FOR RELEASE AUGUST 10, 2017

The Fate of Online Trust in the Next Decade

Many experts say lack of trust will not be a barrier to increased public reliance on the internet. Those who are hopeful that trust will grow expect technical and regulatory change will combat users' concerns about security and privacy. Those who have doubts about progress say people are inured to risk, addicted to convenience and will not be offered alternatives to online interaction. Some expect the very nature of trust will change.

BY *Lee Rainie and Janna Anderson*

FOR MEDIA OR OTHER INQUIRIES:

Lee Rainie, Director, Internet, Science and Technology research
Janna Anderson, Director, Imagining the Internet Center, Elon University
Tom Caiazza, Communications Manager
202.419.4372

www.pewresearch.org

RECOMMENDED CITATION

Pew Research Center, August 2017, "The Fate of Online Trust in the Next Decade" Available at: http://www.pewinternet.org/2017/08/10/the-fate-of-online-trust-in-the-next-decade/

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. The center conducts public opinion polling, demographic research, content analysis and other data-driven social science research. It studies U.S. politics and policy; journalism and media; Internet, science and technology; religion and public life; Hispanic trends; global attitudes and trends; and U.S. social and demographic trends. All of the center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

For this project, Pew Research Center worked with Elon University's Imagining the Internet Center, which helped conceive the research, collect, and analyze the data.

The Fate of Online Trust in the Next Decade

Many experts say lack of trust will not be a barrier to increased public reliance on the internet. Those who are hopeful that trust will grow expect technical and regulatory change will combat users' concerns about security and privacy. Those who have doubts about progress say people are inured to risk, addicted to convenience and will not be offered alternatives to online interaction. Some expect the very nature of trust will change.

Trust is a social, economic and political binding agent. A vast research literature on trust and "social capital" documents the connections between trust and personal happiness, trust and other measures of well-being, trust and collective problem solving, trust and economic development and trust and social cohesion. Trust is the lifeblood of friendship and caregiving. When trust is absent, all kinds of societal woes unfold – including violence, social chaos and paralyzing risk-aversion.

Trust has not been having a good run in recent years, and there is considerable concern that people's uses of the internet are a major contributor to the problem. For starters, the internet was not designed with security protections or trust problems in mind. As Vinton Cerf, one of the creators of internet protocols, put it: "We didn't focus on how you could wreck this system intentionally." (Cerf is a respondent to the question addressed in this report; his worried quote is featured here).

Moreover, the rise of the internet and social media has enabled entirely new kinds of relationships and communities in which trust must be negotiated with others whom users do not see, with faraway enterprises, under circumstances that are not wholly familiar, in a world exploding with information of uncertain provenance used by actors employing ever-proliferating strategies to capture users' attention. In addition, the internet serves as a conduit for the public's privacy to be compromised through surveillance and cyberattacks and additional techniques for them to fall victim to scams and bad actors.

If that were not challenging enough, the emergence of trust-jarring digital interactions has also coincided with a sharp decline in trust for major institutions, such as government (and Congress and the presidency), the news media, public schools, the church and banks.

The question arises, then: What will happen to online trust in the coming decade? In summer 2016, Pew Research Center and Elon University's Imagining the Internet Center conducted a

large canvassing of technologists, scholars, practitioners, strategic thinkers and other leaders, asking them to react to this framing of the issue:

> ***Billions of people use cellphones and the internet now and hundreds of millions more are expected to come online in the next decade. At the same time, more than half of those who use the internet and cellphones still do not use that connectivity for shopping, banking, other important transactions and key social interactions. As more people move online globally, both opportunities and threats grow. Will people's trust in their online interactions, their work, shopping, social connections, pursuit of knowledge and other activities be strengthened or diminished over the next 10 years?***

Some 1,233 responded to this nonscientific canvassing: **48%** chose the option that trust will be strengthened; **28%** of these particular respondents believe that trust will stay the same; and **24%** predicted that trust will be diminished. (See "About this canvassing of experts" on Page 28 for further details about the limits of this sample.)

Participants were asked to explain their answers and were offered the following prompt to consider: *Which areas of life might experience the greatest impact? Economic activity? Health care? Education? Political and civic life? Cultural life? Will the impacts be mostly positive or negative? What role might the spread of blockchain systems play?*

Many of these respondents made references to changes now being implemented or being considered to enhance the online trust environment. They mentioned the spread of encryption, better online identity-verification systems, tighter security standards in internet protocols, new laws and regulations, new techno-social systems like crowdsourcing and up-voting/down-voting or challenging online content.

One particular focus of participants' answers involved blockchain technology, because our follow-up prompt specifically asked people to consider the role of blockchain in the future of trust on the internet. Blockchain is an encryption-protected digital ledger that is designed to facilitate transactions and interactions that are validated in a way that cannot be edited. Proponents have high hopes for the spread of blockchains. The Economist magazine has argued that blockchain "lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority …. In essence it is a shared, trusted, public ledger that everyone can inspect, but which no one single user controls." A more-complete outline of how blockchain operates and these survey

respondents' predictions about its future can be found in the discussion about Theme 4 later in this report.

The majority of participants in this canvassing wrote detailed elaborations explaining their positions. Some chose to have their names connected to their answers; others opted to respond anonymously. These findings do not represent all possible points of view, but they do reveal a wide range of striking observations. Respondents collectively articulated six major themes that are introduced and explained below and are expanded upon in sections that begin on Page 33 of this report.

Six major themes on the future of trust in online interactions

Theme 1 **Trust will strengthen because systems will improve and people will adapt to them and more broadly embrace them**

- Better technology plus regulatory and industry changes will help increase trust
- The younger generation and people whose lives rely on technology the most are the vanguard of those who most actively use it, and these groups will grow larger

Theme 2 **The nature of trust will become more fluid as technology embeds itself into human and organizational relationships**

- Trust will be dependent upon immediate context and applied differently in different circumstances
- Trust is not binary or evenly distributed; there are different levels of it

Theme 3 **Trust will not grow, but technology usage will continue to rise, as a "new normal" sets in**

- "The trust train has left the station"; sacrifices tied to trust are a "side effect of progress"
- People often become attached to convenience and inured to risk
- There will be no choice for users but to comply and hope for the best

Theme 4 **Some say blockchain could help; some expect its value might be limited**

- Blockchain has potential to improve things
- There are reasons to think blockchain might not be as disruptive and important as its advocates expect it to be

Theme 5 **The less-than-satisfying current situation will not change much in the next decade**

Theme 6 **Trust will diminish because the internet is not secure, and powerful forces threaten individuals' rights**

- Corporate and government interests are not motivated to improve trust or protect the public
- Criminal exploits will diminish trust

PEW RESEARCH CENTER and ELON UNIVERSITY'S IMAGINING THE INTERNET CENTER

The following introductory section presents an overview of the themes found among the written responses, including a small selection of representative quotes supporting each point. Some comments are lightly edited for style or due to length.

Theme 1: Trust will strengthen because systems will improve and people will adapt to them and more broadly embrace them

About half the respondents to this canvassing believe that trust online will be strengthened in the next decade. Their reasoning generally flows in two streams: **1)** Some expect to see improved technology emerge that will allow people to have confidence in the organizations and individuals with whom they interact online. They argue that improvements in identifying and authenticating users will build trust. They also maintain that the corporations depending on online activity have all the incentive they need to solve problems tied to trust. **2)** Some say trust will grow stronger as users employ online activities more fully into their lives. They think this will be led by younger users who are fully immersed in online life.

Adrian Hope-Bailie, standards officer at Ripple, replied, "The technology advancements that are happening today are beginning to bring together disparate but related fields such as finance, identity, health care, education and politics. It's only a matter of time before some standards emerge that bind the ideas of identity and personal information with these verticals such that it becomes possible to share and exchange key information, as required, and with consent to facilitate much stronger trusted relationships between users and their service providers."

Stephen Downes, researcher at National Research Council Canada, wrote, "We experience many reasons to distrust our interactions. And traditional media are reporting numerous cases where they should be distrusted, so we think rising distrust is the norm. And yet, on a personal basis, as time goes by, we are more and more trusting. People who did not even know people in other countries, much less trust them, now travel halfway around the world to participate in conferences, rent and live in their homes, meet on a date, participate in events and more. Sure, things like catfishing are problems. But the exception is a problem only in the light of the trust that is the rule (Wittgenstein: A rule is shown by its exceptions). People who did not trust online retail a decade ago now purchase games, music and media on a regular basis (they're still a bit wary of deliveries from China, but they're coming around to it). People who did not trust online banking a decade ago now find it a much more convenient and inexpensive way to pay their bills. They also like the idea that their credit

cards are now protected. People who were sceptical of online learning a decade ago now live in an era when, in some programs, some online learning is required, and where there is no real distinction (and no way to distinguish) between an online or offline degree (and meanwhile, millions of people flood in to take MOOCs). We can see where this trend is heading by looking at a few edge cases. For example: What would we say of a pilot who never trained in a simulator? What would we say of a lawyer who did not rely on data search, indexing and retrieval services? We trust them more in the future because they are taking advantage of advanced technology to support their work."

David Karger, professor of computer science at MIT, urges a "healthy distrust" and encourages the public be more vigilant in working to understand the risks and limitations of emerging technologies. "We've seen tremendous growth in use of these online tools," he wrote, "so it is natural to assume it will continue. Your specific question of trust is a complicated one. On the one hand, I believe we are just at the beginning of development of good online tools and I expect significant improvement – even over the next 10 years – that will draw more users to these better tools. On the flip side, I at least *hope* that people will become generally more educated about the risks and limitations of online interactions, which may lead to a certain healthy distrust even as usage becomes more widespread."

Subtheme: Improved technology plus regulatory and industry changes will help increase trust

Many technologists and futures thinkers among the respondents said they expect that constantly evolving improvements in the network of networks will maintain or boost trust; some also added that security cannot be completely perfected and staying ahead of the "darker forces" will require vigilance. Some suggested regulation. An **anonymous respondent** said, "Trust will be increased if governments put in place policies for consumer protection, data protection, etc."

Mike Roberts, Internet Hall of Fame member and first president and CEO of ICANN, wrote, "The designers, developers and users of computer-based systems are still in a primitive era. From an S curve perspective, we are hardly at the steep lower-left end. The rise of an entrepreneurial culture among developers has accelerated the diffusion of these systems but there is far to go. Because of the tangible benefits in convenience, quality, quantity, etc., of using such systems, humans will develop advanced techniques for protection from criminal behavior on the 'net,' but such activity will persist online as it does offline. You don't stop going to the grocery store because there was a carjacking incident last week, etc."

Richard Adler, distinguished fellow at the Institute for the Future, observed, "Technologies such as biometrics, encryption, digital IDs, blockchain and smart contracts are emerging that can enhance security and build trust. But they are in a race with darker forces who continue to become more effective in breaching security measures. We need to get serious about creating a truly secure internet if it is to realize the potential for empowering a big portion of the world."

Oscar Gandy, emeritus professor of communication at the University of Pennsylvania, commented, "Of course, as a privacy and surveillance scholar, my answer is more hopeful than analytical. I am hopeful that the public will become much more aware, and less 'resigned' to the fact that their transaction-generated information (TGI) is routinely used to shape their experience within economic, social and political markets/environments. These areas of impact are tightly interconnected, although some analytical assessments can determine differential influences for different population segments. I am most concerned about the nature and extent of surveillance and the strategic use of TGI in the public sphere, or in 'political and civic life.' Hopefully, the public will come to understand the myriad ways through which their TGI is used to shape the information environment in which they make important choices, including those we would identify as being political. What I have seen of late leads me to see the balance between benefits and harms in the political area to be largely negative, and worsening."

Hume Winzar, associate professor in business at Macquarie University in Australia, wrote, "Governments and financial companies want their systems secure and transparent, so they will work hard to make them so. This will relieve people's concerns. Also, many services will be simply unavailable except online, so people will have to trust them whether they're skeptical or not."

Subtheme: The younger generation and people whose lives rely on technology the most are the vanguard of those who most actively use it, and these groups will grow larger

Some respondents observed that familiarity breeds acceptance, thus those who are younger and have spent most of their lifetimes immersed in implementing online are those least likely to see trust issues as a reason to deny themselves the affordances of online life. One noted it will be "like the air we breathe."

Glenn Ricart, Internet Hall of Fame member and founder and chief technology officer of U.S. Ignite, said, "Trust will be strengthened over the next decade because there is a strong

generational shift to interacting online. The expectation of Millennials and others is that they can and should be able to trust online transactions. That expectation will provide fuel to efforts improving trust."

David Durant, a business analyst for the UK Government Digital Service, wrote, "People who have grown up using mobile technology for social media, interaction with businesses and increasingly as a way to interact with government will see doing so as entirely normal and consider it the natural channel for a very significant proportion of all their life's interactions."

Sam Anderson, coordinator of instructional design at the University of Massachusetts, Amherst, wrote, "The internet will be so ubiquitous that it will be like the air we breathe: Bad some days, good others, but not something we consciously interrogate anymore."

Theme 2: The nature of trust will be more fluid as technology embeds itself into human and organizational relationships

One striking line of argument, particularly among some of the most prominent analysts responding to this canvassing, is that trust will become a more conditional and contextual attribute of users' online behavior. They argue that trust is becoming "transactional" – an idea distinct from the notion that trust is a kind of property tied to an individual, group or organization. A number of respondents added that throughout human history the highest levels of trust are often found within personal networks, rather than via organizational actors.

Dan McGarry, media director at the Vanuatu Daily Post, wrote, "Trust will change in its nature. It will no longer be invested so much in systems and institutions as in individuals. Relationships will matter. On the negative side, much behaviour will be defined by allegiance, which will allow some actors to motivate significant numbers to act against their own interests at times. The human capacity to invest trust in others won't change unless we undergo significant evolutionary change."

Cory Doctorow, writer, computer science activist-in-residence at MIT Media Lab and co-owner of Boing Boing, responded, "The increased impoverishment/immiseration of larger and larger segments of society thanks to mounting wealth inequality will drive more reliance on informal networks, barter, sharing, etc., that will be enabled through online activity."

Subtheme: Trust will be dependent upon immediate context and applied differently in different circumstances

While many institutions have gained the public's trust over time, many are now being questioned. Some respondents say that individuals' influence has gained more importance in this atmosphere, and trust is – now and in the coming decade – more likely to be applied differently to different circumstances. An **anonymous respondent** replied, "The change will be in the dynamism of trust, not the valence. We will place small amounts of trust in people and organizations and exit or voice more quickly when we sense it has been violated."

danah boyd, founder of Data & Society, commented, "Actually, trust will be both strengthened and diminished [in the coming decade], depending on context. People will stop seeing it as 'the internet' and focus more on particular relationships. Increasingly, large swaths of the population in environments where tech is pervasive have no other model."

Aaron Chia Yuan Hung, assistant professor at Adelphi University, replied, "People will change *what* they trust. Just as people used to prefer an oral agreement over a signature in the past, people grow to accept what they can or are willing to trust. People are also likely to believe what they want to believe because confirmation bias is inherently human nature. Farhad Manjoo's 'True Enough' is a wonderful read on this topic. It does make critical thinking more difficult, and education must play a big role in making sure people look at people, facts, data, etc., with a more analytic lens."

Subtheme: Trust is not binary or evenly distributed; there are different levels of it

Bob Frankston, internet pioneer and software innovator, commented, "The choices for the question are too limited. Trust is not binary. We need to have new forms of trust and Plan B's for when trust fails. This is where algorithms can help – as with credit card companies seeing patterns – but it cuts both ways."

Andrew Walls, managing vice president at Gartner, said, "Trust is not achieved merely through effective implementation of security processes and systems. Trust is a quality of a relationship between two entities. Trust is also both a conscious and unconscious attribute of a relationship. For example, many people state that they do not trust Facebook, yet the behavior of those same people demonstrates that they entrust Facebook with many details of their lives. It is possible to claim that these people do not understand the 'trust' ramifications and implications of their sharing behavior in social media, but that same claim can be made of every social interaction, online or otherwise. Rather than speak of trust as an absolute or binary situation (trusted or untrusted), trust must be viewed as a spectrum or continuum

with multiple levels. For example, I might trust a bank with my money, but I do not trust them with the details of my social life, whereas, I won't trust my cousin with my money but will trust him/her with details of my social life. Trust is a subtle, dynamic attribute of social relationships between entities."

Theme 3: Trust will not grow, but technology usage will continue to rise, as a 'new normal' sets in

Are people "placing trust" in a technology when they use it or are they just willingly taking a chance in order to obtain or attain something they desire? A significant share of participants think it is the latter. They argued that the level of online activity by 2026 might make it *appear* as if the level of trust is fairly high, but the more appropriate way to interpret it will be that people are resigned to operating in an environment that does not allow them to be selective about whom they trust.

Ebenezer Baldwin Bowles, founder of Corndancer.com, wrote, "Trust will be strengthened, but it will be blind trust enforced by the ceaseless demands of The System, hell-bent to drive everyone online. 'Resistance is futile,' the alien superpower said to the altruistic starship captain. Resistance to the interests of the corporate state will be futile if one wants to participate in the commonplace activities of household management and personal finances, or seek diagnosis and treatment from medical practitioners, or pass a bricks-and-mortar course in high school or university."

David Sarokin, author of "Missed Information: Better Information for Building a Wealthier, More Sustainable Future," wrote, "I'm not sure 'trust' is the right word here. It's more a matter of attrition and familiarity. As more and more activities migrate online, and as ever larger numbers of people simply grow up with the internet, it seems inevitable that its use will expand, both in terms of overall numbers of people using it [and] the types and scopes of activities available."

An **anonymous research professor** proclaimed, "Trust is dead now. Thus, it will stay the same: Dead."

An **anonymous respondent** wrote, "The general public trust in these systems will grow … but the question of whether such trust will be deserved … remains to be seen. Call it trust by default, in the same way we are powerless to criticize a surgeon's or airline pilot's technical maneuvers."

Subtheme: 'The trust train has left the station'; sacrifices tied to trust are a 'side effect of progress'

Some respondents argued that trust cannot be assumed to be an element of transactions, and many who used the word "trust" in saying they expect higher participation in online interaction may likely agree that their use of it was as a slightly inaccurate umbrella term used to match up with the language of the survey question and that it actually might signify they see a likely rise in people's participation, trusting or not.

An **anonymous chief marketing officer** commented, "The trust train has left the station, continues to gain speed, and shows very little chance of slowing down. As mobile payment technology proliferates, from our phones to our watches to our Internet of Things devices, and as digital natives continue to grow in their share of the world's economic power, concerns about trust in online interactions will seem antiquated and quaint. Breaches may continue and even proliferate, but the technologies will be so embedded in our lives that they will be considered a mere inconvenient side effect of progress."

Brad Templeton, chair for computing at Singularity University, wrote, "Trust will be strengthened even though that may be an unjustified trust. Our systems are today extremely insecure and we trust them, and those who are not using them are not staying away because of [a lack of] trust. Also, I think billions more will come online, not hundreds of millions. Biggest impacts will be in economic activity and cultural life."

Bart Knijnenburg, assistant professor in human-centered computing at Clemson University, responded, "Secure technologies will not do much to increase trust, because most people simply don't understand them. They will just run in the background."

Peter Levine, Lincoln Filene professor and associate dean for research at Tisch College of Civic Life, Tufts University, said, "I suspect that people will gain trust in electronic tools, per se, so that more people will be willing to bank, vote, shop, etc., online. But distrust in the underlying institutions continues to grow, and I am not particularly optimistic that it will change."

Subtheme: People often become attached to convenience and inured to risk

Convenience is one of the most-recognized features of all new technologies, including the internet. A number of respondents made the case that it is the convenience of using popular internet applications that makes the internet most appealing and addictive. Further, they noted that it is convenience that creates the most challenges for internet users when it comes

to trust. In making trust decisions, people weigh risk and reward and generally choose reward.

An **anonymous respondent** adapted a classic line from U.S. history, writing: "Give me convenience or give me death."

Tom Ryan, CEO of eLearn Institute Inc., replied, "'Trust' is neither the inhibitor nor driver for adoption of online interactions. Convenience will drive adoption. For example, motor vehicle deaths in the U.S. reached as high as 51,091 in 1980 and still remain over 30,000 deaths annually, yet the number of vehicles registered in the U.S. continues to grow. People accept the life-or-death consequences of driving for the convenience it provides. I recognize the threat that a hacker and some businesses may pose, through internet access, of my health and financial data, but the convenience and benefit I perceive keeps me online."

An **anonymous respondent** noted, "People will distrust more and more and still accept the use of these systems more and more."

An **anonymous network architect at Vodafone** noted, "For the reasons trust will be strengthened refer to Cory Doctorow's 'peak indifference' essay."

Louisa Heinrich, founder at Superhuman Limited, wrote, "I fear trust will be diminished (i.e., we will be certain we are being watched, that our communications and interactions are not secure) but we will use the technology anyway, either because we have no other choice or because it's just too convenient."

Subtheme: There will be no choice for users but to comply and hope for the best

Some respondents noted that there will be no alternative but to use online systems, whether they trust them or not – and many who use them will not necessarily do so because they "trust" them.

An **anonymous respondent** commented, "When compliance can be mechanically enforced at scale, trust is unnecessary."

Randy Bush, research fellow at Internet Initiative Japan and Internet Hall of Fame member, wrote, "Given that there will be less and less alternatives to electronic paths to daily transactions, people will have no choice but to 'trust' them. But they will remain nervous, with justification."

Naomi Baron, a linguistics professor at American University, replied, "To the extent that more and more people use the internet for these kinds of connectivity, logic suggests we conclude that trust in the system will be strengthened. However, I suspect that what in fact will be happening is that people will increasingly stop thinking about the trust issue, sensing they have no other option but the internet for conducting the business of daily life. Much as internet users today commonly believe they have no choice when it comes to giving up privacy, I predict users will feel the same way about trust."

Tony Pichotta, creative director at Recess Creative, replied, "Online interactions will be strengthened because of the lack of alternatives. Systemic technologies will shape the masses, leaving the dissenters out in the wilderness."

An **anonymous researcher at the MIT Center for Civic Media** said, "Trust is less relevant when there is no need to develop loyalty because there are no alternatives. We will use what we have available and mistrust it because there won't be obvious incentives for service providers to work in our favor. Worldwide, people will increasingly use cellphones and the internet to do work, shop, engage socially and learn. People will use these services because they have no choice, as the services will not be available offline as it's too expensive to maintain brick and mortar (something we are seeing in banking, retail and government services). And there will be few options because value is determined by the network effects leveraged by many companies."

Theme 4: Some say blockchain could help; some expect its value might be limited

One of the most interesting developments online in the past decade has been the rise of blockchain systems, which were first created to enable the use of the digital currency bitcoin. Blockchain product designer Collin Thompson describes blockchain as "a type of distributed ledger or decentralized database that keeps records of digital transactions. Rather than having a central administrator like a traditional database – think banks, governments and accountants – a distributed ledger has a network of replicated databases, synchronized via the internet and visible to anyone within the network." He elaborates on the blockchain process:

> "When a digital transaction is carried out, it is grouped together in a cryptographically protected block with other transactions that have occurred in the last 10 minutes and sent out to the entire network …. The validated block of transactions is then timestamped and added to a chain in a linear, chronological

> order. New blocks of validated transactions are linked to older blocks, making a chain of blocks that show every transaction made in the history of that blockchain. The entire chain is continually updated so that every ledger in the network is the same, giving each member the ability to prove who owns what at any given time."

Such a dependable ledger could conceivably be used for securing any kind of transaction, and that has prompted advocates to argue that it could replace the kinds of activities now performed by trusted – and expensive – intermediaries such as banks, firms that validate real estate transactions, accounting operations and legal services.

Of course, this might powerfully affect the overall level of trust in online interactions, thus we asked respondents to consider in their written elaborations the impact of blockchains on trust in the next decade. A number were quite positive, but some expressed reservations about how rapidly and effectively blockchains would be adopted.

Susan Price, digital architect at Continuum Analytics, said, "Blockchain technologies hold the most promise for making such a trust system possible. Much will depend on the first few popular examples. Although blockchains so far remain robustly secure, systems that interface with and leverage them are subject to the same security problems we're familiar with (e.g., Ethereum's DAO recursive hack). Let's assume blockchain technologies and related will make such a trust system possible. Individuals could conduct secure trades with one another without the use of intermediaries, or with intermediaries operating at greatly reduced costs. More people worldwide could find sustaining outlets for their creativity and endeavors. The financial services industry will be revolutionized and reinvented. With little to no 'float' for exchanges of value, whole sectors such as clearinghouses will vanish. Citizens of countries where payments are most delayed today will enjoy faster settlement and thus their citizens enjoy less graft and corruption and benefit more directly from their productivity. Voting and civil rights will be completely transformed. It will be feasible for political structures to transcend geography. Though we'll still need local law enforcement and security forces, we could choose to become 'citizens' of organizations with specific goals, agendas and benefits that align with our needs and beliefs regardless of our current location or residence. This could speed human rights advances and productivity even more. Health care and advances in medical technology and solutions would evolve more quickly and be available to more people. This utopian view assumes that the identity interface remains outside the direct control of any corporation or government. Distributed control over such a system is vital to prevent abuses (or to recover from power plays or attacks)."

Marcel Bullinga, trend watcher and keynote speaker, wrote, "Strengthened trust is my hope, not a prediction. It is the great promise of blockchain of course, in combination with a host of other privacy and trust technologies, that it will make trusted peer-to-peer transactions possible. This is not in the interest of current technology companies and powerful platforms like Google, Facebook and Uber, so it will be heavily battled. Yet, it would revolutionize our economy into a true, trusted DIY world."

Lee McKnight, associate professor at Syracuse University's School of Information Studies, replied, "Trust can only be strengthened when people and systems actually have a reason to trust each other more. With bots attempting every 14 seconds to break into *every* large enterprise, it would be foolish to trust more. (In a decade we can only assume attacks will be even more frequent.) Still, in a re-architected information environment, properly designed systems, services, devices and networks supporting organizations with information-security awareness embedded in the organizational culture can do a much better job of distinguishing between that which they can trust and that which they do not know. Online transaction volumes will continue to grow, even as malicious insiders, bots, criminal gangs and nation-states also grow. Blockchain technology is an incredibly promising piece of a much bigger conundrum. Secure irrevocable ledgers are a great accounting mechanism without which the Internet of Things should not be trusted. But, as continued hacks of Bitcoin indicate, a secure ledger pointing to resources of value can also be used as a map to point out to thieves and bots where the money is."

Subtheme: There are reasons to think blockchain might not be as disruptive and important as advocates hope

Some respondents in this canvassing expressed doubts about the efficacy of blockchain.

Jerry Michalski, founder at REX, wrote, "Trust will grow, but not because organizations delivering services will be more trustworthy. Instead, systems will become more robust and we humans will become more acclimated to what they do. Our resistance will weaken. Our appetites will be whetted. Cybersecurity breakdowns do not seem to be hurting public confidence much. The blockchain may shift trust considerably, away from traditional institutions and out to the open ledger. But the blockchain is an act of faith as well, and may end up as flawed as previous platforms have been."

Gus Hosein, executive director at Privacy International, commented, "Oh, stop talking about blockchains – it's just the latest in the trend of 'tech X shall solve woe Alpha.' We have

the knowledge and the capabilities with technologies that have been around for years but a lack of imagination and political understanding has inhibited useful dispersion."

Theme 5: The less-than-satisfying current situation will not change much in the next decade

About a quarter of respondents to this canvassing predicted that trust will stay about the same in the next decade. They generally see a persistent arms race between those trying to exploit the vulnerabilities of the internet – regularly shattering the trust of at least some users – and those trying to fight back. They see no end to cybersecurity problems.

Jason Hong, associate professor at Carnegie Mellon University, noted, "The main reason trust won't advance significantly in the near future is cybersecurity. Every single week there is news about some new massive data breach or malware attack. These kinds of cybersecurity problems rightfully erode people's trust in the internet, and they are only getting worse over time as script kiddies, criminals and state-sponsored hackers get more sophisticated."

Charlie Firestone, communications and society program executive director and vice president at The Aspen Institute, wrote, "Security measures and hacking are in an arms race. For every advance there will be setbacks. I expect the balance to remain about where it is, with peaks and valleys as the race continues. With trust, people will increase use of online media for transactions. Blockchain technology is a net plus in this ongoing saga."

K.G. Schneider, a higher-education administrator, wrote, "We will see the same cycles of increasing trust followed by breaches followed by new technologies."

Ian Peter, an internet pioneer and historian based in Australia, wrote, "Trust is currently rather low and I expect it to stay that way, while, paradoxically, usage is likely to rise dramatically. Despite their mistrust, people are likely to give more weight to the convenience of online transactions than they to do the risks involved."

Theme 6: Trust will diminish because the internet is not secure and powerful forces threaten individuals' rights

A number of the most highly respected experts, many of whom preferred to remain anonymous in answering, were among the quarter of respondents who said they expect trust will actually diminish over the next decade. They listed various reasons, but those cited most often were: **1)** Corporate business models are tuned to profit-making and government motivations tend toward national security, leaving little attention paid to individuals' rights

to personal privacy and personal security protections. **2)** The internet was not created with trust-building in mind, and criminal exploits and other manipulative gaming of networks by political and social actors are expected to rise, possibly exponentially, in the future.

Vinton Cerf, vice president and chief internet evangelist at Google, co-inventor of the Internet Protocol and Internet Hall of Fame member, noted, "Trust is rapidly leaking out of the internet environment. Unless we strengthen the ability of content and service suppliers to protect users and their information, trust will continue to erode. Strong authentication to counter hijacking of accounts is vital."

Marc Rotenberg, executive director of the Electronic Privacy Information Center, commented, "Technology is far outpacing security, privacy and reliability. The problem will intensify with the Internet of Things, as the internet connects more machines in the physical world."

Richard Stallman, president of the Free Software Foundation and Internet Hall of Fame member, wrote, "I expect people will learn to distrust online commerce more, as they see servers will be cracked and their personal information will become available to bad actors (both criminals and states)."

Subtheme: Corporate and government interests are not motivated to improve trust or protect the public

Henning Schulzrinne, a professor at Columbia University and Internet Hall of Fame member, wrote, "Under the current system, almost all the risks of breaches are borne by individuals, particularly in terms of time and effort of fixing problems. Data once leaked cannot be un-leaked. I'm assuming that the current sorry state of system security will persist, with buggy IoT [Internet of Things] software, slow upgrades of Android and websites that are still subject to SQL injection and other common programming problems. Currently, blockchain systems do not seem to address any real problems, except if you are in the business of distributing ransomware."

Jim Warren, longtime technology entrepreneur and activist, responded, "As much as I use, enjoy and am mostly an enthusiastic user of online interactions, sadly, I have to say that it is becoming more and more difficult to do many of them in a reliably secure fashion. Assuring that such interactions are *surely* reliable and secure is *not* easy, and perhaps impossible. It certainly doesn't help when governments do everything possible to make sure that such activities – notably some 'types' of communications – are difficult or impossible. No matter

how much it *might* – and often might *not* – help governments protect their citizens (or too often much more important to them, protect themselves and those who govern)."

Dave Burstein, editor at Fast Net News, observed, "Surveillance is the biggest obstacle to trust. It will increase as countries other than the U.S. deploy the tools. Multinationals like Facebook and Google/Doubleclick will become even more effective at tracking, and they will be ubiquitous."

An **anonymous professor of digital media at an Australian university** wrote, "The internet will be a less open and diverse environment in the next decade. Facebook will be as likely to control [the internet] as a distributed system like blockchain."

An **anonymous systems engineer** observed, "Corporate greed prevents things from being done well/secure."

Alf Rehn, professor and chair of management and organization at Åbo Akademi University in Finland, said, "Call it the iron law of internet trust – with more engagement comes more chances of glitches and hacks, which means that intelligent distrust will be a civic skill just like media literacy."

An **anonymous freelance consultant** commented, "Trust will be strengthened *if and only if* the door is opened to effective, open-source security and corporate and government liability for security negligence. Current trends are the opposite, making security research illegal with the TPP (Trans-Pacific Partnership) and other trade deals, DRM (Digital Rights Management), etc. Transparency is necessary. We've known for centuries that markets are only effective when there is trust backed up by rule of law. When laws prevent effective security, we destroy trust and thus destroy markets. We're on the wrong path."

An **anonymous programmer and data analyst** said, "Corporations grant us access to technology and services in order to increase revenue. This will not change, as the basic infrastructure of the internet is not amenable to privacy and security. Instead we've seen a series of patchwork solutions that ultimately always fail or are subverted. Without a total rebuild of the internet itself this will not change, therefore, trust is an illusion."

An **anonymous respondent** said, "The internet is a security [farce]. Everyone knows that. The NSA [U.S. National Security Agency] is logging this right now. I'm sure three Russian mobs already have all my passwords."

Some respondents predict the public's dismay and distrust could lead to "rebellion." An **anonymous senior software engineer at Microsoft** said, "We will trust the experiences less as the larger structures (corporate, government) try to remain in control, yet we will become more dependent on them than ever through the pervasiveness (i.e., online micropayments) and lure (i.e., virtual reality). It will be a phase of a love-hate relationship which could cause rebellion against the system."

Subtheme: Criminal exploits will diminish trust

While some optimistic respondents whose remarks are included in earlier segments of this report believe that technological solutions will upgrade trust by 2026, many of these respondents have no faith in rescue by tech. An **anonymous computer scientist** commented, "We are now paying the 'technical debt' for an internet that lacks essential facilities for security (e.g., association control). The 'attack surface' is growing faster than our ability to protect it; complexity is growing due to shoddy science and poor programming. There is no magic solution in tech itself; it is a process and culture change, rather like how financial services regulation has matured in response to past crises."

Raymond Plzak, former CEO of a major regional internet governance organization, commented, "Trust will be diminished. It is eroding now. There are too many instances of abuse and misuse today."

Jan Schaffer, executive director at J-Lab, replied, "It just appears that anyone and anything can be hacked and likely will be eventually. It's hard to figure out how to put that trust back in the bottle."

An **anonymous project manager** said, "Online security is a complex problem that depends on human behavior to function. With so much infrastructure moving online and a lack of focus on re-engineering our systems with security and privacy at their heart, a string of high-profile failures will taint these new technologies for years to come."

Another **anonymous respondent** wrote, "The dystopian, tiered future of science fiction is going to be considered a quaint underestimation. There will be a hated elite of genuinely computer-literate people who will be relied upon to maintain the oligarchical power structure we have now.

A third **anonymous respondent** observed, "The intrusion of networked computing into many new areas, such as digitally networking hospitals for diagnostic imaging, self-driving

cars, creates the potential for a startling security threat that could cause widespread chaos. This is not a new idea. Clifford Stoll's book 'The Cuckoo's Egg' (1989) pointed out that the hackers infiltrating his Unix system could just as well have been infiltrating the operating system of a gamma camera or other clinical system. We know that many governments are putting efforts into cyberwarfare. This offers another avenue for disaster."

An **anonymous sociologist at the Social Media Research Foundation** commented, "Weaponized information systems will corrode the credibility of these systems. Once faith in the validity of network-delivered data is eroded, the entire superstructure of the network will collapse. If stock prices, weather reports and news articles are clearly seen to be manipulated and fraudulent, how will the means of communication survive?"

An **anonymous respondent** replied, "We create these processes with reactive technologies, not proactive, so the hackers will constantly be one step ahead. I don't see trust strengthening, or us winning on this one. Blockchain systems will hopefully help, but I firmly believe humans can outwit anything we come up with."

Beyond the major themes: Some broader explorations of trust

Beyond those pointed themes, some respondents wrote answers that looked at the grand sweep of the trust problem and how it will evolve.

The answer of **Susan Price**, digital architect at Continuum Analytics, had that tone and offered a solution: "The paradox is that in order for individuals to realize the incredible potential of technology, we must each uniquely self-identify. Doing so involves great risk. Individuals routinely surrender their rights and commit to legal agreements without studying or understanding the risks and value changing hands. What's needed is a system (a human application programming interface, or API) that gives individuals appropriate control over their online activities and the data that most closely concerns them. Corporations and governments could 'opt in' to support such a system, but must not be the primary creators or maintainers of it. Unless such a system is created and popularized, trust in online systems overall will diminish because governments will continue to violate citizens' privacy, hackers and thieves will thrive, and corporations will shift more and more of the burdens onto consumers. If an appropriate system emerges and everyone plays by the same rules, trust would ensue."

One **anonymous respondent** devised a human solution to the trust problem – one that might also have the virtue of creating a new category of jobs: "People will not have a choice.

Online/automated/precast dealings will be involuntary. One possible new future 'job' role: Personal Interactive Consultant (PIC). Someone who specializes in knowing you and your family in order to more effectively interface with companies/corporations/government. Kind of like we used to use travel agents and insurance brokers, and even lawyers, the PIC works as our advocate in order to get something done within an industry or institution that would otherwise be beyond the average person's ability or convenience level. The PIC probably would not be able to handle all interactions; the PIC would likely be a hired face for a large company with specialized resources to handle all types of inquiries and interactions. Let's call it a Lifestyle Information Management company (LIM). There already are PICs today, but on a smaller scale. And maybe LIMs already exist in some rudimentary form."

Another such sweeping answer came from an **anonymous institute director** who wrote, "All areas of life will be changed dramatically by data-driven algorithmic cognition and decision-making. The network will break down traditional social domains, such as business, politics, health care, education, science, etc. Networks cut across these domains and make them increasingly inefficient. There is no smart city without smart education, science, healthcare, business, etc. And smartness comes from integration of all data sources and networked infrastructures. Whether positive or negative is a pointless question. Who is to judge? According to what criteria? If you had asked the ancient Greeks whether the Roman Empire was positive or negative, would the question have made any sense? … The network norms of connectivity, flow, communication, participation, transparency, authenticity and flexibility will influence how society changes."

And a final thought along these lines was offered by **Tse-Sung Wu**, a project portfolio manager at Genentech, who said, "As long as access to and innovation in the internet and related devices remains relatively unfettered, it is likely more and more interactions will be mediated by these devices. All kinds of commerce, the provision of services and goods, health care, the sharing of ideas, teaching, leisure/entertainment, etc. Where it will break down is when we try to replicate a face-to-face interaction online but underestimate the breadth and depth of the face-to-face interaction. Technology is inherently reductionist, and we have many examples where this has failed us, or worse, it has failed us but we don't notice it till too late. Environmental crises are a perfect example: Technology mediates our relationship with the natural world, leading us to underestimate its value to our way of life. We have now evolved into a relationship with the natural world that is unsustainable, and this happened in part because technology has numbed us to signals that otherwise would have informed us to act differently. Online technology, insofar as it permeates all the spheres of human interaction, will likely do the same. The creation of online communities where people still feel lonely; the illusion of choice of the many potential dating/life partners, yet people stay single:

Many such contradictions will continue to abound because of reductionist, incomplete understanding of human interactions that form the basis of the technologies intended to replace them."

Responses from additional key experts regarding the future of trust in online activities

This section features responses by several of the many top analysts who participated in this canvassing. Following this wide-ranging set of comments, a much more expansive set of quotations directly tied to the six primary themes identified in this report begins on Page 34.

Distributed privacy, defensive agents and personal control can build trust

Jamais Cascio, distinguished fellow at the Institute for the Future, observed, "The strengthening of trust is contingent upon the lack of a big 'asteroid-impact' event, and assumes that the dynamics currently at play (tension between crime and law enforcement, surveillance and privacy, etc.) continue. Blockchain and similar technologies will help drive this increased trust, but not simply because of broader use of encryption. Blockchain, etc., will make possible truly novel approaches to banking, shopping, learning and nearly every other kind of online interaction. Distributed privacy, defensive personal software agents, and increased individual control over personal information will create new playing fields of transactions. Big corporations will leap at those fields, but won't be able to totally control them. The analogy here is the use of mobile phone minutes as a pseudo-currency in Africa, which started as a bottom-up, ad-hoc phenomenon. Formalization as mPesa and similar programs streamlined the process, but in this scenario ultimate control over the uses of the minute/currency would still rest in the hands of the users."

As data breaches rise, device use continues unabated due to convenience

Amy Webb, futurist and CEO at the Future Today Institute, observed, "Our trust in our devices tends to stay constant until a catastrophic event – like our accounts being hacked, or a national news story about surveillance, or our devices being stolen. And even then, our concern lasts only as long as we're dealing with the immediate consequences, such as having to change our passwords or canceling our credit cards. Paradoxically, in the past decade we have seen a dramatic increase in data breaches, and yet we continue to entrust our devices with our fingerprints, our faces, our heart rates, our exact locations and more – in addition to our credit card numbers and bank accounts. We willingly put our trust in our devices and digital networks when the benefits of convenience outweigh our fears about privacy. Over time, as our codependent relationship with our devices becomes more acute, the very notion

of privacy, and indeed its importance, begins to erode. Those areas of life that will ask for more and more of our personal data include health care, state and national government, travel, commerce, and of course, personal communications – technology companies and social networks. We will put up a fight unless the benefits are immediately understandable and daily life is little bit better for the exchange. This is why we hear people grumble about Facebook and Google's privacy policies, and we continue to use both – because they've become indispensable part of our lives. The fact that the government has access to similar personal data – in fact, some would argue it's less than what we're sharing with tech companies – continually enrages us. Why? Because we're not distracted by immediate, tangible benefits in exchange for our data."

'Social machine natives will trust their ubiquitously connected environment'

Jim Hendler, a professor of computer science at Rensselaer Polytechnic Institute, replied, "The issue isn't areas of application, but the socio-technical issue of the trust of users in the technology. Given that young children now increasingly have access to smartphones and computing, that access is becoming more ubiquitous, and that the use of these is increasing in all population sectors, it is clear that the generation growing up as 'social machine natives' (like digital natives, but more embedded in the social fabric) will age without the distrust their grandparents and parents may have had. Technologies like blockchain, etc., are enablers, but much as modern drivers have more trust in their vehicles without knowing how the engines function, social machine natives will trust their ubiquitously connected environment without needing to know the implementation details."

People will trust less when they learn more about the nature of the tech they use

John Markoff, retired senior writer at The New York Times, commented, "Inevitably as people learn more about the nature of the technology they are using their trust will decline."

Maybe a little reduction in trust could be healthy

Jonathan Grudin, principal researcher at Microsoft, commented, "This question should be prefaced by asking, 'Do people today trust in online interactions too much, too little or just the right amount?' Mass media stories make it clear that many people trust online media too much and come to regret it. A little reduction in trust could be healthy. The other questions are: Will online media become more trustworthy? Will most people become better at assessing when to trust it? It could become more trustworthy, but I won't hold my breath. I think people will become somewhat better at assessing trustworthiness."

A vast loss of agency accompanies the gain of convenience, a trade-off with limits

Doc Searls, journalist, speaker, and director of Project VRM at Harvard University's Berkman Center for Internet and Society, wrote:

"Phones are already extensions of our hands and minds. Yet they are also only a nine-year-old technology (dating from the advent of apps, in the summer of 2007), and dominated by handheld units that tend to be replaced by their owners about every 18 months. Meanwhile, the services behind many of the most-used apps are becoming more intelligent, complex and opaque about the full extent of what they are up to. We tend not to see these services' involvements with surveillance, manipulative algorithms, artificial intelligence and collaborations with parties unknown. For the most part this seems benign, but on the whole it masks a loss of agency behind a gain of convenience.

"At some point, however, this trade-off – which is one we never consciously made – will reach limits. It isn't clear yet what those will be, but the Faustian nature of this non-bargain will surely become manifest. This is when trust will break down. In fact it already has in the regulatory sphere. The abuses of surveillance capitalism (the term coined by Shoshana Zuboff of Harvard Business School) are well-known and highly irksome to lawmakers and regulators, especially in Europe. This is why, for example, we now have the General Data Protection Regulation (GDPR) in the EU. Expect this single law to radically alter the way online businesses treat users and customers, and personal data gathered from them. The anticipated arrival of the GDPR's full regulatory might in 2018 (with severe penalties for noncompliance) is already altering the way many big businesses approach personal data. In the words of one executive (who works for one of those big companies and asks to stay unnamed), personal data is quickly becoming a 'toxic asset.' He also calls surreptitiously gathered personal data the 'radon gas' of business, and 'a silent killer.'

"But the most important moves will not be made by big business. Instead they'll be made by independent individuals and smaller businesses that need to interact in a fully trusting way, where exposure to risks and bad acting are minimized by point-to-point and end-to-end conversations, transactions and relationships. There will also be a rise in conditional sharing of personal information on a need-to-know basis, and on terms set by individuals as well. Some of these terms will be sourced in neutral and trusted dot-orgs such as Customer Commons, which will do for personal terms what Creative Commons did for personal copyright.

"Also, expect a distinction to appear between sovereign personal identity – the kind given to people by their parents at birth and fully controlled by the individual – and administrative identifiers. Identity in the future will be anchored in the former rather than the latter. So will

control over how we are known by others. Imagine, for example, getting married and changing your last name. You should be able to change administrative records of your last name at all the government and commercial entities with which you have a relationship in one move. That is only possible when you are in full control of your own sovereign-source identity and the means by which others know it, and can trust your authority over it. Expect to see this change in the way identity works come to pass over the next few years. Also expect to see distributed ledgers (e.g., blockchain) involved."

Rather than feed on fears, promote what could go right – we can figure it out

Jeff Jarvis, a professor at the City University of New York Graduate School of Journalism, said, "To believe that our trust in technology will be diminished is to believe that we are powerless against it – and I do not believe that. We have many tools at hand to govern our own use of technology – norms, laws, regulation, the market – and we are using them. Sadly, media do not help with this process by usually donning dystopian glasses, asking what could go wrong with any technology rather than also exploring what could go right. Moral panic – #technopanic – often ensues. Also, whole markets of new companies pop up to feed on these fears. And, especially in Europe, industries and institutions that are challenged by the change technology brings resort to political pressure, regulation and legislation as protectionism. So it is important for the technologists to do a better job of acknowledging and addressing what could go wrong and of exploring and promoting what could go right. It is important for other institutions – government, media, education – to help explore the opportunities, if for no other reason than to remain competitive in the world. We're smart. We'll figure it out. We always have, eventually."

Setting appropriate choices in engineering the technology can improve outcomes

Fred Baker, fellow at Cisco Systems and longtime Internet Engineering Task Force leader, wrote, "Fundamentally, I don't think the average individual understands the communication media they use, whether it is a postal envelope, the dial on a rotary phone, Morse code or the many different kinds of communication that use the internet. They trust them implicitly, until they are given a reason not to, or they don't trust them. If anything, that's why we have to limit their choices, such as by forcing the use of https over http, or the use of TLS in SMTP, or other places. It helps them make better choices. Where that breaks down is when trust is clearly violated. In my father's era, General/President Eisenhower had to tell people to beware the military/industrial complex, and Washington had to tell citizens to 'beware foreign entanglements.' Governments have grossly failed us in the past 50 years, leading UK people to distrust the EU, U.S. people to distrust NSA and FBI, and so on. That hopefully forces people to use the media more wisely, but I don't believe that they do."

People's trust in online interactions are now and will continue to be unconscious

Barry Chudakov, founder and principal at Sertain Research and StreamFuzion Corp., replied, "While database hacking and identity theft will continue to bedevil users and make headlines, for most of us, convenience and immediacy will continue to far outweigh trust in our online interactions over the next decade. Today the default position of virtually every business is to move online. Try calling an insurance company or an airline to ask a quick question: The queue has moved from outside the store to the 888 number. Online is the new landline …. While some may grumble about the impersonal nature of online interactions, most people have little choice but to trust the online experience. If you don't want to physically visit and buy from a brick and mortar store, what else is there? Most people will say or think: The decision has been made and I wasn't part of the decision-making.

"As a result, people's trust in online interactions will be implicit, unconscious. It is now, and will continue to be, like driving a car on roads where accidents happen regularly. You need to go somewhere so you get in the car, despite traffic and road construction and obstacles and even the danger of accidents. This doesn't mean you won't at some point complain about highway congestion; likewise, people will continue to both like the ease of online interactions yet grumble about security, identity chasing and tracking as they conduct more business than ever in cyberspace.

"There is no area of life that won't be affected. Economics, health, education, politics, culture – all are changed by the interaction of devices and the Internet. This is because as people use cellphones and the Internet we have tangibly altered reality …. The impacts are and will continue to be both positive and negative; this is because the impacts are revolutionary and, again, cannot be contained by binary formulations. This new reality changes our behaviors and especially how we see others and ourselves. Cellphones, smart devices, are now instruments of documentation, and in this measure, are tools of validation. I text, therefore I am. I am here. This is what I saw. I am alive. I am dressed (or undressed) a certain way …. The act of showing the act may now be more important than the act itself. This is not inconsequential: Crimes that might have gotten a slap on the wrist now send athletes and others to jail or into retirement because a cellphone captured their questionable (or criminal) behaviors. Citizen journalists who witness a disturbance, a shooting, an accident, especially with political overtones, are now not only adjuncts to the news – they are the news. They are bringing us first-hand reports that are raw, unfiltered and often devoid of context. Yet, the immediacy of these reports – the lack of filter, and often the lack of vetting – is both thrilling and disturbing.

"We have to construct protocols to respond to this new phenomenon that is changing our sense of reality …. Our identity is portable and, with some effort, able to be manipulated, stolen, recast, taken from us. Ask anyone who's had an episode of identity theft how weird it is to plead with authorities to recognize you – as you. The result is that recognition technologies, already gaining sophistication (face recognition, voice recognition, emotion recognition) will increasingly be used to validate what we once thought was obvious and we took for granted: our ability to be ourselves, to be who we are."

Resigned and uncomfortable, the public has no other realistic option

Susan Etlinger, industry analyst at Altimeter Group, wrote, "In the early days of the internet when there were no precedents for 'e' business, venture capitalists funded business models they understood. Of course, the prevailing model in those days was advertising: eyeballs, clicks and any measure of 'engagement' that would prove that organizations were earning their customers' attention. This has made consumer data the dominant currency of the internet. But while we've become good at earning attention, we haven't done so well at earning trust. Study after study reiterates that consumers are uneasy with the ways organizations collect and use their data. They feel resigned and uncomfortable, but they have no other realistic option. They may do a 'digital detox' for a few days, but not too many people are trying to live off the grid. So there is a tremendous opportunity to realign two seemingly conflicting imperatives: the imperative to innovate and perform, and the imperative to sustain long-term, trusted relationships with customers and consumers. I think we can do both, but it's going to get worse before it gets better. Organizations are going to see a continued flight from open platforms to closed ones like Snapchat, WeChat and other messaging apps, and they're going to have to prove that they're trusted actors in order to woo customers back to the open web."

There should be expanded 'public defenders' for online systems

Ben Shneiderman, professor of computer science at the University of Maryland, commented, "Trust is essential to success of online systems. Clearly identified responsible parties should be available to answer user questions, deal with errors/failures, and promote continuous improvement. Public presentations of the number of fraudulent translations, criminal attacks, malicious uses, etc., should be available, just as police crime data or airline delays are public. The ombudsman idea, Better Business Bureau and public defenders need to be expanded for online systems."

About this canvassing of experts

The expert predictions reported here about the impact of the internet over the next 10 years came in response to one of eight questions asked by Pew Research Center and Elon University's Imagining the Internet Center in an online canvassing conducted between July 1 and Aug. 12, 2016. This is the seventh "Future of the Internet" study the two organizations have conducted together. For this project, we invited nearly 8,000 experts and members of the interested public to share their opinions on the likely future of the internet, and 1,537 responded to at least one of the questions we asked. This particular report covers responses to one of five questions in the canvassing conducted in the summer of 2016. Overall, 1,233 people responded and answered this question:

> ***Billions of people use cellphones and the internet now, and hundreds of millions more are expected to come online in the next decade. At the same time, more than half of those who use the internet and cellphones still do not use that connectivity for shopping, banking, other important transactions and key social interactions. As more people move online globally, both opportunities and threats will grow. Will people's trust in online interactions, their work, shopping, social connections, pursuit of knowledge and other activities, be strengthened or diminished over the next 10 years?***
>
> *The answer options were:*
>
> *Trust will be strengthened – 48%*
>
> *Trust will be diminished – 24%*
>
> *Trust will stay about the same – 28%*

Then we asked: *Please also consider addressing these issues in your response. You do not have to consider any of these. We have added them because we hope they might prompt your thinking on important related issues: Which areas of life might experience the greatest impact? Economic activity? Health care? Education? Political and civic life? Cultural life? Will the impacts be mostly positive or negative? What role might the spread of blockchain systems play?*

The web-based instrument was first sent directly to a list of targeted experts identified and accumulated by Pew Research Center and Elon University during the previous six "Future of the Internet" studies, as well as those identified across 12 years of studying the internet realm during its formative years. Among those invited were people who are active in global internet governance and internet research activities, such as the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Society (ISOC), International Telecommunications Union (ITU), Association of Internet Researchers (AoIR) and Organization for Economic Cooperation and Development (OECD). We also invited a large number of professionals and policy people from technology businesses; government, including the National Science Foundation, Federal Communications Commission and European Union; and think tanks and interest networks (for instance, those that include professionals and academics in anthropology, sociology, psychology, law, political science and communications), as well as globally located people working with communications technologies in government positions; technologists and innovators; top universities' engineering/computer science departments, business/entrepreneurship faculty, and graduate students and postgraduate researchers; plus many who are active in civil society organizations such as the Association for Progressive Communications (APC), the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF) and Access Now; and those affiliated with newly emerging nonprofits and other research units examining ethics and the digital age. Invitees were encouraged to share the canvassing questionnaire link with others they believed would have an interest in participating, thus there was a "snowball" effect as the invitees were joined by those they invited to weigh in.

Since the data are based on a nonrandom sample, the results are not projectable to any population other than the individuals expressing their points of view in this sample. *The respondents' remarks reflect their personal positions and are not the positions of their employers; the descriptions of their leadership roles help identify their background and the locus of their expertise.* About 80% of respondents identified themselves as being based in North America; the others hail from all corners of the world. When asked about their "primary area of internet interest," 25% identified themselves as research scientists; 7% as entrepreneurs or business leaders; 8% as authors, editors or journalists; 14% as technology developers or administrators; 10% as advocates or activist users; 9% as futurists or consultants; 2% as legislators, politicians or lawyers; and 2% as pioneers or originators. An additional 25% specified their primary area of interest as "other."

More than half the expert respondents elected to remain anonymous. Because people's level of expertise is an important element of their participation in the conversation, anonymous

respondents were given the opportunity to share a description of their internet expertise or background, and this was noted where relevant in this report.

Here are *some* of the key respondents in this report (note, position titles and organization names were provided by respondents at the time of this canvassing and may not be current):

Robert Atkinson, president of the Information Technology and Innovation Foundation; **Fred Baker**, fellow at Cisco; **Naomi Baron**, a professor of linguistics at American University; **danah boyd**, founder of Data & Society; **Stowe Boyd**, managing director of Another Voice; **Marcel Bullinga**, trend watcher and keynote speaker; **Randy Bush**, Internet Hall of Fame member and research fellow at Internet Initiative Japan; **Jamais Cascio**, distinguished fellow at the Institute for the Future; **Barry Chudakov**, founder and principal at Sertain Research and StreamFuzion Corp.; **David Clark**, Internet Hall of Fame member and senior research scientist at MIT; **Cindy Cohn**, executive director at EFF; **Anil Dash**, entrepreneur, technologist and advocate; **Cathy Davidson**, founding director of the Futures Initiative at the Graduate Center of the City University of New York; **Cory Doctorow**, writer, computer science activist-in-residence at MIT Media Lab and co-owner of Boing Boing; **Judith Donath**, Harvard University's Berkman Klein Center for Internet & Society; **Stephen Downes**, researcher at the National Research Council of Canada; **Bob Frankston,** internet pioneer and software innovator; **Oscar Gandy**, professor emeritus of communication at the University of Pennsylvania; **Marina Gorbis**, executive director at the Institute for the Future; **Jeff Jarvis**, a professor at the City University of New York Graduate School of Journalism; **Jon Lebkowsky**, CEO of Polycot Associates; **Peter Levine**, professor and associate dean for research at Tisch College of Civic Life; **Mike Liebhold**, senior researcher and distinguished fellow at the Institute for the Future; **Rebecca MacKinnon**, director of Ranking Digital Rights at New America; **Larry Magid**, CEO of ConnectSafely.org; **John Markoff**, author of "Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots" and retired senior writer at The New York Times; **Jerry Michalski**, founder at REX; **Andrew Nachison**, founder at We Media; **Frank Pasquale**, author of "The Black Box Society: The Secret Algorithms That Control Money and Information" and professor of law at the University of Maryland; **Demian Perry**, director of mobile at National Public Radio; **Susan Price**, digital architect at Continuum Analytics; **Justin Reich**, executive director at the MIT Teaching Systems Lab; **Mike Roberts**, Internet Hall of Fame member and first president and CEO of ICANN; **Michael Rogers**, author and futurist at Practical Futurist; **Marc Rotenberg**, executive director of EPIC; **David Sarokin**, author of "Missed Information: Better Information for Building a Wealthier, More Sustainable Future"; **Henning Schulzrinne**, Internet Hall of Fame member and professor at Columbia University; **Doc Searls**, journalist, speaker and

director of Project VRM at Harvard University's Berkman Klein Center for Internet & Society; **Ben Shneiderman**, professor of computer science at the University of Maryland; **Richard Stallman**, Internet Hall of Fame member and president of the Free Software Foundation; **Brad Templeton**, chair for computing at Singularity University; **Baratunde Thurston**, a director's fellow at MIT Media Lab, Fast Company columnist and former digital director of The Onion; **Patrick Tucker**, technology editor at Defense One and author of "The Naked Future"; **Steven Waldman**, founder and CEO of LifePosts; **Jim Warren**, longtime technology entrepreneur and activist; **Amy Webb**, futurist and CEO at the Future Today Institute; and **David Weinberger**, senior researcher at Harvard University's Berkman Klein Center for Internet & Society.

Here is a selection of some of the institutions at which respondents work or have affiliations:

AAI Foresight, Access Now, Adobe, Altimeter Group, The Aspen Institute, AT&T, Booz Allen Hamilton, California Institute of Technology, Carnegie Mellon University, Center for Digital Education, Center for Policy on Emerging Technologies, Cisco, Computerworld, Craigslist, Cyber Conflict Studies Association, Cyborgology, Dare Disrupt, Data & Society, Digital Economy Research Center, Digital Rights Watch, DotTBA, EFF, EPIC, Ethics Research Group, European Digital Rights, Farpoint Group, Federal Communications Commission, Flipboard, Free Software Foundation, Future of Humanity Institute, Future of Privacy Forum, FutureWei, Gartner, Genentech, George Washington University, Georgia Tech, Gigaom, Gilder Publishing, Google, Groupon, Hack the Hood, Harvard University's Berkman Klein Center for Internet & Society, Hewlett Packard Enterprise, Human Rights Watch, IBM, InformationWeek, Innovation Watch, Institute for Ethics and Emerging Technologies, Institute for the Future, Institute of the Information Society, Intelligent Community Forum, International Association of Privacy Professionals, ICANN, Internet Education Foundation, Internet Engineering Task Force, Internet Initiative Japan, Internet Society, NASA's Jet Propulsion Laboratory, Karlsruhe Institute of Technology, Kenya ICT Action Network, KMP Global, The Linux Foundation, Lockheed Martin, Logic Technology Inc., MediaPost, Michigan State University, Microsoft, MIT, Mozilla, NASA, National Institute of Standards and Technology, National Public Radio, National Science Foundation, Neustar, New America, New Jersey Institute of Technology, The New York Times, Nokia, Nonprofit Technology Enterprise Network, New York University, OpenMedia, Oxford Martin School, Philosophy Talk, Privacy International, Queensland University of Technology, Raytheon BBN Technologies, Red Hat, Rensselaer Polytechnic Institute, Rice University's Humanities Research Center, Rochester Institute of Technology, Rose-Hulman Institute of Technology, Semantic Studios, Singularity University, Social Media Research Foundation, Spacetel, Square, Stanford University's Digital Civil Society Lab, Syracuse University, Tech Networks

of Boston, Telecommunities Canada, Tesla Motors, Department of Defense, U.S. Ignite, UK Government Digital Service, Unisys, United Steelworkers, University of California (Berkeley, Irvine, Los Angeles and Santa Barbara campuses), University of Copenhagen, University of Michigan, University of Milan, University of Pennsylvania, University of Toronto, Vodafone, We Media, Wired, Worcester Polytechnic Institute, Yale University, York University.

Complete sets of for-credit and anonymous responses to the question can be found here:

http://www.elon.edu/e-web/imagining/surveys/2016_survey/trust_in_internet_activities.xhtml
http://www.elon.edu/e-web/imagining/surveys/2016_survey/trust_in_internet_activities_credit.xhtml
http://www.elon.edu/e-web/imagining/surveys/2016_survey/ trust_in_internet_activities_anon.xhtml

Theme 1: Trust will strengthen because systems will improve and people will adapt to them and more broadly embrace them

A plurality of respondents expect participation in online interactions to grow in the next decade. They cited a variety of reasons, including 1) continued improvement of global security and personal privacy in technical systems, as well as civic and industry support for social strategies, that will in turn build trust; and 2) people's increased capacity over time to use the technology smartly. A number of the answers focused on the special role these experts expect younger generations to play as they grow up with technology. At times, however, respondents expressed concern that these younger users' enthusiasm would be misplaced or be blind to the risks of trusting technology-mediated interactions.

Janice R. Lachance, interim president and CEO of the Better Business Bureau Institute for Marketplace Trust, said, "All will be impacted, mostly for the positive. Blockchain, crowdsourcing and the increased miniaturization of devices and tools will dramatically increase access to trusted networks and services. For example, people in remote locations won't have to travel to banks to cash checks or pay fees for wire transfers. Those services can come to them, as can critical health services. The internet will continue to change the world for the better, in ways both dramatic and unknown at this time. The potential is limitless."

An **anonymous principal consultant** commented, "There is this Dilbert comic where someone at lunch is bragging how they would never give out their credit card online, then turns around and hands it to a minimum-wage server. The risks from the internet aren't greater than what we have always faced, they are just less familiar to some. The database where Amazon stores my credit card number is way more secure than the drawer where some mom and pop operation used to store my credit card impressions. Technology also allows vendors, processors and banks to respond to problems much more quickly. Are people still going to get swindled? Of course, just as they always have. But at the same time we have the ability to let a wide audience know that no, there is not a Nigerian prince who wants your help smuggling money out of the country. Scams are going to have a much shorter life span than they once did."

Avery Holton, an assistant professor and humanities scholar at the University of Utah, said, "As technologies and access expand, privacy in areas such as personal finance and health will certainly continue to be questioned and tested. At the same time, organizations and companies are working to enhance the protection and security of individual data. Beyond

encryption and multiple password requirements, new technologies in the coming decade should work to provide fail-safes for individual information should the security for such information fail. Where now a bank may send an individual a new debit card if their account information was breached (a process that may take days or weeks), they may be able to simply reset EMV (or forthcoming) chips remotely. We must remember that with each test to the security of our data comes an opportunity to improve our security. Part of the current problems rests on the shoulders of individuals who recognize threats to their security but struggle to change (e.g., many still use a single password across multiple channels). So, organizations and companies must also focus on engaging individuals and encouraging a change in their habits."

Cindy Cohn, executive director at the Electronic Frontier Foundation, warned that people must advocate for the most-positive future of trust in online interaction. "The pressure to build a more-secure internet and tools will build in both the public and corporate sphere. The government will be unsuccessful in efforts to reduce [individuals' personal] security and the result will be that more people will, rightfully, trust in the security of their tools. That's the happy story. There is the opposite one, too, though; the direction is up to us."

Jon Lebkowsky, CEO of Polycot Associates, commented, "Currently, trust is diminishing. The high commitment to online data systems for sensitive transactions and storage of sensitive data is still a relatively new thing, and we've seen breaches where there were security flaws that were not obvious until the breaches had occurred. We're still perfecting systems and processes, and expectations are low and will probably be lower. *However*, this will drive security innovation, and I'm confident that we will eventually restore trust as systems improve."

Stuart Shulman, CEO of Texifter, wrote, "We have all created gaping holes in our privacy in exchange for convenience, happiness, economic gain, self-promotion, affection and certain kinds of indulgence. Most people would not willingly create such gaping holes if they did not believe, at some level, [that] what is lost pales in comparison to what is gained."

Subtheme: Improved technology plus regulatory and industry changes will help increase trust

Some experts in this canvassing expressed trust that technological improvements will enhance trust in online systems. One of the many such prospects respondents predicted is the rise of more-secure personal identification schemes that might allow individuals more

control over their personal data while buttressing security via creation of a greater capacity for activities and transactions to be authenticated by others.

An **anonymous Internet Hall of Fame member** wrote, "The use of verified identity can provide for much better accountability on the internet. Knowing who you're dealing with will make it reasonable to 'trust, but verify.' "

Paul Davis, a director based in Australia, observed, "The drift to digital-first engagement will certainly benefit anything which is transactional in nature, across most services. Trust will continue to develop and mitigations be put in place after significant breaches of that trust. The digital self will play an ever-increasing role in political and civic life, with that self eventually merging with the whole, whereby people who reject their digital identity become today's 'hippies.' There will be a social cost to *not* being 'online,' potentially increasing discrimination in some areas; however, the overall benefits will grow through greater accessibility."

An **anonymous associate professor** commented, "I'd like to believe trust will be strengthened but I believe that depends on effective regulation of online services. A lot depends on whether government is given the authority and resources to regulate online trade."

Garth Graham, board member at Telecommunities Canada, advocated for individuals' right to own their identity. "Trust will only be strengthened when my digital identity is owned by me as a matter of right," he commented.

Marshall Kirkpatrick, co-founder of Little Bird, previously with ReadWriteWeb and TechCrunch, replied, "There is a clear path from less to more familiarity with new platforms. Carrying out many social functions by mobile device ID is quickly becoming the new normal."

Dave Kissoondoyal, CEO of KMP Global Ltd., responded, "Technology will evolve [so] that people will trust online interactions more than today. It is technology itself that will bring this trust and more and more people will interact online than anything else."

Larry Magid, CEO of ConnectSafely.org, said, "Technology will get better and more secure, and more people will realize the benefits of online financial transactions. Besides, there will be fewer (or more expensive) alternatives."

An **anonymous respondent** observed, "The organizations developing the standards upon which the infrastructures are built have security and privacy as prime directives in that development. There may be isolated enclaves where the trust may decrease due to mandated weaknesses, but generally the trend is toward much greater protections and a legitimate basis for trust."

Paul Jones, clinical professor and director at the University of North Carolina, commented, "Remember traveler's checks replacing cash? ATMs replacing your favorite teller? We're seeing that again. Not just with financial transactions but with social interactions, health and education. At this point, there is no stopping the transitions already underway. Blockchain systems are only the latest technical augmentation of trust. Expect more. Soon."

An **anonymous respondent** replied, "If there is money to be made, industry will find an answer to security." And an **anonymous researcher at a futures institute** agreed, writing, "It is in the financial interest of powerful companies that this trust be strengthened, and they have the ability to make that happen."

Industry is also expected to continue to encourage public trust – deserved or not – through information campaigns.

Beth Corzo-Duchardt, assistant professor at Muhlenberg College, wrote, "Whether warranted or not, trust in online activities will be strengthened because there are so many industry forces invested in garnering trust through advertising and indirect propaganda."

T. Rob Wyatt, an independent network security consultant, agreed with her but worries over the lack of actual industry investment in security. "Although we live in a digital house of cards and our national infrastructure targets are frighteningly porous, the global economy relies on confidence in digital transaction infrastructure and security," he said. "We will continue to invest heavily in the perception of security even as we ignore it. Digital security is the toxic waste dump of our age. The willful blindness of corporate and government entities of the need to invest in basic security has resulted in the externalization of these costs in large pools of accumulated technical debt. Not only is the cost deferred and shifted to external parties, but it is amplified by orders of magnitude when the cleanup and effects are finally expressed."

Nigel Cameron, president and CEO of the Center for Policy on Emerging Technologies, observed, "The net will be likely be strengthened in regard to trust, though this is a risky judgment and there's, say, a 40-60 chance of a collapse of trust through a series of

catastrophic failures, whether the work of asymmetric bad actors, crooks, power-grabbing corporations, or mere systemic incompetence – OPM [U.S. Office of Personnel Management], etc. If it goes the 40 way, we could end up with a rush to an analog future."

Valerie Bock of VCB Consulting said, "We will learn how to secure our critical infrastructure, and in the meantime we are learning how to hold consumers harmless for the breaches that occur within our current systems. The benefits of being able to loan an e-book to a new friend instantaneously to keep a conversation going, the ability to shop the world for things there is only a small market for, the ability to transfer value at low cost, and the ability to access the latest scientific information, all offer powerful ways to connect people to one another and hence enhance trust."

Nobody expects perfection, but many expect that despite "bumps along the way" the online experience will remain mostly positive.

An **anonymous associate professor and director of a university center for policy informatics** replied, "Not only will trust be strengthened, it will be the expectation of interactions. Many people will probably have at least one negative interaction with sharing their information online; it will be important that the biggest brokers and legislators create a culture of trust as stability (similar to the government insuring banks or credit cards ensuring that you will never pay for a fraudulent transaction)."

An **anonymous software engineer** commented, "We're just at the beginning of the use of online systems for commerce and banking globally. The system already works as well online as it does offline. There will be bumps along the way, but overall it will be mostly positive for buyers and sellers. Economic activity will be foremost, but education and health care will also benefit. However, the impact on political and civic life will be mostly to drive information bubbles and foster divisiveness."

An **anonymous head of privacy** said, "Wireless devices and security for IoT [Internet of Things] applications and online services will continue to improve. As devices and connectivity are made available to more individuals, positive economic and socialization opportunities will expand. Cross-border law enforcement and consumer and privacy protection, in addition to mobile authentication regimes, will encourage expanding trust."

An **anonymous open source technologist** observed, "The emergence of companies like Amazon, Google and Apple is indicative of the great trust people already place in these

organizations and the online world. This will grow as better governance, systems and software take hold."

An **anonymous respondent** said, "Twenty years ago the web was really the Wild West. You never knew what to trust. Now there are largely trusted intermediaries like Google and Mozilla that block or identify many threats. This trend will strengthen over the coming decade."

Adam Nelson, chief technology officer at Factr, predicted, "Economic activity will become much more efficient and secure. Keep in mind that the 'analog' economy with cash is also encumbered by theft and fraud. These won't go away but the frequency will be lessened. Government/public oversight will be higher, though."

Dan York, senior content strategist at the Internet Society, is encouraged by technological advances but warned against stringent regulation, writing, "I hope trust will be strengthened, but I fear that if we don't do anything about it, trust will be diminished. Trust will probably be diminished over the next 2-5 years, but after that I hope it will be strengthened, as technologies and policies get adopted that raise the level of trust. So my answer for 10 years out is different from five years out. We are seeing an erosion of trust right now as more and more data breaches happen, more and more surveillance happens, and more and more security vulnerabilities happen. There are ways to make that trust stronger, some of them technical, some of them policy – and I believe we *must* implement these tools …. I'd give about even odds as to whether those things will happen. The impact of diminished trust could be strongest on economic activity. It could also cause governments to want to 'take action to protect citizens' that could result in the imposition of harsh legislation or the further fragmentation of the internet. This could lessen the opportunities available to all."

Demian Perry, director of mobile at NPR, noted that he already sees tech improvements that might enable trust in his business. "The reality is that online transactions are now far safer than traditional transactions and they will only become more so," he commented. "My credit card has been stolen multiple times in the past two years, all as a result of security holes at brick-and-mortar point of sale that would have been avoided had I made the transaction online. In just one example of how online transactions are so much more secure, we are now working with our member stations to implement a donation method that will effectively authorize a new credit card for each transaction and immediately destroy that card after the transaction. In the short moment when the card is active, it will have a credit limit that is very close to the intended donation amount. And as we continue to improve the

security of online transactions with advances like this one, consumers will become increasingly confident in their online purchases."

One **anonymous respondent** spoke in support of the types of online "neighborhood watch" that are expanding to allow netizens to report violations: "Providers of social media, retail, information, games, etc. will provide as safe an environment as possible to conduct these activities, otherwise they'll lose users. As far as interpersonal correspondences go, trusting someone online will come with the same perils as real life. Stalkers stalk, whether online or off. Abusers abuse, whether online or off. But online reporting is quickly becoming more reliable than law enforcement. It's easier to get someone banned for stalking online than to get a restraining order from law enforcement. That will go a long way toward building trust in social interactions. If someone becomes abusive or stalker-ish, report them and they disappear."

An **anonymous respondent** observed, "One, the protection mechanisms will get stronger and people will be more accustomed to these transactions. [Two,] the younger generations will just do this as a matter of course, so trust will improve. On the other hand, the hacking systems and such will get stronger, such that there will be many ways to get into someone's data. The more secure the data, the more sophisticated hackers will have to be. And that's dangerous."

David Williams, who chose not to share any additional identifying information, replied, "As folks gradually shift more of their life online (and they age into a more pure online world), trust will naturally increase and breaches of that trust will be seen as the cost of living in this century rather than the last. Encryption that promises to remain strong in light of advances in quantum computing will be more important. The challenge to cellphone dominance will likely remain in the transactions that require more screen real estate than anyone is willing to carry in their pocket. There will continue to be efforts to simplify everything down to cellphone-sized chunks, which will reduce the value of some of the current offerings. Technology will continue to evolve to gain and hold that trust, and malicious folks will continue to find ways to abuse it. On the whole, I expect the malicious folks will be gradually diminished in their abilities to leverage purely technological attacks."

Nick Tredennick, a technology analyst, said, "Historically, net contributions are positive, so adding more people and more interactions will bring greater trust capabilities to interactions."

A number of respondents shared their opinions regarding which particular aspects of online interaction might be trusted most in 2026.

Ray Schroeder, associate vice chancellor for online learning at the University of Illinois, Springfield, observed, "Online interactions will become the default norm; it will be as comfortable and considered as reliable as a visit to the bank in the 1980s; an in-person visit to a doctor in the 1990s; or an in-person purchase at a grocery store in the first decade of the 21st century. Elections will be conducted online, resulting in greater participation and a more complete canvassing of the public."

An **anonymous respondent** predicted, "Trust in online banking will go down. Trust in health care will be negative and positive. Health care is very much in the dark ages when it comes to online security, record keeping and HIPAA protection. Most doctors and nurses don't have much skill when it comes to using computers and many are actively dragging their feet on implementing changes. Also, insurance companies deliberately make things more difficult and time-consuming to enter and they use confusing and outdated computer programs and databases that are not user-friendly. From personal experience, I know they deliberately discourage startups from using their data to get better pricing for services and medicines or from making things more user-friendly. Even federally mandated data is unavailable except for in a badly physically printed stack of paper in tiny print for thousands of dollars and by the time it's made available, all the prices have changed. Trust in cultural life – opportunities have improved, but people get locked into social platforms that make certain kinds of social interaction harder (I'm looking at you, Facebook). In regard to blockchain systems, accountability might help prevent 'griefing' in certain online social contexts, as long as the blockchain is used as an introduction of sorts."

An **anonymous managing director** predicted, "Commercial applications will grow faster; government applications for trust (health care, education) will take a while. This requires transformations of whole sectors, which is a slow and tedious process."

An **anonymous respondent** commented, "Health care and education should see the greatest positive impact, but the former and economic activity raise significant security risks. In addition, the latest popular app, 'Pokemon Go,' shows how criminals are learning how to manipulate even cultural/societal types of engagements."

Another **anonymous respondent** commented, "Trust in social media will decline, but trust in services such as banking and shopping will increase."

An **anonymous technical operations lead** said, "*Economic* – Obviously, we will have more of the economy be purely virtual, such as purchasing in-game virtual items. Right now, this is the all-or-nothing 'give us your credit card,' but there will be many more fine-grained ways of buying things in the future. *Health care* – Ideally, there would be a standard way of noting your health, and it would be stored/owned by you. (Instead of health records being 'owned' by companies providing care, and transfer of records being a 'value-add' service that costs more.) We could even have people do 'research' by asking a question that queries everyone's records, but doesn't expose any individual data. *Politics* – I hope we have reached peak indifference and in the future politicians will be held to a higher standard instead of a lower one."

Stephen Schultz, who chose not to share any additional identifying information, wrote, "Payment systems via smartphone will become as common as consumer credit within the next four years, and, with it, public trust in those systems. Also, I see the principles of encryption becoming common knowledge in the near but indeterminate future and with it, an increase in public trust generalized to any system transmitting or retaining personal information. I don't feel nearly as confident making any such predictions for medical care and personal medical histories. In smaller nation-states, especially those with single-payer medical care, the implementation of a portable, accessible personal medical record is already within reach. At the other extreme (i.e., the U.S.), there are some startups with a mission to achieve the same thing (e.g., Ohio-based CrossChx), but I imagine it would have to be some kind of open standard in order to work, and that process will almost certainly take several years."

Some of these experts argued that there is a special pressure on civic systems to build trust in an increasingly challenging media environment. An **anonymous respondent** who works in the government wrote, "Most-affected will be political and civic life. Trust is a function of knowledge and shared information and belief sets. As more facts become available, more trust is generated. As more opinions are disguised as facts, less trust and more polarization will occur." And an **anonymous systems manager** commented, "Trust will go up if and only if advocates for open systems and transparency inherent in civic big data can continue their work."

One **anonymous respondent** warned that currently emerging applications that gauge user behaviors will be applied, writing, "Trust will be strengthened, but through perceptual and behavioral manipulation rather than stronger security infrastructure or realistic comparative outcomes. Technologies' ability to manipulate behavior is outstripping humans' ability to react in the time scales involved. Some people will take advantage of that."

An **anonymous process manager** said that blame for problems is regularly misplaced, observing, "Most people don't think about their trust in terms of systems. Even those whose identity has been stolen or data breached only develop anger toward the group immediately responsible for the loss – they're mad at Target, or PlayStation, or whoever. They are not mad at the infrastructure. Most people turn their anger on the 'bad driver' who caused an accident, not the road builder who designed a blind turn in a busy area."

An **anonymous respondent** predicted, "The market will continue to improve in ways to build societal trust, but I would not be at all surprised to find these efforts derailed by economic catastrophe in the very near future, from which a more trustworthy internet may potentially arise."

Subtheme: The younger generation and people whose lives rely on technology the most are the vanguard of those who most actively use it, and these groups will grow larger

Many respondents observed that younger generations and those who feel they must rely upon it to stay competitive have historically been the most likely to put trust in technology. An **anonymous research officer** said, "This is purely a demographic issue. Distrust of technology skews toward the older sections of society so, by necessity, trust will grow as time passes. Trust could be further amplified by companies improving efforts to ensure digital security and avoid fraud."

Uta Russmann, communications professor at the FHWien University of Applied Sciences in Vienna, said, "People's trust will be strengthened over the next 10 years, as most of the people who are shopping, banking, etc., will have been socialized and educated within the online world."

An **anonymous professor at a state university** noted, "Trust will be strengthened mainly because people will become used to using these tools daily for these functions. Twenty miles an hour was once considered a dangerous speed for human travel."

Dave Howell, a senior program manager in the telecommunications industry, replied, "Convenience will outweigh distrust, and today's 10-year-olds will have grown up with the same easy familiarity with blockchain and algorithmic identity their parents did with DVD and cellphones and their grandparents did with TV, jet travel and automobiles. Location-based services will inundate these kids with offers; they'll learn to ignore them. Parents will get headaches and be frustrated while kids will skip along. Health care? Maybe not in the

next decade but within the next three [it] will see huge efforts to automate it to reduce costs. Blockchain and algorithms had better be bulletproof in identifying persons, and trusted records kept inviolate."

An **anonymous respondent** commented, "This strengthened trust is a matter of generational replacement. Children today won't even consider that there's an alternate way of conducting business."

An **anonymous respondent with the Internet Engineering Task Force** predicted, "I doubt [trust] will change much for individual people. But on average it will increase as old people die and new people enter the system. I do most of my work with an internationally distributed community. It is very powerful to assemble a team without regard to geography."

An **anonymous assistant professor at a state university** wrote, "Trust will be strengthened … I expect information security will improve, on the whole. Further, I imagine younger generations are and will be more comfortable with sharing information – including sensitive information – online. I expect, for instance, that most voting will eventually move online, and that more health care discussions between doctors and patients will move online. I think, for the most part, these are positive changes, though there is probably some negative consequence to diminished in-person contact."

Many said they expect that online interaction will become so normalized that trust might not be figured into many people's decision-making when it comes to such actions. Some see it as a sort of implicit trust.

David Morar, a doctoral student and Google policy fellow at George Mason University, replied, "Societal understanding and acceptance of online interactions and of mobile devices as an important pillar in human life will only grow into the future. The fact that these tools can also be used for horrible things should not and will not completely overshadow the potential benefits of using these tools in more aspects of life. One example of this is the near-mainstream appeal of online and mobile dating. Once seen as a place reserved for 'creeps' and 'deviants,' online dating is now as normal as making dinner reservations online through an app. This shows that social norms change, adapt and expand (or not) in a constant back-and-forth with technology. A serious educational endeavor will be desperately needed in the near future in order to help citizens evolve their current understanding of fundamentals such as privacy, security and the limits of the tools being used."

Megan Browndorf, a staff member at Towson University, said, "Crime will increase. Accidental use and misuse will increase. But that is simply a matter of opportunity and numbers. Overall, we will see the development of the internet as a space …. Individuals will become more used to existing on the internet: working, and being and communicating there. And that is enough to build trust. In the next decade, as the number of adults who do not remember a time before the internet grows and the number of individuals with familiarity with the internet grows, it will become a trusted fact of life."

Glen Thomas, a head of computing in an educational setting, commented, "My students do not care for online security, so there is implicit trust throughout the younger generation. They just want the features and companies and governments can do what they wish with their data. There will be issues when bulk medical data makes its way to employers and insurance companies."

Richard Lachmann, a professor of sociology at the University at Albany, noted: "As people use online services more, they will become more confident in them. However, familiarity will [be] undercut by the frequent security breaches."

Anonymous respondents also commented:

- "Most of the people who don't trust the tech are older. As they die off, younger folks who mostly don't think about privacy and security become a larger portion of the consumer base of those devices."
- "For young users it will be second-nature and seamless."
- "As younger generations who have grown up with technology get older, you will see increased trust in online interactions – whether or not that trust is deserved – because of a high level of complacency."
- "Generations are coming online who know nothing else. Nostalgia for old methods will die off."
- "Trust will remain the same, but the penetration and use will grow as it becomes more commonplace and the generations who either never used the internet or were just present for its birth will give way to people who have never known life without it."
- "Apps and the mobile web are still often clunky or not as useful as doing some things in person. People will gravitate to whatever is easiest, cheapest and most reliable. When state and local government services are reliably operating on apps and the mobile web, people will use them there."

There were several strong dissenters, though, to the notion that the successor generation will be a vanguard.

For instance, an **anonymous senior technology architect at a Canadian telecommunications provider** commented, "If there is a significant change in the perceived trust people are willing to give, it will be incremental at best. In large part I expect this because, if anything, the generation coming up now has even less reason to trust the internet than the older generation does. Their day-to-day experience is of friends having accounts hacked, of having personal information leaked, of large organizations and governments being compromised. There will be no basis for them to believe that access to their health records online or paying with their phone is natively more secure than it was. That doesn't mean they won't do it. You may see greater adoption rates, but people may also partition themselves and their transactions in other ways. It will require a sea change in the IT industry to significantly improve security. Privacy can't be expected to improve without this change, although an improvement in privacy is not a given. The status quo is a state of nearly constant compromise, which is more or less what we have now. Sadly, increased surveillance is almost easier to implement than this improvement in security. More than that, it's easier to comprehend. There is a net downside to adding monitoring, although improvements in detection and response to breaches may appear to outweigh it."

Theme 2: The nature of trust will become more fluid as technology embeds itself into human and organizational relationships

Many respondents pointed out that trust is a complicated and many-layered concept with numerous variables that can be in constant fluctuation. Some respondents described a trust timeline that will gradually evolve. One example came from **Jannick B. Pedersen**, a futurist and impact investor, who said, "I strongly believe that smart trust will steadily rise. We are in a continued race between good and negative applications of technology. In the past, periods of blind trust in the printed media or the banking system were replaced by increased personal vigilance and smart trust. The very same process will occur as the world moves online: New users will begin with high trust. After disappointments their trust will dramatically diminish and then grow again as the users develop smart trust – by becoming more shrewd in judging online interaction."

David Wuertele, a software engineer for a major company innovating autonomous vehicles, commented, "There are different kinds of trust. One kind is the trust you have that comes from knowing that a service is trustworthy, another kind is the trust you must have because there is no other choice. Although I believe most retailers are not capable of keeping my personal data secret, I still am forced to yield my personal data to them. I am forced to 'trust' them, even though I do not 'trust' them. The fallback is the legal system. If a party with whom I perform a transaction betrays my trust, I may be able to recover some damages by suing. It is not a guarantee and is mostly a huge waste of time, but it is a small consolation."

An **anonymous user-experience designer** said, "Trust is a funny thing, more a function of psychology and perception than of technology. While the internet is getting incrementally more secure, I suspect most people believe it to be far more secure than it is. Their trust will be strengthened, but probably at a quicker pace than the technology warrants. As for the impact, there's a certain equilibrium at which people are happy with just enough online commerce and no more. There will always be people who prefer stores and meat-space interactions."

Subtheme: Trust will be dependent upon immediate context and applied differently in different circumstances

An **anonymous respondent** wrote, "Trust for online interactions such as shopping and banking where one's financial information and identity are put at risk depends on the quality of security available. People's trust may diminish if they hear about too many hacks in the

news. Trust in social interactions depends on the degree of privacy available using a particular system. Whether or not people place trust into online systems is based on whether governments will choose to embrace encryption and respect the privacy of peoples' online identities or not. If not, people will begin to trust less and the results will be negative particularly for political and cultural life."

An **anonymous technology analyst at Cisco** observed, "We will have more anonymizing tools, so our activity will be less public than today. The greatest impact is that the fracturing of my identity for each participation in my life will have its own authority over related circumstances."

Irina Shklovski, associate professor at the IT University of Copenhagen, commented, "Trust has little to do with the reasons why people do not use the internet for shopping, banking or socializing. Trust is not in 'the internet' anyway but in the entities with whom people interact on the internet (your bank, your book seller, etc.). As these entities create conditions that make online interactions the most effective way to achieve particular goals, more of such interactions will happen. I am curious as to why 'key social interactions' are part of this list (and what these key interactions are envisioned to be). Arguably, key social interactions happen online all the time but it is hard to identify what these are. How do you know that a conversation in a bar or over messenger is going to be key in advance? At the same time, people will continue to insist on meeting in person but this, once again, has nothing to do with trust in online interactions."

Timothy C. Mack, managing principal at AAI Foresight, wrote, "The question is not so much [about] areas of life [and trust], but [how different] geographic areas [handle trust issues]. Africa and, in some lesser part, South America, will see a great deal of growth in the economic arena, especially where previous economic structures were rudimentary. We have already seen the growth of political and civic life (especially in South Korea) through smartphones, etc., and health care is now ramping up as well, especially in Africa. Cultural life, not so much. And of course the growth of language-training apps is just the first step to regional or even global digital-education systems. The trust issue will have to be resolved in the arena of 'hard knocks' and is likely to be quite brutal before viable solutions are established."

Christopher Mondini, a leader with a major Internet governance organization, wrote, "The development of the 'offline' ecosystem is what will drive greater trust and reliance in online transactions. In more-mature markets, trust in institutions and leaders is in general decline, while in newer internet frontiers, better financial, contractual and political structures

are rising to meet the challenge of demand for more online social discourse and commercial exchange. Globally the net effect is neutral."

An **anonymous professor** noted, "The boundary between online and offline activity is already pretty fuzzy. One effect of the widespread adoption of mobile phones and social media is that many people seem to maintain loose ties with friends and family members who they would have otherwise lost touch with. As this cohort ages, I expect that there will be surprising social effects to this relationship-maintenance."

Ben Railton, a professor of English and American studies at Fitchburg State University, commented, "Our use and familiarity will grow, and with them a sense of trust or at least instinctive reliance. But threats will continue to grow, especially those related to cyberterrorism and hacking, and so it will be impossible not to fear such threats."

Subtheme: Trust is not binary or evenly distributed; there are different levels of it

Some respondents propounded a related line of reasoning: that trust is not the same in all circumstances at all times or for all people.

Andrias Yose, a freelancer, wrote, "The areas of life experiencing the greatest impact in regard to trust will be communication, interaction, communal bonding. The impacts will not be mostly positive or negative. They will swing from positive to negative to positive continuously, or new/hybrid negatives/positives will surface that will be countered by the opposite. The spread of blockchain systems will increase the frequency of and create a significant time reduction for communication to reach a target or targets."

Ian O'Byrne, co-founder of BadgeChain, replied, "Over the coming decade we will be forced to identify, on a granular basis, the role and function of aspects of trust. Trust is the grease that holds our society together. Trust is evidenced when we drive down the street and expect oncoming cars to stay in their lanes. Trust in digital spaces will increasingly have as much of an effect on our well-being as the analogy of the car driver, [though] it won't seem as dire of a consequence for now. But, as we increasingly pour much of our identity in online spaces, and trust the businesses and governments that oversee these spaces, we'll have questions about how specific that trust is. As breaches of this trust and the acts of whistleblowers opens our eyes to issues of trust, it is my hope that web-literate citizens speak up and determine their own determination of the value and currency of this trust."

Robert Bell, co-founder of the Intelligent Community Forum, responded, "The word 'trust' is misused here. I don't think anyone will become more trusting of online systems – they just will not be able to function well without them. One place where trust does function is in e-government. At the community level, governments have the chance to build more effective, trusted relationships with their constituents by offering transparent, easy-to-use services and access to useful information."

Christine Maxwell, an entrepreneur and program manager of learning technologies at the University of Texas, Dallas, said, "Access to the internet is seen today as a 'global right.' [In 2026] people will be more connected and more reliant on the internet than ever. Areas of greatest impact will include e-health, where it will be positive in many respects but dangerous from a privacy point of view. Economic activity will continue to expand exponentially. Education will continue to grow exponentially at all levels. However, helping the public to be able to recognize 'provenance' and be aware of bias will be essential to making careful choices about what to access, etc."

Bob Garfield, a journalist, said, "I'm confident that secure structures are on the horizon. The problem is that the status quo is so insecure, potentially catastrophically so."

An **anonymous professor of information and history at a state university** said, "For commercial purposes, trust will increase simply because people become used to it. Some kinds of goods, especially clothing and food, will remain with retail stores, but many others will see online shopping become an ever-higher percentage of sales. Health care will be improved, and eventually (but not soon) will become cheaper as kinks in EPRs [electronic patient records] are ironed out. For some users, sophistication will increase, and for most users, access to higher-quality knowledge will improve their lives. Negative implications of this trust in online interaction are already apparent: increased belief in conspiracy theories, distrust in government (despite greater transparency), the 'echo chamber' effect in which climate change and vaccine denialists continue to circulate false facts. I don't think blockchain systems or digital currencies will expand much further; for one thing, they are very costly in terms of energy use."

Pamela Rutledge, director of the Media Psychology Research Center, wrote, "Mobile devices offer greater access, enhance self-efficacy and agency, and they become personal extensions of individual identity and one's social world. Providing peer-to-peer connectivity on a global scale reduces hierarchies and challenges existing social models. The impact will be felt across all sectors, as generations who grew up mobile move into positions of greater social and economic influence."

An **anonymous respondent** said, "Transactions will be routinely performed online. At the end of the day, this is about trust in the company that one is dealing with and in their online presence, and less about online technology in the abstract – there will be shady players online, just as there are offline …. Social interactions will continue to be a mix – they will never move entirely online, but the role of online interactions and communities will continue to increase."

An **anonymous respondent** noted, "No one 'trusts' these systems. No one with any sense, anyway. The question isn't about 'trust,' but rather about recourse and accountability. I don't care what happens with my credit card number, per se, because fraud-detection systems will catch errant activity and alert me. And their profit margins are sufficient that I am indemnified against unauthorized use. Moreover, not enough people have heard stories directly from people they know to be appropriately suspicious. The question you should ask is, who will bear the brunt of 'breached' systems? Will an algorithm error that gets my friend on a no-fly list be resolvable easily? Will an algorithm or breach that absconds with my friend's life savings be remediable? How will we know what systems offer us recourse? It's not a hard problem. FDIC insurance enabled banking expansion. No insurance, no expansion. It's not a technical problem. It's a social problem. Trust is the wrong question."

Anonymous respondents also commented:

- "Trust will continue to fluctuate, and many will simply accept the risks involved with online interactions as the cost of living in a more connected world."
- "Trust will be more volatile (already there is a trend in this direction). It will be easier to establish trust (through relationships) and to lose it. Reputation will still be important."
- "Specific items will be regarded as trustworthy."
- "The more being online is our natural habitat, the more the question becomes not 'Do I trust online interactions as a class?' but 'Do I trust this particular interaction?' "

Theme 3: Trust will not grow, but technology usage will continue to rise as a 'new normal' sets in

Many participants pointed out that a person's use of a technology does not necessarily equate to any level of trust in that technology. They said while some users may gain some level of trust in online interaction for various reasons in the next decade, many will be interacting in online spaces because it is convenient, because they are ignorant of or choose to ignore any potential negative consequences, or because they have no alternate options. A higher percentage of online participation certainly does not indicate a higher level of trust.

Vance S. Martin, instructional designer at Parkland College, commented, "I am not sure that 'trust' will actually be strengthened, but use will increase. In order for there to be trust, people would have to actively think about the security of their digital information, and I don't think most people do. My S7 came preloaded with Amazon, Facebook and my carrier's account software. So there is presumed 'safety' in accessing these on my phone. My wife installs banking software and investment software on her phone as well. We mostly trust the safety of our information, but are also diligent about access and location of our phones. However, I work at a college where I see countless times how students lose their phones which are unlocked; they log in to various sites and never log out; and they get hacked (many times due to the first two points). Perhaps it is blind trust, perhaps it is ignorance of potential threats, but the use of mobile devices for all of young people's interactions is increasing. Could blockchain systems like bitcoin increase the safety? Sure. Could the successful mass use of quantum computing decrease the safety? Sure. From surveys on our campus we know that 91% of our students have smartphones, 100% have cellphones of some sort. My guess is that very few of them have thought about security or whether they should actually trust their information's safety."

An **anonymous respondent** replied, "It is becoming clear that the norms that governed social interactions do not scale to the technologically mediated social networking we use today. One cannot, for instance, have any faith in secrecy of digital correspondence, even in a trusted human partner, because so many of us use technologies that necessitate a third party to have access to metadata, and often content, as a product of that transaction. Apps that upload address books to servers and email providers that read email have become the norm. Third parties inserting themselves into our social interactions, and our readily accepting that as normal, is a telling thing for trends to come."

Subtheme: The trust train has left the station; sacrifices tied to trust a 'side effect of progress'

A share of these respondents expect people's trust in online transactions to be no different from their trust in institutions, which is to say that there is very little of it if any at all. Others observe that people will continue to expand their uses of digital technologies but trust is generally not a factor in their decisions to do so or – if it is – it is misplaced or undeserved trust or "trust by default."

Miles Fidelman, a systems architect and policy analyst at the Protocol Technologies Group and president of the Center for Civic Networking, wrote, "People seem to have … a willingness to defer to authority and the human tendency to turn a blind eye to issues in favor of convenience. At the same time, experience generally breeds a level of cynicism. The result seems to be that people 'don't trust anyone, but do it anyway.' And then lurch from crisis to crisis. (Example, credit cards and passwords get leaked daily – we still use them with impunity.)"

An **anonymous principal security consultant** predicted that security will improve but attacks will continue to rise and systems are unlikely to gain more trust, writing, "People … will not have any other realistic choice. The use of these systems will likely be expected in many interactions in the future. However, in the next decade, it seems *unlikely* that the systems will be significantly more secure than they are currently without a major push from all involved parties. A number of new technologies are being rolled out to improve a number of areas of security, but they frequently fall victim to the same flaws that have been in software for decades already. Security will improve, but attacks will improve. It seems likely that systems will be engineered to more gracefully handle such issues: for example, making it easy to change your credit card number. This will improve ease of use when systems fail, but won't necessarily engender *more* trust."

A number of respondents argued that many of those online now and in future are relying on personal cost-to-benefit calculations estimating that the worst will not happen to them. An **anonymous respondent** wrote, "Trust is irrelevant. We know that people are wildly uncomfortable with the amount of information that, e.g., Google, has about them, but it does not stop them from using Google. People need to live their lives and they will use the services they find necessary."

An **anonymous respondent** said, "Trust will be irrelevant. Hacking, identity theft, trolling, doxxing will become increasingly commonplace and a daily cost of doing business on the internet. Convenience and convention will keep us transacting; but our expectations will shift to accommodate those problems which are currently framed as trust issues."

An **anonymous respondent at the U.S. Department of Defense** observed, "I work for a Navy cyber organization, so I'm aware of the concerns today. And, as a classic Gen X person, I am naturally aloof and untrusting. That said, people sold their personally identifiable information a long time ago with Google, Netflix, Twitter, etc. The genie is out of the bottle for most with regard to the interest of 'privacy.' "

Luis Lach, president of the Sociedad Mexicana de Computación en la Educación, said, "We are suspicious of frauds, cyberattacks of our sensitive personal and financial information, but we are starting to accept that it is safe most of the time. The big challenge is to really have safe procedures over our financial records and personal information. The same principle applies over other areas: health care, education, etc."

An **anonymous deputy CEO** warned that "misplaced trust will be widespread," writing, "People will become more and more used to the digital platforms in their lives. This doesn't mean trust will be strengthened, rather that misplaced trust will be widespread. The increase in the use of mobile apps – low-functionality programs that run on small-screen devices [and] frequently do not implement sufficient security in their operation – does not help matters. As more economic activity takes place on mobile apps, the cost will go up, as the levels of fraud will only increase. I hope this will change."

An **anonymous researcher at a state university** said, "As security technology increases and as people become more normalized to online transactions, sales of goods and services online will increase and likely increase sales across borders and even-greater globalization of the service industry."

An **anonymous senior research scholar at a major university's digital civil society lab** replied, "The business of commerce depends on 'just enough trust' – the incentives are aligned to keep just enough trust in place."

Theo Armour, a coder, said, "I trust a candle and a match more than I trust a light bulb and a power company. But I can do a lot more with the latter. And my trust becomes more informed and increasingly nuanced the more I use the transformed, transported power."

Some experts who study trust and systems say they don't expect a lot of improvement will emerge in the next decade.

Mary Griffiths, associate professor in media at the University of Adelaide, South Australia, commented, "The mobile users I surveyed recently in two Australian cities noted security of

information and lack of privacy as major concerns which affected decisions on the use of apps. Others noted the smartphone's locative functionality as something they did not particularly like. This suggests that increased surveillance of the individual by parties unknown is a continuing concern. Some respondents spoke about their trust that if something 'went wrong,' it would be fixed by responsible agencies. My view is that while a significant number will opt out in future, many will accept change and expect problems to be worked out by regulatory bodies as development occurs. They will create the pressure for accountable systems."

Some respondents complained about surveillance, the lack of disclosures of attacks and data thefts, the push by governments to include back doors by which they evade or overcome encryption and other security measures and called for the public to have more access to the data that companies like Facebook have collected about them and information about how it is used.

An **anonymous respondent** said security will rise and privacy will fall by the wayside, predicting, "Confidence in the ability of companies to secure information will increase, while there will be a decrease in the confidence that companies can be trusted to not use the information at the user's expense."

Another **anonymous respondent** observed, "People's 'trust' is going to depend upon how sophisticated they are. There doesn't seem to be a huge push to make them more sophisticated, although right now the internet is more open and so people have an opportunity to learn if they so choose. I think disclosures in PLAIN LANGUAGE should be right at the top. We are learning almost daily about the abysmal security practiced by companies large and small – even security companies. So will this knowledge diminish trust? For me, yes. For others, no, unless they become personally liable."

An **anonymous state employee** replied, "This will depend heavily on the rate at which people are victimized, online versus brick-and-mortar retailers. If credit cards and personal information are stolen at both institutions at the same rate it will remain the same. If these are stolen less at one or the other then the perception will be swayed in that direction. Media coverage will also play heavily into the perception of safety."

An **anonymous respondent** commented, "The biggest challenge will come from ensuring that the processes used by the trusted systems are fully reviewed and do not contain back doors required by governments. We need open processes and communication. Secrecy is for the data inside the messages, not for the process that is supposed to keep our secrets."

An **anonymous community advocate** said, "Widespread trust will be harder to earn, and there is certainly a distrust of centralized resources (e.g., Facebook). In the future we should have more access to data to base our decisions on, socially and otherwise."

An **anonymous respondent** wrote, "I remember the pulse-pounding fear I felt the first time I entered credit card information into a website to order something, which probably would have been in the mid-2000s. My trepidation would be laughable to a person of my socioeconomic status growing up today. In my lifetime I've seen a clear trend toward more spheres of one's life being opened up to the internet rather than fewer, and I don't see how that genie goes back in the bottle barring some unforeseen crisis. Within my lifetime, I predict that many things I would never do online will become the norm for people younger than me. I'll be able to put a drop of blood in my computer and upload data to a web service that will tell me if I have high cholesterol or diabetes or HIV. At some point this database will be hacked and a lot of people's private information will be made public, as has happened in many other areas of the internet. People will freak out, but continue using the service because it's convenient and has many benefits, and eventually private medical information will just enter the domain of things people know about one another. There are legitimate concerns to be addressed around government and law enforcement surveillance."

Subtheme: People often become attached to convenience and inured to risk

Many participants in this survey argued that immediate rewards outweigh perceived risks, thus reliance on digital tools for interactions requiring trust will spread even more widely as the infusion of technology into people's lives and their environment expands and they become increasingly familiar with and dependent upon it.

The convenience of digital devices is regularly cited as a primary reason people are willing to interact and execute important transactions online despite any doubts they may have in regard to security and privacy issues. An **anonymous web and mobile developer** commented, "Being able to buy groceries when you're commuting, talking with colleagues when doing a transatlantic flight, or simply ordering food for your goldfish right before skydiving will allow people to take more advantage of the scarcest good of our modern times: time itself. Although, to be honest, I fear people will not be able to reclaim that time as theirs and, instead, spend it on more work."

Kevin Novak, CEO of 2040 Digital, replied, "We are all changing our thoughts and concepts around the definition of 'place' and 'physical,' and we will be more willing, open and trusting

to receive services that help us solve our problems or needs in the most efficient and effective way."

Richard J. Perry, a respondent who did not share other identifying background, said, "Trust takes a back seat to convenience for most."

Julie Gomoll, CEO at Julie Gomoll Inc., commented, "We'll keep trusting, and trusting more, even if we shouldn't, because we can't bear the idea of giving up our digital transactions. We're stubborn that way."

An **anonymous chief problem solver** observed, "People are fundamentally lazy. Our best and brightest typically make systems and products so the rest can get more benefit from less work. Desensitization happens soooooo much faster on the internet because you're having thousands of stimulae hurtled at you every minute instead of a few stimulae per minute doing just about any other activity in the known world. The combo of a desensitized user base and consumer-protection activities is quite likely to increase everyone's concept of 'the internet is safe' because so many stakeholders care so much about actually making that happen (more or less). I doubt we'll be 'safer' in any objective way in 10 years than we are now, but I think the average person will spend a lot less time worrying about it."

An **anonymous professor** said, "People will expect data breaches, but will use online services anyway because of their convenience. It's like when people accepted being mugged as the price of living in New York."

An **anonymous consultant** observed, "Let's assume the cybercrime arms race between bad actors and our defenders will continue without either a mass migration to some new, locked-down web or the triumph of evil. As more people spend more time performing more tasks online, their comfort should increase simply by becoming accustomed to the digital world. Abusive behavior will continue, but I don't see that driving down trust overall. Some people are unaffected by this, for various reasons. Instead, rising awareness of abuse and sympathy and support for those affected by it should help increase [trust in the internet]."

An **anonymous assistant professor of data ethics, law and policy** observed, "People will receive less information about how their data are being used, and in the absence of massive public disaster, they will trust more and question less."

An **anonymous faculty member at a large university** commented, "People are very poor at risk assessment and are desperate to communicate with one another. In general,

short product lifetimes ('fads') will allow connection-addicted users to stay ahead of the massive hacks that destroy each system in turn. This applies to brand apps as much as it does social media. As for shopping, convenience will always trump security, and short-attention-span consumers now have brand loyalties driven solely by the associated perceived social status. Quality and value are irrelevant; why would security matter?"

An **anonymous respondent** wrote, "At this point one can just assume your private information has been stolen; and nearly everyone is now aware of phishing scams and other threats, yet humanity is just as happy to accept those risks in favor of free shipping. Institutions are pushing more services online-only (to save money), forcing people online despite risks. People continue to shrug and carry on."

An **anonymous respondent** commented, "I ticked the box that says [trust will be] 'strengthened' because the majority of people do not care (or don't understand) that the governments of the world (and certain tech corporations) are attempting to harvest our personal data for nefarious purposes. So for most people, they will only see the benefits of internet-connected smartphones, and they will grow to trust the machine."

Another **anonymous respondent** commented, "Best-in-class, encrypted applications will suffer episodic attacks, but the convenience of using them in an increasingly centralized corporate economy run amok will make people trust them without much fuss or critique."

Nathaniel Borenstein, chief scientist at Mimecast, commented, "Because most people are completely unqualified to judge the underlying technical issues, their trust in various online activities will be shaped by what they're told, i.e., whoever commands the biggest ad budget. That would seem to be good news for the purveyors of online services."

Bernardo A. Huberman, senior fellow and director of the Mechanisms and Design Lab at HPE Labs, Hewlett Packard Enterprise, replied, "Unless people learn of a big breach in security at a level that affects them, they will continue to trust blindly the new technology, mostly because of their ignorance of how intrusive it is."

Many said that ubiquitous connectivity and its affordances will cause trust to be "baked into the system" becoming accepted, remaining invisible or at least being transformed to a mostly forgotten factor.

Daniel Berleant, author of "The Human Race to the Future," said, "Digital devices are becoming more pervasive all the time. Questions of trust and privacy will always be there but there is no reason to expect their impact to be greater than has been the case so far."

Luis Miron, a distinguished professor at Loyola University New Orleans, said, "The issue is not complicated in my mind. I believe – though I lack empirical evidence other than general market trends – that prices will continue to fall for smartphones and other digital platforms. This will increase online consumer participation. With increased usage, consumer expertise and access will expand, and so on."

An **anonymous Ph.D. candidate** commented, "People will continue to be comfortable. It is very difficult to remain vigilant."

Alexander Halavais, director of the social technologies master's program at Arizona State University, wrote, "The process of globalization has often been seen as one related largely to politics and technologies of transportation. In practice, we have already moved beyond this. Distance is almost certainly not dead, particularly when it comes to traditional cultural exchanges. However, especially in spaces of economic and commercial exchanges, as well as in some cultural institutions (those that throughout history have been tied to cosmopolitanism), distance will quickly become less important to interactions. Especially in places where mobile devices have provided an opportunity to 'leapfrog' into the information age, we will see the effects of distributed services make interactions across languages and cultures far more common. Trust will be baked into the system."

An **anonymous computing sciences professor at a major technology institute** said, "The connectivity among people, and between people and institutions (e.g., banks, retailers, governments) is going to help both the urban population (e.g., bypassing traffic and other physical obstacles) and the rural population (e.g., shrinking the physical distance)."

Some said cultural acceptance will play the largest role in relieving trust concerns.

Garland McCoy, president of the Technology Education Institute, said, "We have reached critical mass of social acceptance of the internet as a platform for commerce, education and social engagement. Peer-to-peer familiarity will help ensure robust adaption and utilization. The internet is like sex education; you get it through your friends."

Stephan G. Humer, head of the internet sociology department at Hochschule Fresenius in Berlin, wrote, "People's trust will be strengthened because we see an ongoing spread of

digitization throughout the world and a growing knowledge regarding the importance of dealing with digitization. New players will arise, new forms of digitization will be shaped, but there is one area of life that truly makes a difference: culture. The more we have a fully digital culture, the better it will be for trust, for privacy, and for society in general. Trust cannot be built through technology. Trust is a social issue."

Many participants in this canvassing took note of the public's previous transitions to mostly trusting technology despite proven risks – for instance, pointing out that people die in car crashes but that does not stop them from using cars.

An **anonymous respondent** wrote, "Any new technology is not trusted at first: the car, the aircraft and so on. We are still at the infant stages of the internet. By the end of this century the internet and related technologies shall be 'embedded' in most items that we own and will work with little or no user input."

An **anonymous participant** wrote, "We will trust technology with our private information. We love the ease of it too much not to. An example: My boyfriend doesn't carry cash – ever. Cards, phone apps – people prefer comfort over trust. It's too easy to say 'it won't happen to *me*' when it comes to identity theft or other issues. People will take precautions, like wearing a seat belt in a car, and there might even be government regulation, just like seat belts; but even with thousands of deaths on the road, we still drive cars."

An **anonymous professor of media production and theory** said, "This is very complex. I, like many people, engage in vast numbers of transactions globally. We will see more of that on every level. I have done a lot of work/research in Africa, where the phone starts to take on the task of many institutions, from hospitals to banks. I am particularly excited to see increased transparency in government in online contexts. The big problem is that on all fronts, our increased trust is easily taken advantage of by those who provide platforms, pay for information about our activity, etc. Until there is some kind of real 'online bill of rights' I see this increased action as perilous, as potentially devastating as the advent of industrial society was to working people in the 19th century. On the other hand, in my own work, 'the pursuit of knowledge,' the effect of using the internet has increased my ability to research and theorize, as well as to share with colleagues by something over an order of magnitude."

An **anonymous professor at a public university** observed, "We are just at the dawn of developing digital commercial and social applications and there are a number of implementation innovations that need to be developed to improve the experience and

increase security. However, the commercial viability of these applications will drive improvements to increase consumer use of these systems. The applications will be too convenient for most consumers to miss out on and they will become the primary way we do business, shop and engage in social organization."

Subtheme: There will be no choice for users but to comply and hope for the best

A number of respondents went another step in describing how the inexorable march toward mass adoption of online interactions will proceed, arguing that the public will not have the energy, interest or capacity to resist because most aspects of daily life will require compliance. These experts say tech usage and acceptance will simply become normalized – often adding that this acceptance does not imply trust. An **anonymous respondent** said, "Users will be coerced into using online technology more as alternatives are phased out."

Marc Brenman, managing partner at IDARE LLC, commented, "It will be use the systems or nothing. There will be great impacts on national security (negatively), on personal finance, on privacy (negatively), on politics (coarsening)."

An **anonymous respondent** wrote, "Trust will be strengthened only in that relying on online interactions, with risks, will so be normalized that a considerable number of people may not know better, and may not question the architectures of online interaction."

Yar Quasar, a businessman, observed, "Trust will decrease as knowledge of the risks grows and as people's lives get ruined by trust. However, this will not slow adoption since it will become untenable to live outside the new system."

Peter Morville, president of Semantic Studios, said, "Trust exists in a state of persistent disequilibrium. We need it to function as a society, but the threats and breaches will continue."

An **anonymous technology writer** said, "The late adopters will find that yesterday's analog services are no longer offered. They'll be forced to trust in other methods since there's no alternative. I expect the cellphone as a device to be obsolesced by some other media innovation, but it's hard to understand what that might be. It might be a chance to start over with a new and purpose-built structure of online interaction that's less frail and corrupt than the ones we have now."

Bart Knijnenburg, assistant professor in human-centered computing at Clemson University, responded, "I don't think online threats will diminish – in fact, they will likely increase – but users will be increasingly *required* to interact online. As they become more familiar with this, their trust will increase."

Polina Kolozaridi, a researcher at the Higher School of Economics, Moscow, noted, "I answered 'Trust will be strengthened,' but it is more complicated. There are as of yet no other mediums to trust. But I am sure that trust in online interactions will not be anything different from the offline."

An **anonymous professor** said, "People's trust is built exclusively on perception. Increased experience with a thing gives them greater trust, even when it is not deserved. So long as internet retailers and other sites improve their capacity to avoid hackers, there will be greater trust simply by the fact that more people will have to participate in the online economy."

An **anonymous futurist** wrote, "Trust in mobile communications will be strengthened because it must. People will not have a choice. Every area you mention will change. I do not know how, but I know they will be different. Also, you did not mention family life, which is already changing in families that have phones. The phones are designed to mediate communications between people. That is the purpose. All of our social institutions are built upon communications between people. Now, take a device that is designed to change the relationship between people and the institutions must change. The people born into the mobile communications age are just reaching adulthood. I expect a social change more difficult than the 1960s is coming in the next five to ten years. The digital natives will have a very different ethic of behavior than the 'older' generations."

Vin Crosbie, a professor at Syracuse University, wrote, "Although alarming incidents of massive breaches of online security will probably occur during the next 10 years – probably extending upon the public's largely false sense of worry or distrust now about online security – people will nonetheless use utilize online interactions much more during the next 10 years than now."

An **anonymous program director at the U.S. National Science Foundation** commented, "It is already part of the background fabric of our lives, and so will go on unquestioned except when things break. Some of the security must improve, both through technology and education."

An **anonymous software engineer** wrote, "People's trust will have zero correlation with reality. It is not appropriate to expect their feelings of trust to correlate with actual technological details."

A share of respondents argued that the builders and purveyors of these technologies are not illuminating privacy violations and security threats to the public clearly enough, and some note that the public itself will continue to adopt shiny new tools without question, whether out of necessity or just because they want them, of course failing to read any lengthy, dense and undecipherable terms of service and end-user agreements.

Laurent Schüpbach, a neuropsychologist at the University Hospital Zurich in Switzerland, said, "Most new technologies and devices are marketed as more practical (easy to use) and rarely as more secure (more complicated). I've already seen so many scandals – from Edward Snowden to password leaks to privacy negligence on Facebook – that I can't imagine what more is needed so that people start to realise that security and privacy online is a big deal. Trust is given as far as everyone is using [these technologies]. But, as most companies and governments profit from the overall ignorance on these matters, nothing will improve."

John Anderson, director of journalism and media studies at Brooklyn College, said, "Trust is something that can only be developed by an informed populace. Most people have not been adequately informed about how internet technologies work to properly assess their risks and rewards. When is the last time you fully read a terms-of-service document? That said, there are also many unknowns over the next 10 years that could greatly enhance or diminish trust. On the positive side, new security technologies may harden networks, pushing online transactions to near-ubiquity. On the negative side, cyberwarfare/cybercrime or even terrorism utilizing electromagnetic pulse devices may shake our network infrastructures to their cores or even destroy them, waking people up to the real fragility of the digital world."

Sam Punnett, research officer at TableRock Media, replied, "These activities have become integral to people's lives. They are destined to become even more so as institutions incorporate them for a variety of motives. There will be an increasing awareness that systems show their shortcomings periodically, but people will likely keep believing that compromise of these systems is what happens to *other* people. Institutions will continue to move to automated interactions/transactions, assessing benefits to themselves versus risk analysis of encountering catastrophe. Of course it often takes a catastrophe to reveal errors in the risk analysis."

An **anonymous IT architect** noted, "Trust will be strengthened, but that doesn't correlate security or privacy. I've been asked to demo health care apps, and I can't think of anything I'd more rapidly avoid than sharing that sort of data with insurance companies, who already make healthy profits over denying coverage for even the simplest of procedures yet have a government mandate to exist and charge ridiculous premiums for this shabby coverage. Education over a phone is ridiculous. They're far too tiny. Over a regular computer, sure, it works to a degree, but the death of the PC receives frequent press."

An **anonymous research and evaluation director at a major university** wrote, "People are going to have fewer and fewer choices for non-online transactions and will have to come into the cybermarket fold. The security providers will have to stay one step ahead of the thieves."

An **anonymous respondent** said, "People will eventually come to accept that they will be excluded from mainstream economic life and from good health care and education if they are outside the online world. And one hopes that security to protect privacy will also improve such that people will come to trust the systems more. However, it is likely that a growing group will live off the grid, never trusting that they will be protected in this environment."

An **anonymous information security manager** replied, "Unfortunately, it will be strengthened since the majority of users are not IT-savvy on issues of privacy and surveillance. This is why all elected officials should be taking a more responsible approach as the advocates for their citizens rather than simply parroting the greatness of high technology in fighting terrorism."

An **anonymous respondent** commented, "I ticked the box that says 'strengthened' because the majority of people do not care (or don't understand) that the governments of the world (and certain tech corporations) are attempting to harvest our personal data for nefarious purposes. So for most people, they will only see the benefits of internet-connected smartphones, and they will grow to trust the machine."

A number of respondents agreed that the inexorable march to full, fuller, fullest connectivity will overwhelm trust issues, but some also pointed out that connectivity becoming the new normal has beaucoup benefits beyond simple convenience.

Isto Huvila, professor at Uppsala University, wrote, "More and more interactions will take place online. People will have no alternative but to trust in things that make their everyday life work for them. But, on a larger scale, trustworthy and traceable technologies will have an

impact and could play a major role in increasing the trust between those actors who operate online, and between the society and the actors who provide online services. If we can trust in a systemic and systematic sense in online technologies and services, they can really replace others not only in technical sense but also as a basis of how people interact with each other and remember things, and as a baseline of how things are supposed to work. This is unlikely to happen during the next 10 years, but trust in the digital is slowly becoming the new default unless something very dramatic happens that would essentially make online interactions impossible for a time."

M.E. Kabay, professor of computer information systems at Norwich University, replied, "Trust will increase simply because familiarity consistently increases even irrational trust. Risk analysis is not a strong point among human beings. A simple illustration is that many people fear death and injury from terrorist attacks far more than from domestic nutcases armed with automatic weapons, from drunk drivers, and even from ordinary car accidents. Reality has little influence over emotion. Impact is likely to be affected by the growing population of smartphone-equipped users, especially in developing countries. In East Africa, for example, we have already seen major effects on economic justice simply because inland farmers have been able to find out how much their crops are being sold for in coastal cities. The tool for this information exchange? Mobile phones – not even smartphones. In East Africa and elsewhere, impoverished, cash-deprived rural family members have finally been able to benefit from the income of their diaspora simply through text messages facilitating money transfers, quite separately from the official banking systems. This kind of disintermediation can be highly positive. Disintermediation (removing absolute control of centralized power centers) over information flows threatens established dictatorships; they will retaliate to suppress independent information flows. We have already seen several examples in which such governments have interrupted internet access for their own citizens in what they perceive as emergencies. The People's Republic of China routinely does so using the so-called Great Firewall of China for controlling external information inputs. On the positive side, remote interactions for creative work have resulted in brilliant innovations such as virtual choirs (look up the work of Eric Whitacre for stunning examples). Augmented reality can include artistic efforts in addition to chasing imaginary pets as in 'Pokemon Go.' See the materials for my course Politics of Cyberspace for more material on these questions. As for blockchain systems, these cryptographic signatures may help decrease anonymity, but they won't stop pseudonymity."

Frank Elavsky, data and policy analyst at Acumen, commented, "Unfortunately [there will be] less suspicion where suspicion should be due. But, aside from that, I believe the quality of life will significantly improve in the global context (so long as access to the internet is not

restricted at the national level). Reading levels, political views and standards of living will grow as access to the internet increases. I do believe that cultural life will begin to suffer, however, because many exclusive cultural ideologies may lose traditions or practices as access to the internet grows. The impact will be globally more positive, but trust-strengthening could result in vulnerable populations being taken advantage of."

Theme 4: Some say blockchain could help; some expect its value might be limited

Trust is embedded in many things that foster relationships and transactions. Money is the prime example of a trust-infused artifact. People exchange it for other things of value because their governments say that their currencies are "backed" by the authority of those governments and, often, other governments. In days of yesteryear, money was tied to specific other things of value like gold. But nowadays, money has value and can be exchanged for goods and services because there is society-wide "trust" that the institutions supporting it have value.

Blockchain is a system that aims to replace organizational guarantors of trust with a technology-based arrangement. It was designed to be a "trust protocol," as Don and Alex Tapscott explain in their book, "Blockchain Revolution." Blockchain was first created by a person or persons using the name Satoshi Nakamoto for enabling the digital currency bitcoin. The blockchain is like a global spreadsheet or ledger that uses peer-to-peer networks to verify and approve transactions. In the case of bitcoin, it was a scheme aimed at certifying currency-based exchanges. As the Tapscotts write:

> "Each blockchain … is *distributed:* It runs on computers provided by volunteers around the world; there is no central database to hack. The blockchain is *public:* anyone can view it at any time because it resides on the network, not within a single institution charged with auditing transactions and keeping records. And the blockchain is *encrypted* … to maintain virtual security ….
>
> "Every ten minutes … all the transactions conducted are verified, cleared, and stored in a block which is linked to the proceeding block, thereby creating a chain. Each block must refer to the preceding block to be valid. This structure permanently timestamps and stores exchanges of value, preventing anyone from altering the ledger ….
>
> "This new digital ledger of economic transactions can be programmed to record virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims, votes, provenance of food and anything else that can be expressed in code."

The Economist provides another useful blockchain explainer here.

Advocates say they expect that the widespread implementation of blockchains could disrupt every "trust" intermediary in the economy, including banks and other finance institutions, insurance, legal operations, accounting, health care record-keeping and government bureaucracies. They hope it will "cut out the middle man" and allow people to have more secure and private control over personal information and transactions. A share of the experts in this canvassing shared this enthusiasm – or agreed it had substantial potential to build trust in online interactions.

However, some of the respondents to this canvassing expressed some level of wariness about how far blockchain adoption will spread and what its impact will be. This section of this report starts with the most enthusiastic comments, followed by the most skeptical.

Subtheme: Blockchain has potential to improve things

Most people who responded that blockchain technology might have an impact said it could enhance the likelihood of security and privacy. Many said it is just one of the possible approaches that could be implemented to assure more trust in transactions.

An **anonymous longtime Silicon Valley technology firm communications executive** commented, "The fact is we already trust online interactions a lot – for banking, for travel, for job applications, social interactions/sharing, etc. I think, over time, blockchain will help with trust a lot and get people over what concerns they do have. It will take some great use cases (and not technical under-the-hood explanations, which don't help people adopt it) to gain traction."

Brian Behlendorf, executive director of the Hyperledger Project at the Linux Foundation, said, "The net effect will be positive, as the greater use of blockchain technology to tie together the systems of the world outweighs the ever-present concern over the security and sanctity of individual systems."

Dan York, senior content strategist at the Internet Society, commented, "Blockchain systems are *one* of the many different building blocks that can bring about a more-trusted Internet. They may have a role as a distributed ledger system – but we'll need to see how their usability evolves and what kind of deployment we see outside of cryptocurrencies."

John Sniadowski, a systems architect, wrote, "Trust levels will vary across timelines based on the changing threat landscape and high-prominence security failures. Being able to prove identity with high degrees of certainty is of paramount importance. Until identity systems are

improved to become more robust against theft and impersonation there is no real basis for online trust. This will impact across all online activity. Identity systems based on blockchain architectures may be able to improve overall trust on transactions. Loss of control of personal information will have an overall negative impact on online trust."

Glenn Ricart, Internet Hall of Fame member and founder and chief technology officer of U.S. Ignite, said, "Blockchains will help to preserve a degree of privacy in a world which increasingly expects transparency."

Frank Elavsky, data and policy analyst at Acumen, commented, "Regarding blockchain systems, I feel as though the incredible integrity of blockchain systems could lead to serious problems for people in power who [are discovered committing] regular, unsavory acts within the world of finance. Because of this, the result could be very good for the majority of people or it could be very bad – people in power tend to manipulate systems to their benefit."

An **anonymous respondent** commented, "With the rise of bitcoin or other virtual currencies people may switch to these entirely as global currencies, as the dollar and euro may see too many ups and downs."

An **anonymous media industry technology consultant** said, "Blockchain systems may help increase the trust, but these systems will need to be better integrated into existing (and new) online services. Time will increase the trust level. As long as these systems are not compromised and continue to work as 'advertised,' people's trust in them will increase."

An **anonymous computer science professor at a European university** wrote, "People are already engaging in all sorts of activities online, they will just spread more as these can also be done with any sort of mobile device and at any time. There is a need to build trustworthy – private, sound and secure – systems to ensure the increase in usage. I expect health care and political and civic life to be most strengthened by this trend. Blockchain will lead to the disappearance of jobs such as trusted third parties, but it will allow the appearance of new possibilities and new jobs."

An **anonymous respondent** observed, "Blockchain systems feel like they'll remain slightly more specialised, though there's certainly a possibility of a big corporation picking it up and normalising it."

An **anonymous professor of media and communications at an Australian university** commented, "All areas of social life will be affected by deepening of online

interaction. Blockchain systems can play a positive role in strengthening trust – as long as implementation involves all stakeholders, and is framed democratically."

Matt Bates, programmer and concept artist at Jambeeno Ltd., commented, "On blockchain technology … I suspect it might have a great positive effect on, e.g., transparent corporate and government auditing practices."

LT Wilson, a respondent who shared no additional identifying details, commented, "It seems that blockchain and Ethereum will help ensure encrypted, authentic history of much more than financial transactions."

Jannick B. Pedersen, a futurist and impact investor, said, "The emergence of blockchain is not a final answer to perfect trust – just as anti-virus software has not provided perfect protection. Blockchain technology will, however, increase our trust in the online world."

Ray Schroeder, associate vice chancellor for online learning at the University of Illinois, Springfield, predicted, "Blockchain architecture networking will enable students to assemble custom degrees and certificates with online courses and competency assessments collected from a wide variety of sources."

Norwich Unversity's **M.E. Kabay** said of blockchain, "These cryptographic signatures may help decrease anonymity, but they won't stop pseudonymity."

Don Philip, retired lecturer, observed, "Blockchain is a bit of a wild card. It's a new technology and the banks are watching it closely. I would expect that banks will be among the principal users and providers of blockchain-managed transactions, partly because they have already gained people's trust in financial transactions."

Anonymous respondents also wrote:

- "The ease of using online commerce is quickly displacing reliance on brick and mortar. Blockchain trust systems may speed this development."
- "Improved encryption and the emergence of blockchain will improve trust overall. However, there will likely be a period of growing pains; perhaps that is what we are experiencing now."
- "I am excited about blockchain, but can only imagine financial uses. Real applications will overcome my lack of imagination."

- "Blockchain will enable secure transactions in currencies, as well as data. Social reputation will also continue to influence who one chooses to do business with."
- "Trust will be increased if technologies such as blockchain are adopted more and more. Trust will be increased if governments put in place policies for consumer protection, data protection, etc."

And an **anonymous principal security consultant** predicted that 2026 is too soon for blockchain solutions to have significant impact, writing, "Bitcoin and other blockchain-based systems have their benefits, but it does not seem likely that any one blockchain will see massive adoption over the next decade, unless there are significant improvements, particularly in storage requirements and reaction times."

Subtheme: There are reasons to think blockchain might not be as disruptive and useful as advocates expect it to be

Henning Schulzrinne, a professor at Columbia University and Internet Hall of Fame member, wrote, "Blockchain systems do not seem to address any real problems, except if you are in the business of distributing ransomware. For example, the recent SWIFT attacks would not have been prevented by blockchains – since the initial transaction was done by a legitimate actor, internally compromised, all the other signers would have simply confirmed that the compromised bank indeed wanted to transfer millions to a casino in the Philippines. There are real opportunities for improving electronic financial transactions, but anonymity and non-reversibility are bugs, not features."

Adrian Schofield, applied research manager, commented, "Urban dwellers will use more e-commerce, e-retail, e-services products for convenience and speed of service. Rural dwellers will use more e-health, e-education, e-government products. My personal view is that blockchain systems will not become mainstream within 10 years, due to a combination of vested interests in the existing currency markets and lack of trust in the new system."

Will Kent, e-resources staff member at Loyola University Chicago, wrote, "People will become more accustomed to blockchain pay systems. Soon they will become integrated into more-traditional pay systems and no one will bat an eye. Regardless of how technology will impact these activities, users will find comfort in their convenience. Safety will be improved for mass consumption with an 'acceptable' number of compromised accounts, passwords, zero-day exploits, keeping developers, companies and users on their toes. I should clarify that just because people trust their interactions doesn't mean their interactions will be what they want them to be."

One **anonymous respondent** commented, “The blockchain is just one technology among many and its role will likely be marginal compared to the overall system.” Another was highly critical, writing, “Blockchains are not a magic bullet; they might mitigate some of the effects on economic activity, but the crypto-currency scene has been rife with scams so far and I don’t see that changing any time soon. Not to mention there are methods to reverse-engineer or otherwise manipulate chains, which undercuts their position.”

An **anonymous software architect** proclaimed, “The blockchain is overblown and solves nothing that isn’t already solved in some other way. Besides, it doesn’t scale – when you have to have global agreement on local decisions … nope, it’s not gonna happen.”

An **anonymous respondent** wrote, “Blockchain? You are talking gibberish to most people.”

Another **anonymous respondent** said, “I am not convinced the blockchain is essential for everything. I think it will have a few uses. But there are massive costs to run the blockchain, so it might be simpler to just trust a few institutions, and let them charge a tiny fee to run a centralized infrastructure. (Just like we all pay big fees to credit card companies right now, but they are failing at the security aspect.)”

An **anonymous respondent** commented, “It will depend on new systems and evolving expectations. Amazon depends on trust; will it maintain it? Blockchain is about avoiding trust and will prove mostly about libertarian fantasy.”

Theme 5: The less-than-satisfying current situation will not change much in the next decade

A noteworthy number of those responding to this canvassing are not convinced that much progress will be made in people's existing attitudes about trust online.

Ed Lyell, professor of business and economics at Adams State University, wrote, "Security is the key to which direction we go in trusting transactions to electronic form. Passwords are mostly inefficient, especially since to be safe they become so complicated as to frustrate the user. Biometrics are likely to give us more security with less effort. As these emerge, and work, trust will expand and commerce of many types will expand online. It may also be necessary to move toward global policing and significant enforcement. This is the weak link in the chain since all too many nation states participate in as well as harbor the online thieves. Like tax evasion it will take a global response, which is not likely in the near term."

Joe Mandese, editor-in-chief of MediaPost, replied, "Forces will push this simultaneously in both directions. People will trust online interactions more because they will become more familiar with them and because new technologies – especially blockchaining – will create a more secure infrastructure. People will also trust it less, because new forms of interactions will be created that they will not be familiar with and these will create opportunities for less security. Two simultaneous forces pushing in opposite directions."

Scott Fahlman, computer science and artificial intelligence research professor at Carnegie Mellon University, observed, " 'Trust' is the wrong question to ask. Smartphones and non-expert people doing complex things online are recent phenomena, very sudden by historical standards. In the past, human societies have had decades or centuries to come to grips with such disruptive technologies that have great potential for both good and bad consequences. The user community (which might be almost everyone) has to understand what these technologies do, what are the dangers, and society has to make new rules and social compacts about what things are OK, what are bad (in certain contexts), and how to police or prevent the bad ones. That takes time, and we're not there with internet and cellphones. But kids who have lived with these things all their lives now are getting much smarter about what to do and not do, and society is beginning to come up with some consensus views on the limits of privacy invasion, etc. We need to work on this, but we needed to work on the rules for newspapers, broadcasting, high-speed driving, and so on. The difference now is that we need to do this more quickly than before."

Dan Molina, coordinator of special projects for the World Business Academy and former NBC News correspondent, commented, "The internet is a reflection of our character and intentions as people. It does not increase or decrease our propensity to positive or negative purposes. It is another tool, as were the wheel, the telephone, the typewriter and various devices in earlier eras. The differences now are the immediacy of access and the fact that technology abolishes geographical boundaries. So we are forced to confront a global mix of realities that vary widely. We are forced, in some cases, to deal with continuously insidious behavior and facts outside of our everyday thinking. The internet and media technology can and will, as always, be used for anything. This can be the highest of purposes – education, information, illumination, as entertainment and a means of social interaction. It can also be used for crime and to serve the abominable instincts of human nature. The flaw is our regarding these things with indifference. Each expansion of our capabilities requires more of us. Of course we can use it productively, and of course it will be a method of proliferating the worst in human nature. As always, we must relish, celebrate and encourage the best of these opportunities and fight the worst as best we can. Like it or not, we have a lot of new neighbors, like great-grandma on her party line."

Jennifer Zickerman, an entrepreneur, commented, "Trust will stay about the same – low. We continue to use devices and services that put our privacy and economic security at risk, lamenting the risk and paying for it indirectly (bank and credit card fees, etc.). The technology industry has failed dramatically in providing secure mechanisms for data transfer and storage. It is astonishing to me that they are not held accountable for their failures. There will probably be several large-scale security meltdowns with more-immediate consequences that will make people demand improvements. However, systems are so fragmented and ill-designed that there will only be grand pronouncements (by companies and governments) and temporary solutions, leading to an even bigger hodge-podge of draconian front-end security mechanisms while still tolerating security holes in the back end that you could drive a tank through."

Steven Polunsky, Spin-Salad.com, said, "We will see a convergence of online and real life in this area. In both, people will need to be vigilant about their surroundings, skeptical of strangers, and aware of risks in areas they venture online and off."

An **anonymous fellow at an organization assessing the future of privacy** wrote, "This depends on how companies behave, i.e., how aggressive they are in the use of personal information. It also depends upon whether people are comfortable with the risk-to-benefit calculus. And it depends on whether personal information can be secured. Due to problems with global hacking, it is unlikely I will ever do banking using my cellphone. A lot of ongoing

consumer education is needed. Consumer concern and the feeling of resignation about the current situation is already really high and is likely to stay the same."

Karel Kerstiens, retired from the U.S. Air Force, wrote, "There is a certain balance on the internet of 'good versus evil' in reference to technology. I was on the internet back when Google indicated there were less than 5,000 websites indexed. The balance of 'good versus evil' technology back then seems to be roughly the same today. This strongly indicates to me that the future balance between the good actors and the bad actors should closely remain the same as it is today."

Axel Bruns, professor at the Digital Media Research Center at Queensland University of Technology, commented, "I'm not sure that trust will continue to play an especially important role in these questions into the future. It seems more likely to me that there will be a gradual curtailing of alternative options for such transactions: Banks and government offices, for instance, are increasingly moving their client engagement facilities online while reducing offline transaction opportunities. It will become more and more difficult for clients to resist such a push to use online facilities. This may open up a market for small players offering bespoke face-to-face services, but it is unlikely that they will be able to capture more than a small slice of the market. On transactions, essentially what we are seeing is a supplier-driven push to use online services, which is only slightly mitigated by government regulations that require some essential services still to be delivered in non-online modes as well, especially to people and communities who remain offline or poorly connected. On social interactions, as opposed to transactions, the dynamic is different, and there is more of a user-driven pull that is driving adoption; this in turn is related in particular to network effects. Here, remaining offline or poorly connected – deliberately or because of adverse circumstances – is increasingly felt as a significant disadvantage. The more acutely that disadvantage is felt, the more likely users are also to overlook significant concerns about trust: You may not fundamentally 'trust' Facebook's handling of your data, for instance, but you may nonetheless use Facebook because of the substantial peer pressure to do so (and the fear of missing out associated with not using it). One way for many users to address such mistrust of key platforms is likely to be the creative obfuscation of personal information, in an attempt to make personal information less traceable – even if the growing sophistication of profiling algorithms means that such attempts are largely unsuccessful."

John Howard, creative director at LOOOK, wrote, "Wireless technology has allowed developing countries and economies to leapfrog infrastructure requirements (power, telecom, banking, etc.). For many in the developing world – as well as those who want to

interact with them – the risks are outweighed by the opportunities. As a result, both good and bad actors are drawn to the new opportunities this creates."

An **anonymous founder and CEO** said, "Overall, I hope trust will remain the same but there will probably be a trust shakeup – i.e., some big players will abuse their trust and lose their audience/customers and others will step in. I hope."

An **anonymous systems administrator** commented, "The 'drug' is so good that people will use it even if they don't trust it – the platform is too deeply embedded in people's lives. I suspect that the revelations going forward will only get worse. I do think that total surveillance is the norm. I do expect that people will adapt."

An **anonymous respondent** observed, "Barring something exceptional happening – e.g., quantum computing rendering existing cryptography obsolete with no alternatives – nothing will change. The general public will remain largely ignorant of the systems protecting their communications; criminal organizations and states will continue to abuse and hack both the low-hanging and high-reward fruit."

Another **anonymous respondent** wrote, "The internet offers more of everything. If you don't trust one service, you can easily put your trust in another. Distrust will always be an issue, but with more options, people will be more likely to put their trust into something rather than just forego the entire experience altogether. All factors listed (economic, political, cultural, civic, educational, etc.) will be greatly affected. With the internet, people have more choice in where they get their education and news. They choose who they get to interact with, defining their own culture. Don't like your present situation? The internet will inform and give you options. As long as the internet continues this, trust will remain the same."

An **anonymous senior software developer** replied, "Most people don't even think about the issue of trust when it comes to online interactions. They take for granted that they're safe … until they're not, which happens increasingly frequently. But because there's no real separation between the anti-security measures used by law enforcement, intelligence agencies and a growing subculture of cybercriminals, measures to make people more aware of online threats will be suppressed."

An **anonymous respondent** wrote, "If economic justice is addressed in meaningful ways, trust will increase. Until then, trust will remain about the same. Educational initiatives aimed at rebuilding trust also seem lacking. Workplace trust appears diminished, given the lack of mutual loyalty in most jobs, as well as the economic disparities between those at the top and

those actually delivering the products and services. Culture is about the only area where I see change for the better."

Anonymous respondents also commented:

- "We're still a long way from 'Six Sigma trust' in the online world."
- "The cat-and-mouse game will continue."
- "I expect there to be surges of mistrust and trust as users demand more security in various privacy aspects (buying/selling/banking, health care, social media) and more access that weakens the security measures."
- "Trust may stay the same but ignorance of security will grow. People now know all about the NSA bulk email scrapings but virtually no one outside of IT circles has pursued cryptographic solutions."
- "It'll be both (as there are always security breaches) but familiarity causes complacency if not trust."
- "Trust will stay about the same, but use will continue to rise as the use of technologies in general (not just phones) becomes more expected, normative and sometimes necessary. But there will be enough concerns and incidents that I don't think there'll be a major increase in trust, and enough apathy that I don't there'll be a major decrease."
- "On one hand the ratio of web-native users (born in this millennium) will grow larger and therefore trust will be strengthened (due to different privacy concept), but on the other hand media exposures of surveillance such as the NSA and online use of users' information by giant companies such as Facebook and Google who are 'caught meddling' with the data will diminish trust."
- "There's a lot of both good and bad things that happen in an online world. It feels like the sophistication and frequency of hacking, attacking, etc., is going way up, but – on the flip side – it feels as if people are becoming numb to the issues and continuing on (e.g., because they're not 'directly' bearing the cost if their credit card is stolen, etc.)."
- "There does not seem to be broad-based concern about the current and potential impact of mass government surveillance, or about the enormous pool of exploitable personal information being created by the surveillance economy. Where there is concern, the unusability of most encryption technology by non-specialists and the centrality of tools like Google and Facebook make it difficult to take any practical steps to address it. The current status quo will be the future one."

Theme 6: Trust will diminish because the internet is not secure and powerful forces threaten individuals' rights

The internet was not built with trust-building in mind, and about a quarter of these experts predicted that there are a number of threats that will be hard to defeat. Some spoke of the role of criminals and trolls. Others referred to corporate behavior and governments' motives leading to the privacy invasions, surveillance and data breaches that make the public uneasy about online transactions.

An **anonymous professor at a public university** noted, "Two major forces are working against trust: 1) Corporations. They care about trust and security to some extent, but their interests are not aligned with those of consumers. 2) Those [bad actors] who attack individuals and systems and will always be a step ahead of any possible security measures. As people hear more and more about data breaches, etc., they will become more distrustful. Already, many people who are not technically sophisticated take a blanket approach in which they wish to reveal nothing to anyone. And others do just the opposite, believing that no one wants their data, trusting the big corporations will protect them, or deciding they can't function without online interaction and giving in to risks."

Some pointed out that as internet usage continues to rise – with hundreds of millions more people, maybe more than a billion, likely to join those already online by 2026 – interactions will increase, hiking the likely chance of more criminal exploits and more potential for institutional incursions impacting more people, thus less trust. An **anonymous senior researcher who works for Microsoft** observed, "As more and more people come online, that's more and more targets for scammers. Since reaching people online is so easy, the scammers' negative actions are magnified."

An **anonymous principal engineer for an IT and network vendor and service provider** predicted, "Trust will be diminished, but I am not saying that fewer people will use the internet for shopping, work, etc. More people will be driven to use the internet and thus will have more reasons not to trust it. Until software developers stop coding vulnerabilities (e.g., buffer overflows) into the software that runs all these systems, trust won't improve. At this time, I see very little improvement or interest in improvement in industry as a whole. As more 'things' are connected to the internet and permeate society, it will only get worse. Yes, I'm very pessimistic. At some point, society might even have to hold software developers responsible (gasp)."

Giacomo Mazzone, head of institutional relations at the European Broadcasting Union, wrote, "If you look at the number of phishing examples around us and at the number of victims, you can understand why and how a digital world without a digital literacy could become potentially a world more dangerous than the one we have today. The next billions connected will be potentially the more exposed to new generations of digital crooks that have on them dozen of years of experience."

Paul Dourish, chancellor's professor of informatics at the University of California, Irvine, wrote, "The primarily thing that banks, governments and corporations need to do in order to be trusted is to act in a trustworthy manner. Where people don't trust online action, it is not least because corporate actors have not been good custodians of user data, etc. The use of online services will increase because it will become increasingly difficult to opt out, but that doesn't mean that those services will be trusted unless entirely new attitudes toward governance and responsibility emerge."

Christopher Owens, a community college professor, observed, "This is a paradox. Trust will be diminished, but the use of online banking and shopping will continue to increase. As online shopping and banking becomes more and more commonplace, just about everyone who uses these services will at one point or another … have to deal with some act of fraud or identity theft."

An **anonymous senior lecturer in computing based in Australia** said, "I can see trust continuing to diminish as more people get bitten by scams. While one of my students – who may have invented bitcoin – built safeguards into its blockchains, it is easy for those who have little faith in science and mathematics to come to distrust them. Politics is influenced by the trust placed in commentators who admit privately that they don't tell the truth because it doesn't sell."

David Banks, co-editor of Cyborgology, said, "Trust in institutions is at an all-time low, and it does not seem clear to me at all that digital technologies will improve this situation. Trust is a social problem and overall degrees of trust in institutions will only change to the degree that technologies present a kind of stability or some other version of trustworthiness."

Christopher Wilkinson, a retired senior European Union official, commented, "Trust is already challenged. The technologies of creating and maintaining trust are still too complicated for the average use – e.g., I do not know how to encrypt my email."

Shawn Otto, organizational executive, speaker and writer with ScienceDebate.org, commented, "We are still at the early stages in understanding the vulnerabilities created by bringing the world online. As they become more clear via painful experience, trust will likely diminish somewhat."

Matt Bates, programmer and concept artist at Jambeeno Ltd., commented, "It will remain mostly the same but if it trends either direction it will probably be diminished simply because of two effects: 1) People always discount positive effects on their lives and overestimate negative effects; and 2) Online activity can have large effects on one's life, both positive and negative. Shopping (economic activity) will probably precipitate the most drastic shift in many peoples' online lives as inevitable security breaches continue to negatively affect millions (eventually billions) of lives. People will dramatically discount the untold hundreds or thousands of remarkably easy transactions they've made in the past and will focus heavily on the one time their credit information was swiped by unsavory criminals."

Many respondents addressed identity issues when predicting a diminishment of trust.

Dan Lynch, internet pioneer developer and founder of CyberCash, noted, "There are far too many ways to cloak true identity, thus trust will be a big problem online."

Erik Anderson, a respondent who did not provide any other identifying details, wrote, "With identity comes trust. You can't solve online trust issues without identity. However, with more online identity come privacy issues. The technology exists to solve these problems but it has been relatively unused and undeployed."

Maria Pranzo, director of development at the Alpha Workshops, said, "Until an infallible [personal identity] marker is created … the hackers and thieves will always be one step ahead. That said, we're suckers for convenience, and I don't see us going back to in-store banking. And give me Netflix or give me death."

An **anonymous respondent** commented, "Until we have identities that cannot be 'stolen' online we will only have more problems leading to less trust. Maybe blockchain could do it, but the resistance from the large existing financial institutions will be too large for a new normal to develop until we have fundamental change in our economic structure."

Another **anonymous respondent** observed, "Flawless identity verification is the holy grail of online services. Until that exists, there will be 'mattress stuffers' who do not trust online services for banking, health care, etc."

"Healthy distrust" was a quality held in high regard by several respondents. Among comments along these lines mentioned earlier in this report were those by **Jonathan Grudin**, principal researcher at Microsoft, and **David Karger**, professor of computer science at MIT.

Mark Richmond, systems engineer for a major branch of the U.S. government, wrote, "As stories of exploits and losses continue to add up, the general sense of trust in technology enjoyed by the mostly young will gradually diminish. The eventual state of healthy distrust will probably be a positive in the long run."

And **Chris Zwemke**, a web developer, said, "Trust will smartly decline. Distrust in systems is healthy. Activity might increase, but trust will not, and more double-checking will occur."

Arthur Kover, a respondent who shared no identifying background, said, "Overall, trust will diminish. But people will cluster into 'safe' arenas, rarely venturing into the open, unsafe ones."

Dave Robertson, a professor of political science, commented, "Trust is not too good as it is. If there are terrorist or criminal efforts that more seriously disrupt the internet – as I'd guess is likely – trust will diminish."

Janet Salmons, independent scholar, writer and educator at Vision2Lead, wrote, "Those of us who care about the internet – who feel the social, cultural and intellectual values are immense – need to step up and advocate for practices that will increase public trust. At this time, as someone who works and manages most areas of life with some computer-mediated process, I am looking for ways to limit online transactions. My trust was reduced by identity theft and hacking incidents, so I think twice before I do anything involving personal information. Alas, digital literacy has not progressed (users aren't necessary broadly literate) and many people lack basic knowledge about online safety."

Subtheme: Corporate and government interests are not motivated to improve trust or protect the public

A number of participants in this canvassing noted that corporate motivations fall generally under the category of earning profits in order to fulfill fiduciary responsibilities to investors and keep stock prices soaring, causing them to fall far short of serving the public's best interests when it comes to keeping personal information private and anticipating and preventing criminal acts and other exploitation of their technologies. Some say regulation

will be required to remedy the situation, but will government provide it if it also benefits from exploitable weaknesses itself? Most of the people expressing opinions in this category preferred to remain anonymous in answering this survey.

One **anonymous respondent** commented, "The Snowden revelations unveiled the ways in which data collection online leaves people susceptible to government surveillance. But trust in commercial systems is not only open to government snooping but also vulnerable, as it is unregulated data in the hands of private corporations. A few data leaks from now, no one will want to buy anything on their phones."

Another **anonymous respondent** said, "The internet is a security s*** show. Everyone knows that. The NSA is logging this right now. I'm sure three Russian mobs already have all my passwords."

An **anonymous respondent** said, "There is no legal incentive at all to get this right. Absent the return of strict liability for anyone who holds data beyond the session, there will never be adequate incentives to protect data. And while some portion of the population is always too clueless to care, it will not be enough to support the current laissez-faire system. Absent strong regulation, the opportunity to make the internet more useful will be lost."

An **anonymous respondent** warned, "We are **** slaves. Open your **** eyes."

Amanda Licastro, an assistant professor of digital rhetoric, wrote, "Educators and activists are calling for an increased awareness of how our data is collected, monitored and monetized. As awareness spreads I predict a backlash against wearable devices, third-party data-sharing and camera surveillance."

An **anonymous respondent** commented, "Security breaches will primarily impact economic activity, but potentially could have catastrophic effects on health care. Political and civic as well as cultural life will be primarily impacted by a better awareness that all online interactions are being monitored by one entity or another, and the promises of anonymization of that data are disingenuous."

An **anonymous scientific editor** replied, "I *used* to do these things online. I no longer do it if I can possibly avoid it. (And mostly, luckily, I can.) The internet has never been secure, but the scope of its insecurities has become truly daunting. More bad actors, more state-level bad actors, and a massive chilling effect overall. And even if it was possible to address the problem, there's no incentive to do so. 'We take our customers' security very seriously' – sure

they do, also, the check's in the mail. I doubt that blockchains will have any meaningful impact on any of it. Any more than RSA or Tor has made much difference to anyone, or DRM [Digital Rights Management] has had any impact on 'piracy.' (Mind you, biometric-based security is way worse. When the wheels come off that bus, it's really going to be a mess.)"

An **anonymous faculty member at a public research university** said, "Whether people do trust those institutions depends on how the institutions behave. As people get more experiences of online hacks, identity thefts and awareness of massive state surveillance, their trust in online interactions will wane. The only way I can see institutions countering this is if they provide guarantees against dangers."

An **anonymous respondent** noted, "The increasing probability of unsuccessful outcomes (e.g., due to overtly malicious/criminal activity) will probably have less impact on the decline in trust than the increasing non-consensual but unavoidable e-commerce-related 'transactional overhead' (e.g., mandatory 'opt-in' adver-surveillance, etc.)."

An **anonymous principal architect** said, "Smartphones today do not provide adequate protections to rein in surveillance capitalism or totalitarian government. These limitations will become more apparent with time."

An **anonymous respondent** said, "Two ways that trust will be diminished: 1) the security/privacy of the technology (hacking, NSA surveillance, data-mining policies of companies); 2) the realization (by a number of people) that the lack of human interaction leaves them felling lonely and disconnected from community and society."

Another **anonymous respondent** wrote, "As knowledge that the internet is run by profiteers, and the system is gamed, and that it truly is – as the Pentagon has designated – a 'combat zone' in need of high-end security tactics that are beyond the capability of most people to comprehend, more and more people will distrust everything about it."

An **anonymous respondent** wrote, "There will be a backlash. We've seen an increasing threat to our digital information. This includes financial and health care. Lord knows where other data resides behind the cloak of government monitoring. Freedoms are becoming restricted. Look, for example, at any effort to remove your name from the government's no-fly list or the assertion that you can be forced to use your fingerprint by law enforcement to access the data on your phone."

An **anonymous respondent** noted, "Trust in these services will diminish dramatically until either a large segment of the world population stops using certain services or a catastrophic hack adversely impacts a large swath of the population. After that, a series of lawsuits will decimate those service providers and lead to an overhaul in how online services provide security services for the data being shared. As more and more services appear online, there is an ever-growing loss of control of personal information. The companies offering or moving services online appear to be less willing to clearly articulate how they use or protect personal information. Additionally, current history has shown that services that house personal information are ripe targets for hackers and thieves."

An **anonymous principal research programmer** said, "The threats associated with the massive amounts of data collected and used by commercial aspects of the internet are becoming more obvious with each new privacy breach. As more people are forced to confront the hidden costs of these breaches, the conveniences afforded by online systems may become less palatable."

An **anonymous respondent** commented, "I personally find myself being drawn out of the digital realm, not further into it. I don't trust corporate America's values, especially those whose products are digitally based (Apple, Google, Facebook, and the huge list goes on). I don't trust government as it gobbles up every bit of our data it possibly can. If I can incorrectly be detained as a suspected terrorist upon returning home to the U.S., and I was, I simply don't trust these systems. They fail to work properly. They can too easily be manipulated for nefarious intent or to enrich the über-wealthy. I mean, are we *really* going to trust democratic elections to digital machines? Really? I've had to replace my credit cards four times over the past six years because of data breaches. I have loved and depended on my digital tools for just about everything. But I find myself exploring ways to stop using them because of a lack of trust and privacy. And I don't have anything really to hide! Damn, I even pay my taxes. Online."

An **anonymous director of research at a European futures organization** said, "Security and privacy concerns aren't being addressed."

An **anonymous respondent** wrote, "Our government is actively sabotaging the security of these systems and very few companies are powerful or wealthy enough to stand up against that pressure. We're going to see less security, not more, as states feel pressured by the terrorism boogeyman to gather as much info as possible, leaving back doors open for hackers. It also seems like there's very little being done to protect people from identity theft

and online scams targeting older people. As people hear more and more about these events happening, they'll lose trust in online shopping and online social interaction out of fear."

Revolution? Some respondents predict the public's dismay and distrust will lead to it.

An **anonymous data center technician** warned, "The banking system has failed us. The oligarchs have failed. The number of people outraged will increase. The number of people who will not stand for governments recording records of every transaction [that] every human makes will increase."

An **anonymous political science professor** replied, "Trust in major institutions (e.g., firms, governments) is declining across the globe. Trust in 'imagined communities' seems to be on the rise. The internet seems to be becoming more a vehicle of established, monied extractive interests. I believe that anti-globalization is our (near) future, and the internet will come to be seen as globalization's chief vehicle."

Anonymous respondents also commented:

- "Greed and the quest for more market share will drive ever-more-intrusive strategies."
- "Unless business and government find effective ways to halt the growth of hacking, using the internet for financial transactions will become riskier and eventually reduce use of this method of communication and transacting business."
- "My transactions should not be anyone's data."
- "If organizations like the NSA and the FBI in the U.S. are more concerned with hacking foreigners than they are with defending America's infrastructure, and other organizations overseas follow their approach as an example of 'best practice,' then the number and severity of data breaches will only increase."
- "It seems likely that we will experience more data-related scandals that might lead to diminishing trust."
- "The internet has become more and more centralized and commercialized. People already mistrust it much more than they did 10 years ago, and that will continue."
- "More people are likely to be skeptical of commercial services and their ownership of user data. This will particularly affect economic transactions, including banking."
- "I hope trust in these systems will be reduced – it's about intent in the implementation of these systems."

Subtheme: Criminal exploits will diminish trust

A number of respondents observed that more crime and other uninvited and unwanted manipulations of networked systems will emerge as more people get online and more important transactions are conducted there. Many said they expect such attacks to impact trust. An **anonymous respondent** warned, "Expect more-spectacular crimes." Another wrote, "The potential for fraud, misinformation and deception online are tremendous." And another wrote, "Inevitably, there will be increased hacking and identify theft."

Ed Dodds, a digital strategist, predicted, "Ransomware will diminish trust. Blockchain may be used for open-data-driven public policy if the Data Transparency Coalition efforts are successful. iXBRL and smart contracts may reside in both public and private chains."

Joel Barker, futurist and author at Infinity Limited, wrote, "The opportunities for mischief are enormous. Certain activities will have to stay very local and even face-to-face because of the more-sophisticated spoofing that will be developed."

Don Philip, a retired lecturer, observed, "There will be problems. Systems will be hacked and sensitive information will be leaked. This will affect any area in which there is sensitive information: education, health, finances and many more. Despite the negative impacts, the majority of people will want to use such online interactions because of the convenience and ease of use."

James McCarthy, a manager, wrote, "Trust will be diminished. Information … is vulnerable to theft and exploitation. Unless they manage to find a holy grail that effectively precludes unauthorized decryption – which is unlikely – personal and consumer data will always be at risk, and the lines between what is personal and public information will keep blurring."

An **anonymous respondent** predicted, "Financial areas will cause the most concern. With data leaks increasing, it's only a matter of time for financial data to be leaked more than it was in the Panama Papers. Thinking of the Anthem [medical data] breach, millions were affected. The breach of a major banking system like Wells Fargo or Citibank would be catastrophic, and it's only a matter of time until it happens."

Another **anonymous respondent** commented, "Unless and until a secure format for data transmission exists (all the time), trust will be diminished as the services that seemed safe will be hacked and people's information will be at risk. This exposure crosses over all uses – shopping, banking, social media 'private' settings, etc. Think of all the institutions that have your credit card on file – the phone company, Starbucks, Parkmobile, etc. It's scary."

An **anonymous respondent** said, "This issue might see a significant change in the next 10 years – there are enough vulnerabilities throughout systems that it seems unlikely that we *won't* see several high-profile instances of theft, fraud and criminal damage arising from them, and even more unlikely that the various news media will not respond with increasingly apocalyptic coverage of the subject. Net result: less trust."

Anonymous respondents also wrote:

- "We learn more from pain and fear. As bad things happen people learn to be wary."
- "There will be security issues, and more-spectacular hacks."
- "Measured trust has been declining for 30 years and I see no signs of change."
- "Trust requires a belief that both parties are transparent and concerned with mutual outcomes. I see nothing in the tea leaves that says disempowered citizens will become more trusting."
- "Big Brother will look at innocent people instead of the abusers, just like the TSA [Transportation Security Agency] in regard to air travel. There's no trust in that."
- "Trust is an emotional response and, as such, strongly affected by the latest incident or two and rarely by facts, proofs or logic. Since it is a belief system, trust will decline as incidents will increase over the coming years."
- "There have simply been too many data breaches and revelations about surveillance for people to have an increased trust. That being said, the systems in question are simply too useful and ubiquitous at this point for people to stop using them because of a lack of trust, so I am concerned that there will be insufficient pressures for reform."
- "It seems to me that trust just doesn't scale. Dunbar's Number is a good reason for that. I don't see any clear way to address this going forward."
- "Trust will be diminished but we will fail to notice."
- "Privacy will disappear. There will be an acceleration of crimes based on identity theft. People will feel increasingly violated and distrustful of technology."
- "It's hard to establish that a place is safe when it has already been proven to not be."
- "Trust ultimately boils down to trust in people. And as the number of people who join online activities grows, it will become more and more difficult to determine who to trust, and how to build that trust into architectures."
- "If the federal government can't keep our nation's spies' SF-86 [security clearance questionnaire] secure, it's hard to believe anything can ever be secure online. It's like storing a pile of gold in your front lawn and blaming the thieves for hopping your three-foot fence."
- "Expect some disastrous cyberwar or hacking attacks on the horizon. Firms and persons without truly robust backup systems could be burnt badly."

- "I am filling this survey out over a VPN. I am not the usual internet user; I am also running a Tor exit node. I think many people are unaware of the surveillance they are undergoing."
- "Trust is heavily dependent on proper security solutions going forward. Currently, the market as a whole does not focus on these issues, but instead approaches this on a 'fix it if you see it' basis. This leads to late discovery, massive data leaks and consequently distrust."
- "The current trend is negative, although an increased awareness of its importance is showing. A combination of empowered users and new business practices, technology and regulation will be needed and will require multi-stakeholder collaboration."

Acknowledgments

This report is a collaborative effort based on the input and analysis of the following individuals.

Primary researchers

Lee Rainie, *Director, Internet and Technology Research*
Janna Anderson, *Director, Elon University's Imagining the Internet Center*

Research team

Aaron Smith, *Associate Director, Research*
Nick Hatley, *Research Assistant*
Kyley McGeeney, *Senior Research Methodologist*
Claudia Deane, *Vice President, Research*

Editorial and graphic design

Margaret Porteus, *Information Graphics Designer*
David Kent, *Copy Editor*

Communications and web publishing

Shannon Greenwood, *Associate Digital Producer*
Tom Caiazza, *Communications Manager*