 survey.

Interestingly, income also seems to be a driver for different perceptions of trust and control. In 2019 and 2018, those with higher income levels had higher concerns about the Internet being uncontrolled than those with lower income levels.

Governments are increasingly feeling the pressure to address challenges online. As they attempt to do so, we may see a division grow at the core of the Internet-using population—with some reacting negatively to what may be seen as unwelcome government control.

For the majority of users, the notion of Internet control could mean control over content at the application layer or on the World Wide Web. However, the levels of control over other layers of the Internet, like of infrastructure layer, may be less obvious to users. The outcomes of these struggles could have serious implications for trust and privacy of users.

Behavior Changes and the Security Gap

In response to distrust in the Internet, respondents are most likely to make simple changes in how they use the Internet, rather than take more sophisticated actions or adopt the use of new tools. Since 2017, the most common response was to disclose less information, cited by around 50% each year. Other more common behavior changes included taking care to secure their device, using the Internet selectively, and self-censoring what they say online. However, only around 20% each year said they were using more encryption[13] and even less cited that they were using other security and privacy-enhancing tools like Tor[14] or VPNs.[15] It is possible, however, that some users were not aware that the services they were using are encrypted at all.

Yet, the Internet experience is not static across demographic groups and neither are their actions in response to distrust in the Internet or around their privacy concerns. Across the world, those in positions of privilege are more likely to take actions to improve their security and privacy online.

WAYS LACK OF TRUST HAS CHANGED BEHAVIOR IN 2019

Q9. How has your lack of trust in the Internet caused you to use the Internet differently?
Base: Those Who Distrust Internet 2019 (n=6608); 2018 (n=6390); 2017 (n=10,168)

13 Encryption is the process to scramble or hide information so it can only be read by someone with the means (or keys) to return it to its original state.

14 Tor is a widely used tool for protecting your privacy and enabling anonymous use of the Internet without being tracked.

15 VPN, or Virtual Private Networks, encrypt Internet traffic and send it through a server that physically sits in another location. Acting like a tunnel, VPNs mean Internet Service Provider (ISP) will no longer be able track your online activity, but will only see traffic coming in and out of the VPN.

Security and Privacy-Enhancing Technologies

Those with higher education or with a higher income were more likely than others to indicate that they started using more sophisticated privacy and security enhancing technologies. In 2019, those with a high level of household income were much more likely to have noted a behavior change that year of using more privacy settings, using encrypted communications services, using two-factor authentication, or more regular updating of software, than those with a low level of household income.

A report by Pew Research in 2017 found similar results on the use of privacy and security enhancing tools in the United States.[16] In their survey, they found that "low-income internet users living in households earning less than $20,000 per year are significantly less likely than those in higher-earning households to use privacy settings to limit who can see what they post online (57% vs. 67%)."

In the Survey around a quarter of respondents across income levels in 2019 found it easier to use encrypted communications than the year prior, but most indicated that it was no easier or harder. Respondents with low household income were more likely than those with mid-high household income (16% vs. 13% medium & 11% high) to indicate that it has become harder to use encrypted communications in the past year.

The differences among income levels were largely mirrored when results were divided by respondents' educational levels. In 2019, those with lower education were less likely to indicate than both medium and higher educated respondents that it has become easier to use encrypted communications.

Gender, while less than education and income level, seems to affect the use of security technologies. Male respondents were slightly more likely to indicate the use of these tools in response to Internet distrust than female respondents. 22% of male respondents who distrust the Internet in 2019 indicated that they are using more encryption, while only 17% of female respondents said the same. Men in 2019 were also slightly more likely than women to indicate that it has become easier to use encrypted communications in the past year.

HIGHER EDUCATION AND HIGHER INCOME ARE BOTH LINKED TO INCREASED USE OF PRIVACY SETTINGS.

IN RESPONSE TO INTERNET DISTRUST IN 2019:

26% of those with high household incomes said they are using more encryption vs. only 14% of those with low household incomes.

23% with high levels of education said they were using more encryption vs. only 16% of those with low levels of education.

OF RESPONDENTS WHO DISTRUST THE INTERNET IN 2019:

22% of males indicated that they are using more encryption.

Only 17% of females respondents said the same.

16 Madden, Mary. "Privacy Security and Digital Inequality: How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity," 2017. https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf

2019 Highlight: Product Security

Across the globe, respondents said they are willing to pay about 30% more for a product with better security built-in, consistent across all Internet-enabled devices. But, three in ten respondents said they are not willing to pay an extra premium.

Respondents from developing economies appear to be more willing to pay extra for better security in Internet-enabled devices. When making purchasing decisions, respondents in developed economies are less likely to consider security as a top factor than those in developing economies. Consistent with these purchasing priorities, respondents in developed economies are also less willing to pay extra for a more secure product.

Developed economies are often the target market for Internet-enabled devices. Since users in these locations are generally less willing to pay more for security, the market might not create incentives that improve product security.

Basic Mitigations

While those with greater household incomes or higher levels of education were still more likely to engage in basic mitigations (such as avoiding clicking on unknown links, avoiding opening emails from unknown sites, and disclosing less personal information online) to address their distrust and privacy concerns than others, these activities were more common across every demographic group than using specific privacy and security-enhancing technologies. Across household income levels, respondents stated that they used more false personal information online, at around the same rate of roughly 15% in 2019. Providing false (i.e. incorrect) information can be a useful and easily implemented strategy for mitigating privacy threats where accurate personal data is not needed.

Mitigations by Those with Less Income or Education

Concerningly, income and education seems to be a significant factor behind using less effective mitigations, including doing nothing at all. Those with low household income or low levels of education were far more likely than others to respond that they performed none of the behavior changes listed as a result of their distrust in the Internet.

Those at the highest level of income and education were also slightly less likely than those at lower levels of income to use the Internet less as a result of distrust in the Internet.

What This Means for the Internet

An overwhelming majority of Internet users surveyed trust the Internet overall, but a growing number are concerned about the privacy implications of their online activities.

The results of this multi-year survey suggest that the Internet remains generally trusted, even while privacy concerns loom. How users interact with the Internet and the steps they take to increase their online trust vary across demographic groups, with security and privacy looking more like a story of digital "haves and have-nots." Different stakeholders, while they should be contributing to online trust and privacy, are instead viewed as sources of concern. Worryingly, user perceptions of the security and reliability of the Internet itself are leading to distrust. As it stands, the Internet seems to continue to be resilient, but growing concerns around the actions of different stakeholders and high levels of concern around online privacy seem to suggest there are storm clouds on the horizon.

Actions

To ensure the future of the Internet is a bright one for all users, no matter their demographic background, all stakeholders will need to take action to improve trust and privacy online.

Enable, and not restrict, the use of trust and privacy-enhancing tools.

Despite their utility, many of the best tools for improving privacy online, like encryption and two-factor authentication, are not being quickly adopted by users—and even less among those with lower incomes and education levels. Whether through government policies that limit the use of end-to-end encryption, industry choices that exclude users through difficulty of use or high costs, or other reasons, stakeholders must not take actions that limit the adoption of these tools.

To enable, not inhibit, users to adopt these tools, stakeholders should:

- **Foster the development of affordable and usable tools.** Security and privacy should not be a luxury afforded to the few. Stakeholders should facilitate the development of privacy-enhancing tools that can reduce costs or improve usability and facilitate improved implementation of norms and best practices.
- **Use procurement to drive demand.** Market size often influences features and pricing. Stakeholders, particularly governments and large enterprises, can strengthen demand for security and privacy tools at large by making them a part of their procurement policies.
- **Improve user understanding of security and privacy tools.** Users will not use security and privacy tools unless they understand the tools and the threats they would help mitigate. Stakeholders can support or engage in consumer education and capacity-building initiatives to improve understanding and use of security and privacy tools.

Create an enabling environment for online privacy and Internet trust.

The use of security and privacy-enhancing tools is influenced by larger non-technical factors, like levels of education and income. By addressing these factors, stakeholders can help users contribute to a better enabling environment for improving online privacy and trust.

To create an enabling environment for improving online trust, stakeholders should:

- **Take steps to strengthen education.** Education and the use of security and privacy-enhancing tools are closely tied. In line with the 4th Sustainable Development Goal on Education, improving education can help improve the use of security and privacy-enhancing tools.
- **Address inequalities with targeted solutions.** Those at lower incomes are more likely to use ineffective or even harmful techniques to address their distrust in the Internet. Stakeholders should recognize these disparities in user trust and privacy and develop targeted strategies. For example, economies could incorporate cybersecurity literacy as part of their national ICT and educational strategies for all citizens.

Take collaborative actions to mitigate the trust and privacy risks posed by cybercrime and other threats.

The interdependent and interconnected nature of the Internet makes it impossible for any single actor to tackle its challenges alone. Whether it is spam, distributed denial of service attacks, or some other threat, cyberattacks are best tackled by those closest to their source.

To mitigate the threat to online privacy and Internet trust presented by cybercriminals, stakeholders should:

- **Improve information sharing.** Alerting those best positioned to take action against cyber threats is a crucial aspect of cybersecurity. Strengthening threat signaling and information sharing, whether through formal channels like computer incident response teams (CSIRTs) or through informal trusted communication channels, will allow stakeholders to more effectively respond to cyber threats.
- **Highlight successes, explain failures.** Perceptions of cyber threats, and stakeholders' efforts to respond to them, will influence user trust and privacy concerns. Stakeholders must work carefully with the media in order to highlight successful efforts in cybersecurity and simply explain security and privacy threats as they arise.

Strengthen online privacy and Internet trust through their own actions, not weaken them.

Many stakeholders contributed to users' distrust in the Internet and their growing online privacy concerns. Governments, Internet companies, and social media companies were all cited as a cause for concern by a majority of survey respondents.

To improve their own actions or policies, stakeholders should:

- **Implement cybersecurity best practices.** Utilizing cybersecurity best practices can help mitigate cyber threats to their users and to stakeholders themselves. Clearly demonstrating the implementation of best practices, will be crucial to addressing data security concerns and Internet distrust among users.
- **Practice strong privacy and data handling hygiene.** Where stakeholders collect, handle, or process user data, they must do so with fairness, transparency, simplicity, respect, and provide genuine choices for users around how their data is collected.
- **Address pervasive surveillance.** Governments, both domestic and foreign, are a source of Internet distrust and online privacy concerns. Governments must move away from a model of pervasive surveillance, and other stakeholders should take steps to improve the confidentiality and integrity of digital communications.

Foster more reliable and secure networks.

The perceived unreliability and insecurity of the Internet were a major source of distrust in the Internet for respondents in 2019. In 2018, Internet shutdowns, routing incidents, and cyberattacks disrupted Internet access for users around the globe.

To improve the security and reliability of networks, stakeholders should:

- **Invest in in local and regional ICT infrastructures that improve Internet reliability.** Particularly in developing economies, where network resiliency may be lower, improving infrastructure and redundancy is crucial to improving internet reliability. For example, stakeholders can support the development of Internet exchange points, new international gateways and content delivery networks in their economies.
- **Avoid Internet shutdowns.** Internet shutdowns have far-reaching, economic and technical impacts. They undermine users' trust in the Internet, setting in motion a whole range of consequences for the local economy, the reliability of critical online government services, and even the ease of doing business in the country. Stakeholders, particularly governments, must avoid engaging in Internet shutdowns.

Conclusion

At its core, the Internet is a network of thousands of independent networks relying on open standards and trusted relationships to send data around the globe. Yet, for many, this is not the Internet they know or understand. For some, the Internet may be the World Wide Web, for others a set of social media platforms, or something else altogether. For some, the Internet is trustworthy and privacy respecting, but for others this is not the case at all.

How people perceive the Internet matters. While the Internet may provide the building blocks, its true value is in what users make of it. When privacy fears and distrust negatively influence users, they negatively affect the future of the Internet. Each of us have a role in improving security and privacy online, and helping ensure that the Internet is a source of hope, not fear, for all.