TRUSTED FUTURE

ADVANCING A MORE TRUSTED DIGITAL FUTURE

REPORT FINDS ENORMOUS TRUST GAP, BUT HIGHLIGHTS PATHWAY FOR EXPANDING OPPORTUNITY

By the Trusted Future Team | February 2022

We stand on the precipice of a new era of technological progress and innovation with the potential to enable us to do things never before possible, vastly improve the quality of life for billions around the globe, and help solve some of our world's most intractable problems. But it is becoming increasingly clear that we risk missing or delaying these transformational opportunities if people lack the foundational trust in the technologies needed to deliver them.

This paper combines timely new survey research with existing studies to probe the various dimensions of today's trust gap, explores the way it is impeding important digital progress, highlights the key factors which must be overcome, and explores the vast opportunities that can be achieved when we do.

> IN THE END, THE TRUST WE PLACE IN OUR DIGITAL INFRASTRUCTURE SHOULD BE PROPORTIONAL TO HOW TRUSTWORTHY AND TRANSPARENT THAT INFRASTRUCTURE IS, AND TO THE CONSEQUENCES WE WILL INCUR IF THAT TRUST IS MISPLACED."[1]
>
> **President Joe Biden,**
> Improving Cybersecurity Executive Order

IN BRIEF THE SURVEY FOUND:

01. American consumers are very concerned about protecting their privacy and security.

02. Concerns about the privacy of their personal data is a key determining factor when choosing whether to use a software application.

03. There is a cybersecurity gap. Despite nearly all respondents registering a concern about being hacked, only about half indicated they were taking even the most basic cyber hygiene practices to protect themselves.

04. Among efforts to advance the ball, users want companies to do even more to build-in privacy and security in order to keep their data private and their devices secure.

Many of these same concerns are also shared by Europeans, according to a survey conducted earlier this year by the Munich Security Conference, a German think tank.

These survey results, when combined with other insights and research, highlight the need for pragmatic policy choices and provide a potential pathway for advancing trusted frameworks that can facilitate comprehensive action toward a more trusted digital future.

Today, trust in technology has fallen to an all-time low.[2] People are increasingly concerned about being able to protect their privacy, safety, and security online. They are concerned about inclusiveness, accountability, and whether tomorrow's digital ecosystem will be better than today's. It has led to an enormous and challenging trust gap - the vast gap between the ever-accelerating digital-driven opportunities just over the horizon, and the foundational confidence in privacy, security, safety, and inclusion necessary to enable society to reap its many rewards.

If we want to advance a more trusted future, it is clear we need to take a more holistic approach to the challenges we face in order to capitalize on the life-changing opportunities on the horizon:

↗ We need the ability to trust that the technologies we use are secure by design.

Security needs to be a foundational design element built into systems at every level. This will foster agile solutions across the ecosystem that embrace best practices standards, enable continuous innovation in cyber-defenses, advance globally recognized frameworks, and should be underpinned by smart government policies to keep personal and business data secure and our economy moving forward.

↗ We need the ability to trust that our privacy is protected as a basic digital right.

The exponential growth of personal data has elevated the need for a more trusted digital ecosystem where users have the tools they need to control their own data.

↗ We need the ability to trust that the internet is safe for ourselves and for those we love.

As more of our lives move online, especially at a younger age, we need real and modern safeguards that can protect us from malicious, fraudulent, and unethical actors that seek to deceive, harm, or exploit our trust.

↗ We need the ability to trust that our future is more equitable and inclusive.

Technology can be a powerful opportunity equalizer but only if it is inclusive by design, conceived and built by a more diverse group of innovators, overcomes historical biases, and is used to build a more just and equitable world.

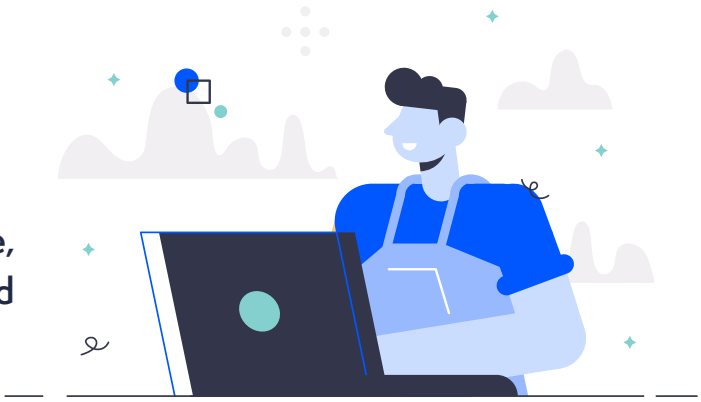
↗ We need the ability to trust that the technologies of tomorrow will be even better than today.

Building a foundational layer of trust into our technological future is a prerequisite for harnessing innovation for a more equitable economy and solving key societal challenges. In a trusted future, the next life-changing breakthroughs are not simply connecting new kinds of devices to the internet, but rather connecting people to new kinds of opportunities.

Trusted Future is coming together around a shared belief that we need smarter, more pragmatic efforts to help tackle today's challenges, restore trust in the digital ecosystem, and expand our opportunities for tomorrow. Because of the near-ubiquity of technology in our daily lives, we need to take a more holistic view of the technology landscape across software, devices, networks, and the cloud, and build a trust framework that encompasses privacy, security, inclusion, and opportunity. Our policy choices must also be assessed through a similarly holistic lens in order to examine the linkages across these issues to ensure that progress in one area does not undermine trust in another.

A future of previously unthinkable opportunities to improve our lives and advance the common good must be based on building and elevating trust. We are coming together to advance that Trusted Future.

SURVEY OF THE US TRUST LANDSCAPE



To get a clearer picture of the US trust landscape, Trusted Future commissioned a survey conducted by the research firm AudienceNet of 2,051 Americans in October 2021.[3]

The survey shows there is an enormous trust gap when it comes to how we use our digital tools, but also highlights opportunities to advance a more trusted digital ecosystem. Among its key findings:

LACK OF TRUST IN PROTECTING PRIVACY:

The survey found that 62% of Americans are very concerned about protecting their privacy from unscrupulous actors. Only 16% of Americans feel firmly in control of their data, and virtually no one (2-3%) over the age of 55 felt confident in their ability to protect their own data.

The privacy of their personal data is a key determining factor when Americans are choosing whether to use apps or programs. Overall, 54% of Americans said privacy concerns dissuaded them from using an app. This was consistent across all age groups, with, for example, 54% of those over 66 and the same 54% of those 35 and under reporting that privacy concerns induced them to not use an app or program. On the one hand, giving users real choices and control over the privacy of their personal data is essential to building trust. Yet as we can see from this data, concerns about privacy are also preventing a majority of Americans from using some apps or programs. In a Trusted Future in which greater choice and control is the norm, new software must be designed with core privacy safeguards built in from the start to ensure widespread adoption.

Consumers have clear ideas about how to protect privacy. When asked what would make them more confident in their ability to protect their privacy, top responses include:

70% → The ability to delete data collected about you

68% → Ability to opt out of companies tracking your online activities

64% → The right to see the data that companies have collected on you

64% → Requirements that companies can only collect the minimum amount of data on you necessary to deliver their service

58% → Greater transparency about how companies use your personal data online

This combination of very low confidence in privacy protections, and a high level of interest in solutions to protect their privacy is likely the result of a nearly constant stream of events and headlines that involve the use of people's personal data - whether it is events like Cambridge Analytica, or the fact that data breaches have already ballooned in 2021 up more than 17% over 2020 so far, and that people want more information and control over what data is collected, shared and sold about them.[4] Importantly, the survey also highlights some of the meaningful steps that can be taken to help close the trust gap.

- **Right to Delete.**
  70% support the ability to delete data collected about them. This high level interest is likely tied to the lack of transparency and control of personal data held by now $239 billion global data broker industry and built upon the collection, processing, and sale of vast amounts of personal information.[5] When large troves of disparate data are synergized, like that combined through social media activity with advertising data, some now say the holder of the data may know you better than your spouse.6 With public interest so high, it's no wonder "Right to Delete" laws are winding their way through several states.[7]

- **Opt out of Online Tracking.**
  At 68%, people strongly support the ability to stop people from tracking their digital activity. This builds on the findings of a major 2019 survey by the Pew Charitable Trusts that showed an overwhelming majority—nearly 80%—of Americans are concerned about data collected about their online activities and 81% feel like they had no control over the personal data. In the same survey, 7 in 10 think all or most of what they do is tracked online, while 8 in 10 are especially concerned about the amount of personal information collected by social media and advertisers. Giving users choice about whether they want to be tracked across apps and websites by advertisers and allowing them to choose whether data is collected about them are key elements of building trust and returning a sense of control over their personal data.

- **Right to see what's collected.** 64% of people want the ability to know about the data that is being collected about them. Transparency tools are a proven way to improve trust. In addition to states like California that have recently adopted laws to give consumers such access, mobile phone app stores have also now created mandatory "privacy labels" for each app which allows users to learn about the data the app may collect, and whether that data is linked to them or used to track them. Because the labels are in an easy-to-understand form, they can be used to quickly compare the data handling protections between seemingly similar apps, or to identify if the application is collecting extraneous information unrelated to the purpose of the app.[9]

- **Transparency on how companies use your data.** 56% support greater transparency about how companies use their personal data online. People neither have time to read a 20-page terms and conditions, can be expected to understand the complicated legal fine print, nor really have a choice in whether to accept it. Increasingly consumers want easy to understand information about what is collected, why it is being collected, how it will be used, and whether it will be shared or sold.

SIMPLE SECURITY MISTAKES PUT LIVELIHOODS AT RISK:

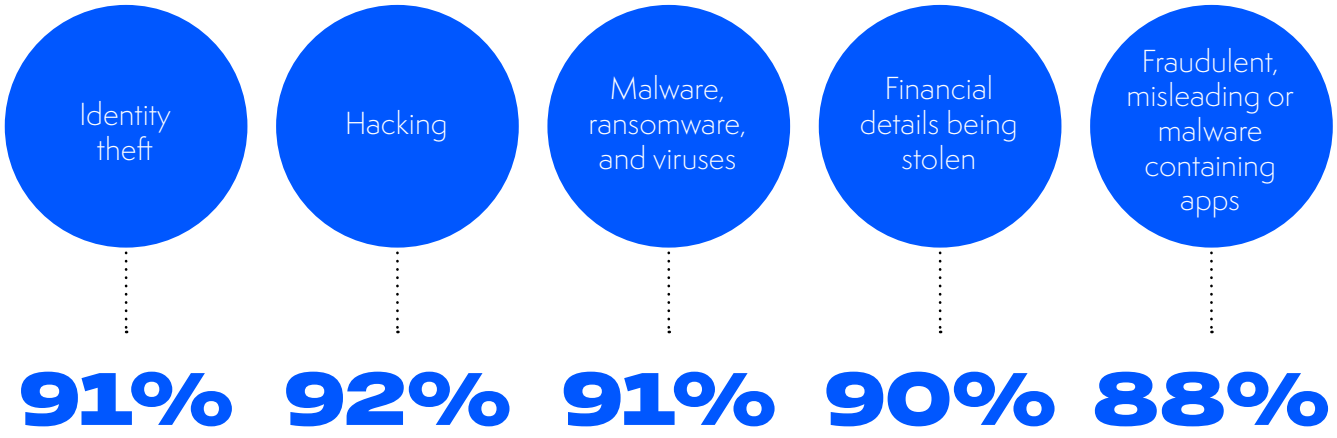
One bad password allowed hackers to disrupt Colonial Pipeline. *The hackers behind the attack on Colonial Pipeline, which led to panic buying at gas stations across the U.S., were able to gain access to the company's systems because one of Colonial's employees reused a password from another account. That other account was compromised and the password was available in a batch of leaked passwords available on the dark web.*[8]

"Package Delivery" Text-Message Scam is actually spyware. *Taking advantage of the surge in online deliveries during the pandemic, hackers sent text messages to millions of mobile phones prompting users to download a package tracking app, which is actually a malicious piece of spyware called the "Flubot" malware in an effort to get sensitive data like online banking details. Because the app was not on the official app store, Android devices were only vulnerable if the user changed the default security settings to allow sideloading.*[10]

LACK OF TRUST IN ABILITY TO PROTECT SECURITY:

The survey found that 58% of respondents lack trust in the security of the technology they use. This shouldn't be a surprise since the beginning of the pandemic, there has been a 300% increase in cybercrime, cyber scams have gone up 400%, mobile malware is on the rise, and there has been a significant hike in the frequency and size of ransomware attacks.[11]

AMERICANS ARE MOST CONCERNED ABOUT:



The survey also found that mobile devices have emerged as a primary gateway to the broader digital ecosystem we connect to with more people owning mobile computing devices than laptops or desktop computers. They have become essential in our daily lives as more than half of our web searches are done on mobile phones, we check our phones on average of 262 times per day, it's often the last thing we check when we go to bed and the first thing we check when we wake up. It's why nearly half of American's say their phone is their most valuable possession.[12]

Incredible technological advances in mobile devices and the apps they enable have made it possible for us to use our mobile devices in incredible ways - allowing us to check bank accounts from anywhere, monitor our health and fitness, engage in intimate private conversations, and control our smart homes. It's no wonder consumers want to keep their mobile device's data private and their devices secure.

These mobile devices are quickly becoming the first line of defense against cyberattacks and malware, and the most important pathway for privacy protections. But as they become more ubiquitous, they have also become essential throughout more parts of our lives, and the need to be able to trust that they can protect our privacy and security has risen commensurately.

The survey found that consumers are eager to protect many different kinds of sensitive data on their phones. When asked, what types of personal information do you keep on your phone that you want to make sure you have the tools to protect, they responded:

79%	Personal photos
77%	Banking transactions
77%	Internet browsing history and app use
77%	Private messages
75%	Location history
70%	Social media accounts
67%	Health data

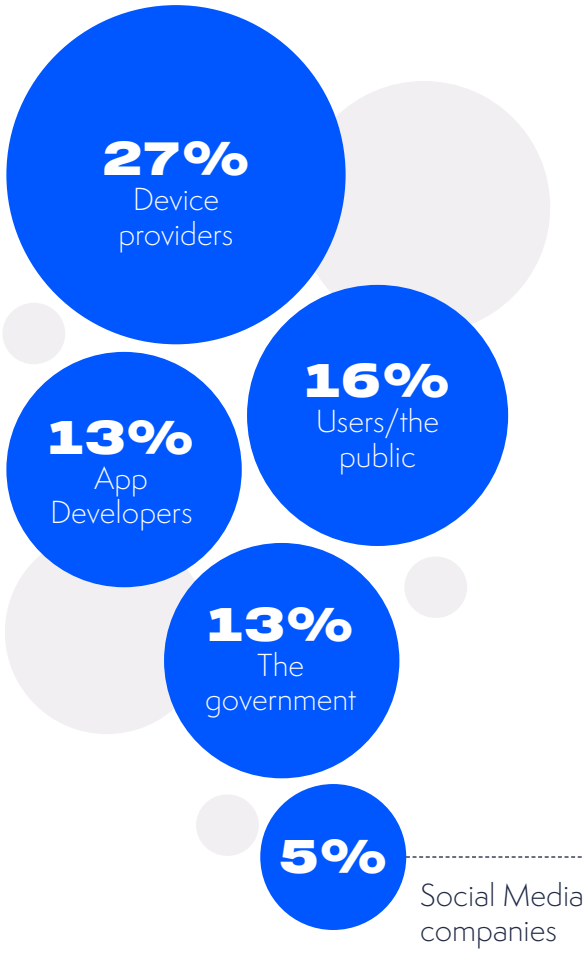
NEARLY

7 in 10

RESPONDENTS FELT COMPANIES SHOULD BE DOING EVEN MORE TO KEEP ALL CATEGORIES OF THEIR DATA PROTECTED.

The survey clearly showed that Americans want tech companies to do even more to protect their personal data online. Whether it was banking transactions, health data, information about their children, or photos, about 8 out of 10 respondents want technology companies to do more to keep that information protected. And virtually no one wants these companies to do less. These numbers were consistent across age, race, and income demographics. The message is crystal clear: Americans want the tech companies to do even more to keep their sensitive personal information protected.

Device developers are the most trusted player today in the app ecosystem. When asked who they trust most to protect and maintain privacy and safety online, respondents indicated:



The survey shows that about half of respondents haven't yet adopted basic cyber hygiene best practices to keep them secure. Because human error, either through outright mistakes or due to social engineering tricks by hackers, leads to 90% of successful attempts to exploit systems, one of the best defenses starts with increasing awareness and adoption of basic cyber hygiene best practices to better protect people from ever-evolving, and increasingly problematic cyber threats - like adopting strong passwords, using multifactor authentication, only downloading from official app stores, and avoiding clicking on untrusted links. To take control of their privacy and security, respondents indicated that they are taking key steps including:

58%	Antivirus software/firewalls
52%	Carefully checking links are legitimate
51%	Regularly updating devices
51%	Not sharing personal information online
50%	Regularly update software
48%	Adopted 2-factor authentication
44%	Only download apps from official app stores
34%	Check default device and service settings for privacy/safety

Vaccinate your technology. Greater adoption of basic cyber hygiene steps, like the FTC's Tips to Protect Your Privacy on Apps could tremendously help protect users privacy and security.[13] When asked if they would prefer the technology they use to be built with robust security standards that can protect them from hackers, malware, and other threats built into the system by design, 50% of users responded positively. That is compared to 28% who prefer the option to install security protections later.

> "HEALTH DATA, PAYMENT DETAILS, AND AN EXACTING HISTORY OF YOUR EVERY STEP SITS NEXT TO CANDY CRUSH AND A FREE CALCULATOR APP YOUR GRANDCHILD INSTALLED ON YOUR PHONE. SAFEGUARDS BUILT INTO YOUR DEVICE AND APP MARKETPLACES HELP PREVENT APPS FROM ACCESSING AND EXPLOITING SENSITIVE DATA, FRAUDULENTLY CHARGING USERS, OR OTHERWISE SCAMMING THEM."[14]
>
> **Former NSA Director Michael Hayden**

COMPARISON TO TRUST FACTORS IN EUROPE

We compare these results with those from the Munich Security Conference's (MSC) European Survey on Digital (Dis)trust from March 2021.[15] The MSC survey similarly shows that Europeans are deeply concerned about their security and that of their personal data online. Interestingly, EU respondents were significantly (by a margin of 18 percent) less trusting of private companies from elsewhere in Europe than of companies in their home country — even though they must abide by the same regulatory rules. Despite the EU's flagship measure on data privacy, the General Data Protection Regulation (GDPR), the implication of this lack of trust among companies from other European countries is that the GDPR has so far been unsuccessful in building confidence among Europeans that their data is protected equally throughout the EU. The survey also reveals a dire state of transatlantic digital trust in public opinion — with respondents' trust in the US government at a low of 13%.

> **"AND THE QUESTION NOW IS WHETHER WE CAN ENGINEER A THIRD WAVE OF THE DIGITAL REVOLUTION—A TURN IN WHICH WE FORGE A DEMOCRATIC TECHNOLOGICAL ECOSYSTEM CHARACTERIZED BY RESILIENCE, INTEGRITY, AND OPENNESS WITH TRUST AND SECURITY, THAT REINFORCES OUR DEMOCRATIC VALUES AND OUR DEMOCRATIC INSTITUTIONS."[16]**
>
> **Former NSA Director Michael Hayden**

At a point where cooperation is needed, the MSC survey finds that there could be a major payoff in terms of building needed transatlantic digital trust, if the EU were able to make tangible progress on consumer security issues such as protecting users from cybercrime, reducing online fraud, and ensuring security of software and hardware products. The MSC survey found that success on issues of user security could establish a baseline of trust that creates opportunity to achieve progress in other fields by demonstrating responsiveness to the Europeans' most pressing concern. Specifically, when compared to other options, the survey found the most support for establishing a cybersecurity framework that the private sector can use to assess and certify the security of different hardware and software products and services. And they found that consumers would be more willing to pay 30% more for hardware with all key components designed with high security standards, versus hardware with all key components designed in the EU.

Here in the U.S., it's becoming clearer that this same kind of globally recognized trust framework could help make big gains in closing our trust gap - and incorporate a broad range of indices for what constitutes a trusted device, software, or service. As nationally acclaimed cyber expert Adam Golodner so aptly put it, "We need a new approach to trust - one that sets out a future-focused Trust Framework laying out key indicia of security and privacy and allows a technology producer or service provider to understand the holistic criteria they could meet that would enable someone to trust their product or service - and if they'd like, state or certify that they exhibit indicia of trust."[17]

What follows is a deeper analysis of the core drivers of trust and distrust, the benefits we can achieve when we can foster greater trust, and a potential path for advancing a more trusted future.

01.

TRUSTED SECURITY

We need the ability to trust that the technologies we use are secure by design.

Our global digital ecosystem is under near-constant threat from malicious actors using techniques that are becoming increasingly more complex, sophisticated and ubiquitous.

One study for the insurer Munich Re found that more than half of U.S. businesses reported at least one cyber attack over the previous year and other surveys have shown similar or worse attack numbers for users.[18]

Criminal gangs, hackers with a business plan, and even nation-states are working around the clock and across the globe to find and exploit vulnerabilities. One of their most effective tools is the development of sophisticated new "social engineering" strategies to trick users into clicking on malevolent links, infected attachments, or downloading mobile malware directly onto devices. Even a small mistake can be leveraged to put your most personal information at risk, put proprietary business information at risk expose national security secrets, or even lock down a pipeline, school, or hospital for ransom. We have to find the right path forward to reduce this risk.

As information technology becomes more pervasive, devices more prolific, and the information we carry with us becomes more sensitive, the attack surface that hackers can attempt to exploit has increased substantially creating new kinds of potential harm. It means that as technology becomes increasingly central to our lives, making it secure and reliable from the start becomes ever more critical.

> "WE NEED TO TRANSITION TO WHERE TECHNOLOGY IS BUILT SECURELY BY DEFAULT. WE'VE BAKED IN BY DESIGN. YOU KNOW, WE DON'T BUY A CAR AND THEN BUY THE AIRBAG SEPARATELY. AND IT'S — YOU KNOW, WITH TECH, WE NEED TO KNOW WE'RE BUYING SECURE TECH."[19]
>
> White House Briefing, August 24, 2021

Just like a home must be built upon a strong

foundation or it will eventually crumble, our new digital home must also be built upon a strong foundation of security - with security built into its very foundation by design. To elevate our cybersecurity posture, we need to elevate our focus on agile solutions across the ecosystem that embrace good best practices, enable continuous innovation in cyber-defenses, advance globally recognized frameworks, underpinned by smart government policies to keep personal and business data secure and our economy moving forward.

> "THE OPERATION OF CRITICAL NETWORKS AND INFORMATION INFRASTRUCTURES DEPENDS ON THE ASSURED AVAILABILITY OF TRUSTWORTHY HARDWARE AND SOFTWARE."[20]
>
> International Strategy for Cyberspace

02.

TRUSTED PRIVACY

We need the ability to trust that our privacy is protected.

Over the past several years the amount of digital data we generate has exploded at near exponential rates. We now collectively generate about 2.5 quintillion bytes of data each day, send 65 billion messages, and now access our phones more than 200 times per day - sometimes communicating, banking, dating, searching, or doing other things we may want to keep private.[21] As a result, there is more sensitive and private information being generated throughout more parts of our lives.

While people want control of their data, too often they don't feel like they have control. The survey we conducted showed 89% of respondents were concerned about their data being shared with third parties and just 16% felt like they were in control of their data. This result is consistent with other surveys, and this broad public concern about the loss of control of their data has led to a great privacy awakening and expanded interest in a more trusted digital ecosystem where privacy protection can be a basic digital right, where clear boundaries exist around what is collected, processed, tracked, and shared, and where users have the tools they need to control their own data.

When so many consumers are worried about their data being shared and so few feel in control of their data, we should all understand that building a trusted future will require new strategies that empower people with the tools they need to regain a sense of control over their personal data, and the ability to prevent tracking across the Internet. When people feel protected from misuse of their personal information, they are more likely to engage in commerce, to participate in the political process, to seek needed health care, and take advantage of tools that can improve their lives.

To build a more trusted future, we also need 21st century consumer safeguards that can protect all of us from malicious, fraudulent, and unethical actors that seek to deceive, harm, or exploit our trust. as parents seek to harness new technologies to improve the way their children learn, communicate and play, they also want to know that they can trust that their children's privacy will be protected, and that they won't inadvertently be tricked into downloading something inappropriate, harmful, or malicious. Already, more than 9 in 10 parents and teens support clear labels about data collection and are concerned about data used to target ads to children across apps, sites, and devices.[22] To build a more trusted future, businesses, consumers and parents need to have faith that the technologies they use are dependable, ethically designed, and will help protect them from flawed, deceitful, fraudulent, manipulative or unsafe applications, websites and services.

03.

TRUSTED CHILD SAFETY

Keeping kids safe online is no easy task.

During the pandemic we've seen how important digital devices can be for kids as their tablet became a gateway to their classroom, enabling them to swipe their hand across the screen to access the whole universe of knowledge the Internet contains. But parents also often want to know that they can trust that their children's privacy will be protected, that they won't be targeted or tracked across websites, and that they won't inadvertently be tricked into downloading something inappropriate, harmful, or malicious.

According to one survey, 76% of parents are worried about the safety of their children online.[23] Parents often need to lean heavily on a combination of having informed conversations with their kids about how to avoid potential online risks, and the safeguards that some technologies provide. Some companies have built child protections mechanisms into their devices, their software or their websites. And while more than two-thirds (67%) of parents surveyed by Sophos worry about cyberattacks impacting their children, it's also that case that protective measures are falling short.[24] We've seen how some bad actors try to get around key protections by specifically targeting kids with games that may trick them into in-game purchases, creating apps that undermine teen's well-being, inappropriately targeting and tracking kids through online ads, sending suspicious links that try and trick them into downloading malware, or engaging in improper online communications that try to trick them into giving away private information or even worse. In some cases, apps have been shown to even hurt sleep, work, relationships or parenting for large number of users.[25] But when companies mislead, put profit-making ahead of advancing a trusted digital ecosystem, or specifically try to extort, scam, or defraud users, every other player in the digital ecosystem needs to be thinking about the unique role they can play in elevating accountability for a more trusted digital ecosystem, while policymakers likewise need to enable innovative and trusted efforts to hold bad actors accountable.

Parents aren't just concerned about keeping kids safe at home, their schools are increasingly being targeted with ransomware. According to government data, ransomware attacks on schools doubled to reach 57% of all ransomware incidents this past fall, up from 28% over the prior spring and summer.[26] How are the schools getting infected and exploited? It often starts with "social engineering" methods targeted at students, parents or school personnel that tries to trick victims into clicking on a link, revealing private information or installing software containing malware. Government agencies cite 10 malware variants as the top strains, social engineering as a primary vector, and recommend a series of best practices to avoid being compromised.

04.

EQUITY AND INCLUSION

We need the ability to trust that our future is more equitable and inclusive.

Technological innovation holds the potential to bring more broadly shared opportunity, economic freedoms, and personal freedom. While technology can be a powerful opportunity equalizer, for too long barriers have meant that some of the people who can benefit most are too often the people who have been left behind. As we made the Internet essential for all, we only made it trustworthy for some. To make progress, we need to start by rebuilding trust among historically disadvantaged communities, make sure technologies are more inclusive by design, and ensure that new products and services are designed by, and for, a more diverse group of people.

AS WE MADE THE INTERNET ESSENTIAL FOR ALL, WE ONLY MADE IT TRUSTWORTHY FOR SOME.

Broadening inclusion starts with addressing privacy, security, and safety inequities, to improve trustworthiness for all. Among the many dimensions of digital inequality is the unequal distribution of user privacy, security and safety risks. A number of key studies have found vulnerable populations are often uniquely vulnerable to various privacy harms, security vulnerabilities, and online scams. They are less likely to feel in control of their privacy, they are more prone to attacks, and when they are victims to hacks, they are often disproportionately harmed, and lack the confidence in being able to overcome these risks. As a researcher at the Data & Society Research Institute put it, "when someone who is living paycheck to paycheck falls victim to an online fraud or loses the ability to use his or her smartphone after it gets hacked, the cascade of repercussions can be devastating."[27]

- **Low-income Americans are more concerned than their wealthier counterparts about losing control over how their information is collected or used.** They are also more worried about being harassed online or having their financial information stolen.[28]

- **Women, minorities, and the elderly are the most vulnerable to online attacks.** A survey by Malwarebytes found, for example, women whose social media accounts get hacked are more likely than men to have that hack result in someone sending suspicious messages to friends and family (48 percent compared to 43 percent). They also found Black people, Indigenous people, and People of Color (BIPOC) are more likely to have their identities stolen than White people (21 percent compared to 15 percent), and BIPOC people

are the least likely to avoid any financial impact due to cybercrime (47 percent compared to 59 percent of all respondents).[29]

- **A larger portion of Black, Hispanic, Asian, and other racial minorities are likely to suffer larger financial losses when targeted by scammers,** according to Researchers from the University of Minnesota and the University of Southern California.[30]

- **Identity theft poses a much heavier burden for people living on the margins,** one comprehensive survey found.[31]

Broadening inclusion requires making it trusted and safe for all. Too often, distrust has been driven by a growing sense of inequity and unfairness in the system - or further amplified by people who use technology to prey on vulnerable communities. To build trust, we need to more directly target fraud, malware, and malicious behavior targeted at the economically disadvantaged and people of color. We need pragmatic policies and the ability to elevate responsible players in the digital ecosystem who have the ability to advance baseline privacy protections, who can build in security by design, who can help ferret out malicious or unsafe activities, and who can help level the playing field so that every person - regardless of who they are or where they live - are able to take full advantage of the same digital opportunities. Because everybody, regardless of income, geography, gender, disability, or background needs the same opportunity to be connected and participate in today's digital economy.

Broadening inclusion requires a focus on overcoming hesitancy, and enabling onramp technologies like smartphones. When the Pew Foundation looked at the hesitancy behind those who don't yet use the Internet or digital technologies, it found they are more likely to be older, low-income, women, and minorities, and that one of the chief inhibitors was a lack of trust.32 Pew has also found that Blacks and Hispanics are more likely to be "smartphone-dependent" - meaning they are disproportionately more reliant on mobile devices as their primary source of digital access, and thus also more likely than whites to rely on their smartphones for a number of activities, such as seeking health information or looking for work.33 It suggests that mobile devices are on the front lines of protecting privacy and security, and efforts to address inequities must also address the needs of robust security and privacy on mobile devices in order to protect every user.

Boosting equity requires opening up good paying jobs to more diverse people in more diverse communities. To make our digital world more inclusive, we also need to tackle structural barriers and advance strategies that expand access to the skills needed to access the good paying jobs that the technology sector often creates, ensure technologies are designed and developed by a more diverse workforce, and improve access to capital to empower the entrepreneurs who have been left out and left behind.

It means forging a new path toward an inclusive economy, one that supports a thriving tech and innovation ecosystem in a way that creates equitable opportunities for all. However today, the benefits of technology innovation are not realized equitably across regions. 90 percent of growth in high-tech jobs happened in just 5 metro areas and one-third of the nation's innovation jobs reside in just 16 counties.34 These geographic differences have undercut economic inclusion and have contributed to national economic inequalities.

Fortunately, policymakers are beginning to respond by driving geographically diverse innovation hubs throughout the country - where applicants have to demonstrate that they have "an equity lens."[35] Policymakers are also advancing critical efforts to ensure that minority serving

A MORE TRUSTED FUTURE IS A MORE EQUITABLE AND INCLUSIVE FUTURE

institutions like Historically Black Colleges and Universities can become global innovation hubs and can build the next generation of STEM leaders. We also need to ensure that black, brown and other underrepresented entrepreneurs have access to capital, including through venture capital, to grow thriving, dynamic, and innovative new startups.

These more inclusive steps can have profound benefits for companies and the economy too.

Research shows that more diverse teams are more innovative and generate more revenue.[36] One study found that innovation would quadruple if women, people of color, and children from low-income families were able to invent at the same rate as other groups who are not held back by discrimination and structural barriers.[37] That's why a more trusted future is a is more equitable and inclusive future.

05.

BOOSTING INNOVATION AND EXPANDING OPPORTUNITY

We need the ability to trust that the technologies of tomorrow will be even better than today.

Despite enormous advances, we've only seen a fraction of what the digital revolution has yet to deliver. Already the Internet has brought untold advances that have fundamentally changed the way we work, learn, and live. And just over the horizon amazing new advances in 5G and 6G, artificial intelligence, mobile devices, wearable technology, cloud computing, quantum computing, and Internet-connected devices are converging and have put us on the cusp of a new technological transformation with the potential to impact each of our lives in positive and profound ways. But lack of trust is emerging as one of the most critical gating factors with the potential to dramatically affect the speed at which future technologies are adopted, and corresponding benefits achieved.

WHILE TRUSTED TECHNOLOGICAL INNOVATION CAN'T SOLVE ALL OF OUR PROBLEMS, NEITHER CAN WE SOLVE ALL OF OUR PROBLEMS WITHOUT IT.

THE ENORMOUS OPPORTUNITIES AT STAKE REQUIRE A MORE TRUSTED FUTURE:

As Chris Inglis, the nation's first national cyber director recently put it: *"National cyber policy must be driven not only by the crimes and disruptions it seeks to prevent, but by the goals it seeks to achieve … Imagine what we could accomplish if cyberspace were stable and reliably secure, if data could be stored and transmitted with confidence in its privacy and integrity, and if cyberattacks were quickly defeated and seamlessly remedied."*[38]

There is so much that can be achieved when we can fully trust the technologies we use. Experts say new innovations just emerging over the horizon have the potential to dramatically improve health outcomes for millions, radically improve energy efficiency to help meet climate goals, revolutionize education, and help millions attain personal financial security. And when done in trusted ways, these opportunities can also reach across economic and social divides and help individuals and communities that have been neglected, oppressed, or discriminated against leap forward into a more equitable, prosperous, and healthy future.

It means that in a trusted future, the next life-changing breakthrough are not simply connecting

new kinds of devices to the internet, but rather connecting people to new kinds of opportunity.

As the digital ecosystem has now become a vital enabler for almost every sector of the economy, trust now stands at the gateway holding the key for unlocking vast future opportunities. Building a foundational layer of trust into our technological future is not only a prerequisite for unlocking our ability to harness innovation for a more equitably economy, but it's also essential for solving some of our most important societal challenges. And while trusted technological innovation can't solve all of our problems, neither can we solve all of our problems without it.

- ***Enabling Smarter Better More Inclusive Ways to Improve America's Crumbling Infrastructure.*** Our outdated analog era infrastructure has enabled widespread congestion, unsafe bridges, air traffic delays, lack of safe drinking water, and regular power outages. Experts predict that smarter digital infrastructure can improve traffic flow by as much as 25%, save as much as 200 billion kWh of electricity, and reduce air traffic delays by as much as 35%.[39] For example with privacy and security baked in from the start, connected stop lights and vehicle-to-infrastructure communication can speed traffic flow, connected bridges can monitor their own safety, train control systems can help avoid crashes, connected water systems can detect leaks, a connected grid can boost energy efficiency, and a connected community can increase digital equity. They can not only enable a more holistic approach to managing, monitoring, and maintaining infrastructure, but we can unlock opportunities to do things in better ways never before possible. Despite massive investments, nearly one-third of smart city projects fail.[40] As CISA points out, these projects can inadvertently lead to security, safety, privacy, and infrastructure risks for communities, either by creating such issues themselves, or by providing attack vectors that allow malicious use of the services and components.[41] In addition, when privacy is not built-in by design, communities that collect data with passive sensors, such as cameras, risk losing community trust which can slow or halt smart city gains. And when trust or inclusion aren't baked in from the start they too often fail. For example, Toronto's much-heralded Quaysides smart city project failed after it couldn't address core privacy and inclusivity issues raised by the community.[42] By contrast Portland's Smart City PDX put privacy principles and equity priorities at the forefront of its efforts - underscoring why smart city efforts need to be built with trust from the start, and in conjunction with the communities it intends to help, not for, in order to succeed.[43]

- **Helping manufacturers imagine the un-imaginable, make the un-makeable, and create the unbelievable.** Emerging manufacturing technologies allow manufacturers to use software to design smarter and use digital designs to control a new class of connected machines like 3D printers, laser cutters, CNC machines, and multi-axis robots that use software to make things with digital precision. New factory technologies can better protect workers, improve factory floor efficiency, and enable new connected smarts to build directly into the product itself. These technologies can cut development time by 50% enable a 10 times improvement in time to market, boost factory productivity by as much as 25%, boost energy efficiency by 25%, reduce safety incidents by 40%, and enable entirely new designs, products, and business models.[44] But companies are unlikely to make this digital transformation at a time when ransomware has the ability to shut down production lines, and as ransomware attacks in manufacturing are on the rise - tripling in 2020.[45] Already, 36% of

manufacturing and production organizations were hit by ransomware in 2020, the average ransomware recovery cost was $1.52 million, and 25% expect to be hit in the future, according to a survey by Sophos.[46]

- **Transforming digital innovation into climate action.** At a time when global leaders are looking for innovative approaches for reducing greenhouse emissions and tackling climate change, new connected technologies, when deployed pragmatically and pervasively, can help us reduce overall net electricity demand by more than 25%, cut greenhouse gas emissions by 19%, save billions on our energy bills, help make us more energy independent, and enable a smarter electric grid that is more efficient, reliable, and resilient.[47] But as the International Energy Agency recommends, two of the keys to enabling positive digital energy transformation is 1) "Security by Design" - "the incorporation of security objectives and standards as a core part of the technology research and design process," and 2) privacy protections because "aggregated and anonymized individual energy use data can improve understanding of energy systems, such as load profiles, and help lower costs for individual consumers."[48]

- **Helping people live longer healthier lives.** Smart watch and phone sensors are saving lives.[49] These devices are demonstrating they can detect diabetes with 85% accuracy rate, sleep apneas with 90% accuracy, hypertension with 82% accuracy, and abnormal heart rhythms with 97% accuracy.[50] McKinsey estimates that connected digital devices could help cut the costs of chronic disease treatment by as much as 50 percent.[51] Goldman Sachs estimates that the digital health revolution could reduce health costs by a whopping $300 billion by increasing access to diagnostic treatments, preventative care, and chronic disease.[52] During the pandemic, some telemedicine platforms saw as much as a 2,000% increase in visits.[53] But according to Accenture's Digital Health survey the top ranked concern about using digital health tools (38%) was privacy and data security followed by a lack of trust in the technology.[54] Without addressing these underlying trust issues, use of these potentially lifesaving tools could be diminished or delayed.

- **Growing agricultural opportunities for more delicious and nutritious foods to feed the world.** To feed the world by 2050, farmers will need to produce 70% more food, using basically the same amount of land. Experts believe farmers can take advantage of a new generation of precision farming technologies that experts project will help boost global crop yields as much as 67 percent.[55] If precision farming technologies are pervasively deployed, experts predict they can cut water use by up to 30%, reduce herbicide use by 99.99%, reduce fuel use by 10%, and cut food prices in half.[56] But lack of trust could stall these important gains. A DHS/USDA sponsored analysis has identified, privacy and security as top concerns of farmers considering implementing precision agriculture techniques because private data can be exploited for traumatic financial and emotional impacts, security exploits can risk equipment availability, and ransomware can damage crops and herds.[57] Given that 9 out of 10 farmers already use a smartphone in their combine and about one in 3 use a tablet, often to use decision support systems to control their assets, it's no wonder that the DHS analysis warns that third-party applications are "haphazard at best."[58] They identified these third-party downloaded apps as the most likely threat because there are some mobile device decision support system "apps which could be malicious by design to steal data." They therefore recommend baseline security controls necessary to mitigate these threats.

These issues are very real. The FBI recently reported that attacks on the agriculture industry are increasing, with at least eight major attacks on agricultural companies in 2021 alone including the international meatpacking company JBS.[59] In one case, an Iowa grain co-op was targeted by a Russian cybercrime operator demanding a $5.9 million ransom and nearly crashing the grain market.[60] Since mobile devices are often a key vector in agriculture attacks, ensuring their security is of critical importance.[61]

- **Saving fuel, saving lives, and saving the planet with more efficient transportation technologies.** Recent and continuing advances in transportation technologies and current research on and testing of exciting vehicle innovations have created completely new possibilities for improving highway safety, increasing environmental benefits, expanding mobility, and creating new economic opportunities for jobs and investment. While an estimated 35,000 people get killed on the road every year, and 94 percent of serious crashes are due to human error or choices, a new generation of intelligent and autonomous vehicles that enable anyone to ride with a driver that never gets drunk, tired, or distracted could reduce traffic accidents by as much as 90%.[62] Autonomous vehicles not only promise to make transportation safer, but they also can make it cleaner, more accessible, and more efficient. But studies show that distrust is a potential obstacle to consumer acceptance of autonomous vehicles and cybersecurity attacks emerged as the top concern for 63 percent of automotive and technology executives in developing technology for connected cars and autonomous vehicles.[63] If we aren't focused on building trusted technologies that are secure and protect our privacy, we can't advance the technologies necessary to save these lives.

A TRUSTED FUTURE EMPOWERS EACH OF US

It is about giving a factory worker the smarter tools they need to better compete with workers around the globe without fear of the factory being shut down by ransomware.

It's about a recent graduate taking a job as an innovator when she can trust that the pathway to a more prosperous future is also paved for people with disabilities like her.

It's about enabling a farmer trying to produce more with less knowing he can trust his precision farming investment can't be shut down by malware.

Even though nothing is more sensitive that an individual's medical records, this is about enabling an elderly patient to connect with their doctor for more personalized home-monitored care without fear that her privacy will be undermined.

It's about enabling every student - regardless of geography or income - to take full advantage of digital learning so they are prepared to compete and win the new jobs of the future without fear that their digital records will be exploited.

It's about empowering a parent with the tools she needs to allow her children to access the whole universe of online knowledge while resting assured that that they are protected from malware and bad actors that might do them harm.

And it's about enabling a scrappy inventor from an economic disenfranchised community to become the next new thing in the global marketplace by trusting that her bright new invention won't be stolen by hackers.

- **Expanding jobs and accelerating economic opportunity for everyone.** By one estimate with the right policies, extending our digital transformation to our physical economy could boost annual economic growth over the next 15 years - adding $2.7 trillion to annual U.S. economic output by 2031, boosting wages and salary payments to workers by a cumulative $8.6 trillion over the next 15 years, and boosting federal revenues by a cumulative $3.9 trillion.[64] Mobile devices alone will have some of the biggest impacts. According to Accenture's latest economic modeling analysis, our mobile 5G future will drive up to $2.7 trillion in additional gross output growth between 2021 and 2025, could add $1.5 trillion to U.S. GDP, help create 16 million jobs, and enable people to do things never before possible.[65] But a lack of trust could slow the rollout of this next mobile revolution as 60% of those surveyed expressed fears that 5G could make more personal data vulnerable to hacking.[66]

Only when we bake trust into our digital future by design can we fully achieve the promise and potential of what it can deliver. If systems are not designed to utilize trusted technologies, or if policymakers fail to incorporate privacy, security, and equity issues into their policymaking process - they could inadvertently slow the critical gains we need to solve some of our most pressing challenges.

CONCLUSION

In order to ensure that innovation keeps fueling positive change that is more equitably shared, it is critical that our digital ecosystem is built upon a foundation of trust that is focused on protecting privacy, security, deterring and defeating attacks, and establishing a safe and secure ecosystem.

To close our trust gap, we need to enable end-to-end inclusion, privacy, and security - across software, devices, networks, and the cloud - and throughout our policy processes. Because technology is near-ubiquitous throughout our economy and throughout our lives, we can't pigeonhole or silo the way we look at policy. While we can help consumers adopt the basic cyber hygiene best practices to help improve their security, we need to advance a framework of trust by design - that can help improve privacy, security, inclusion, opportunity - with the specific steps that consumers, developers, and policymakers can take to help advance a more trusted future.

As former NSA Director Michael Hayden puts it:

> IN THE POLICY ENVIRONMENT WE NEED TO ASK KEY QUESTIONS ABOUT "HOW WILL THESE REGULATIONS IMPACT THE SECURITY OF END USERS? WILL THESE NEW RULES CREATE FURTHER OPPORTUNITIES FOR MALWARE AND FRAUD? HOW DO YOU WEIGH THE SECURITY IMPACTS OF NEW POLICIES WITH POTENTIAL COMPETITION GAINS?"[67]

ABOUT TRUSTED FUTURE

Trusted Future is coming together around a shared belief that we need smarter, better-informed efforts to help tackle today's challenges and enhance trust in today's digital ecosystem in order to expand opportunities for tomorrow. We believe we deserve a vibrant digital ecosystem that is responsible, inclusive, safe, transparent, and accountable -- one where you can trust that your privacy will be protected, that your data will be secured, your safety can be protected, that leads to a more just, equitable and inclusive society, and that fosters previously unthinkable opportunities to improve your life.

We bring together experts, advance new research, highlight common sense policies and recommendations, and explore new ways to foster and enhance the basic trust we need to support and sustain a healthier digital ecosystem in the United States and globally. This trust framework will help consumers and enterprises decide whether products and services are trustworthy and help technology producers adopt practices that exhibit indicia of trust that would encourage users to trust them. Central to this trust framework is our vision of an integrated innovation landscape in which new technological and policy advancements complement each other, elevate our trust in the digital ecosystem, and avoid unintended consequences that could undermine it. Raising the level of trust in the global digital ecosystem is no easy task. But with a more comprehensive approach combined with information, education, awareness, and engagement, we hope to outline a pathway toward a more Trusted Future.

ENDNOTES

1. President Joseph R. Biden, Jr., Executive Order on Improving the Nation's Cybersecurity, The White House, May 12, 2021 (last accessed Nov. 23, 2021); available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
2. *Edelman Trust Barometer: Trust in Technology*, Edelman, 2021 (last accessed Nov. 23, 2021); available at: https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer%20Tech%20Sector%20Report_0.pdf.
3. The U.S. Trust Landscape, Trusted Future; available at: https://trustedfuture.org/the-u-s-trust-landscape/
4. Chris Morris, "The Number of Data Breaches in 2021 has Already Surpassed Last Year's Total," Fortune, October 6, 2021 (last accessed Nov. 23, 2021); available at: https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks/.
5. *Global Data Broker Market Size*, Knowledge Sourcing Intelligence, June 2021 (last accessed Nov. 23, 2021); available at: https://www.knowledge-sourcing.com/report/global-data-broker-market.
6. Frank Leurweg, "The Internet Knows You Better Than Your Spouse Does," *Scientific American*, March 14, 2019 (last accessed Nov. 23, 2021); available at: https://www.scientificamerican.com/article/the-internet-knows-you-better-than-your-spouse-does/.
7. Glenn A. Brown, "Consumer 'Right to Delete' Laws Under U.S. State Laws," Consumer Privacy World (blog), Squire Patton Boggs, March 3, 2021 (last accessed Nov. 23, 2021); available at: https://www.consumerprivacyworld.com/2021/03/consumers-right-to-delete-under-us-state-privacy-laws/.
8. Stephanie Kelly and Jessica Resnick-ault, "One Bad Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators," Reuters, June 2021 (last accessed Nov. 23, 2021); available at: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.
9. Chris Smith, *Visualized: The Terrifying Amount of Data Facebook Messenger Collects Compared to Signal, iMessage, and What'sApp,* Boy Genius Report (blog), January 5, 2021 (last accessed Nov. 23, 2021); available at: https://bgr.com/tech/app-privacy-labels-facebook-messenger-vs-imessge-signal-whatsapp/.
10. "FluBot: Warning Over Major Android 'Package Delivery' Scam," BBC News, April 23, 2021 (last accessed Nov. 23, 2021); available at: https://www.bbc.com/news/technology-56859091.
11. *For increase in cybercrime*, Jenna Walter, "Covid-19 News: FBI Reports 300% Increase in Cybercrimes," IMC Grupo (blog); May 2, 2020 (last accessed Nov. 23, 2021); available at: https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/; *For cyber scams*, Christo Petrov, "25+ Impressive Big Data Statistics for 2021," techjury (blog), November 1, 2021 (last accessed Nov. 23, 2021); available at: https://techjury.net/blog/big-data-statistics/#gref; *For mobile malware*, Charles Q. Choi, "Gaming-Related Malware on the Rise on Mobile, PCs," IEEE Spectrum (blog), October 21, 2021 (last accessed Nov. 23); available at: https://spectrum.ieee.org/mobile-malware-increasing#toggle-gdpr; *For ransomware*, Doina Chiacu, "White House Warns Companies to Step Up Security, 'We Can't Do It Alone,'" Reuters, June 3, 2021 (last accessed Nov. 23, 2021); available at: https://www.reuters.com/technology/white-house-warns-companies-step-up-cybersecurity-2021-06-03/.
12. *For mobile searches*, Nick Statt, "More than Half of All Google Searches Now Happen on Mobile Devices," The Verge (blog), October 8, 2015 (last accessed Nov. 23, 2021); available at: https://www.theverge.com/2015/10/8/9480779/google-search-mobile-vs-desktop-2015; *For checking phones and phone most valuable possession*, Trevor Wheelwright, "Cellphone Behavior in 2021: How Obsessed Are We?," Reviews (blog), April 21, 2021 (last accessed Nov. 23, 2021); available at: https://www.reviews.org/mobile/cell-phone-addiction/.
13. Federal Trade Commission, "How to Protect Your Privacy on Apps," May 2021 (last accessed Nov. 23, 2021); available at: https://www.consumer.ftc.gov/articles/how-protect-your-privacy-apps.
14. Michael Hayden, "Changing How App Stores Operate Could Have National Security Implications," Nextgov (blog), July 16, 2021 (last accessed Nov. 23, 2021); available at: https://www.nextgov.com/ideas/2021/07/changing-how-app-stores-operate-could-have-national-security-implications/183839/.
15. Simon Pfieffer and Randolf Carr, Error 404: Trust Not Found, Munich Security Conference, March 2021 (last accessed Nov. 23, 2021); available at: https://securityconference.org/assets/02_Dokumente/01_Publikationen/MunichSecurityBrief_Error404_TrustNotFound.pdf.
16. "Remarks of National Security Adviser Jake Sullivan at the National Security Commission Artificial Intelligence Global Emerging Technology Summit," The White House, July 13, 2021 (last accessed Nov. 23, 2021); available at: https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit/.

17. Adam Golodner, "We Need a Cyber Trusted Future and a New Trust Framewok," Morning Consult (blog), September 17, 2021 (last accessed Nov. 23, 2021); available at: https://morningconsult.com/opinions/we-need-a-cyber-trusted-future-and-a-new-trust-framework/.

18. *For Munich Re survey*, "Survey Cites More than Half of U.S. Businesses Have Experienced a Cyber Attack," Moran Insurance, 2017 (last accessed December 16, 2021); available at: https://moraninsurance.com/newsletter/survey-cites-half-u-s-businesses-experienced-cyber-attack/; *For survey of users*, "ESET Cybersecurity Survey Amongst Internet Users in APAC Reveals Large Gap Between Threat Awareness and Taking Action," Yahoo.com, November 21, 2021 (last accessed on December 16, 2021); available at: https://www.yahoo.com/now/eset-cybersecurity-survey-amongst-internet-020000704.html.

19. "Background Press Call By Senior Administration Officials On the President's Upcoming Cybersecurity Meeting," The White House, August 24, 2021 (last accessed Nov. 23, 2021); available at: https://www.whitehouse.gov/briefing-room/press-briefings/2021/08/25/background-press-call-by-senior-administration-officials-on-the-presidents-upcoming-cybersecurity-meeting/.

20. President Barack Obama, "International Strategy for Cyberspace," The White House, May 2011 (last accessed Nov. 23, 2021); available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

21. Petrov, "25+."

22. Michael B. Robb, Privacy Matters: Protecting Digital Privacy for Parents and Kids, Common Sense Media, 2019 (last accessed Nov. 23, 2021); available at: https://www.commonsensemedia.org/sites/default/files/uploads/kids_action/csm_privacymatters_protecting_digital_privacy.pdf.

23. People Staff, "Distance Learning has 76% of Parents Worried About their Child's Safety, New Survey Finds," People, September 25, 2020 (last accessed Nov. 23, 2021); available at: https://people.com/human-interest/distance-learning-parents-worried-childs-safety-survey/.

24. "How Has Covid-19 Changed Children's Online Security," Sophos (blog), March 23, 2021 (last accessed Nov. 23, 2021); available at: https://home.sophos.com/en-us/security-news/2021/parents-cybersecurity-survey.

25. Georgia Wells, Deepa Seetharaman, and Jeff Horowitz, "Is Facebook Bad for You?, It Is for About 360 Million Users, Company Surveys Suggest," *The Wall Street Journal*, November 5, 2021 (last accessed Nov. 23, 2021); available at: https://www.wsj.com/articles/facebook-bad-for-you-360-million-users-say-yes-company-documents-facebook-files-11636124681.

26. "Joint Cybersecurity Advisory: Cyber Actors Target K-12 Distance Learning to Cause Disruptions and Steal Data," The Federal Bureau of Investigation, the Cybersecurity and Information Security Agency, and the Multi-State Information Sharing Analysis Center, December 10, 2020 (last accessed Nov. 23, 2021); available at: https://us-cert.cisa.gov/sites/default/files/publications/AA20-345A_Joint_Cybersecurity_Advisory_Distance_Learning_S508C.pdf.

27. Mary Madden, "The Devastating Consequences of Being Poor in the Digital Age," The New York Times, April 25, 2019 (last accessed Nov. 23, 2021); available at: https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

28. Mary Madden, Privacy, Security, & Digital Inequality, Data & Society Research Institute, September 27, 2017 (last accessed Nov. 23, 2021); available at: https://datasociety.net/wp-content/uploads/2017/09/DataAndSociety_PrivacySecurityandDigitalInequality.pdf.

29. Demographics of Cyber Crime Report, Malwarebytes, 2021 (last accessed Nov. 23, 2021); available at: https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html.

30. Scam Tracker Risk Report 2020: Online Scams Rise During Covid-19 Pandemic, Institute for Marketplace Trust, The Better Business Bureau, 2020 (last accessed Nov. 23, 2021); available at: https://bbb.org/bbbscamtrackerriskreport/.

31. 31. Sarah Dranoff, "Identity Theft: A Low Income Issue," Dialogue (blog), American Bar Association, December 15, 2014 (last accessed Nov. 23, 2021); available at: https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/.

32. John B. Horrigan, "Digital Readiness Gap," Pew Research Center, September 20, 2016 (last accessed Nov. 23, 2021); available at: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2016/09/PI_2016.09.20_Digital-Readiness-Gaps_FINAL.pdf.

33. Monica Anderson, "Racial and Ethnic Differences in How People Use Mobile Technology," Pew Research Center, April 30, 2015 (last accessed Nov. 23, 2021); available at: https://www.pewresearch.org/fact-tank/2015/04/30/racial-and-ethnic-differences-in-how-people-use-mobile-technology/.

34. Rani Molla, "90 Percent of Growth in High Tech Jobs Happened In Just 5 Metro Areas," Recode (blog), Vox, December 9, 2019 (last accessed Nov. 23, 2021); available at: https://www.vox.com/recode/2019/12/9/21000162/high-tech-job-growth-concentration-brookings.

35. Adria Schwarber, "Commerce Department Dedicating $1 Billion to Spur 'Regional Industry Clusters," FYI (blog), American Institute of Physics, August 5, 2021 (last accessed Nov. 23, 2021); available at: https://www.aip.org/fyi/2021/commerce-department-dedicating-1-billion-spur-%E2%80%98regional-industry-clusters%E2%80%99.

36. Jack Myers, "The Numbers Don't Lie: Diverse Workforces Make Businesses More Money," Outside the Box, MarketWatch, August 1, 2020 (last accessed Nov. 23, 2021); available at: https://www.marketwatch.com/story/the-numbers-dont-lie-diverse-workforces-make-companies-more-money-2020-07-30.

37. Alex Bell, Raj Chetty, Xavier Jaravel, Neviana Petkova, and John Van Reenen, Who Becomes An Inventor in America? The Importance of

Exposure to Innovation, Opportunity Insights, November 2018 (last accessed Nov. 23, 2021); available at: https://opportunityinsights.org/wp-content/uploads/2019/01/patents_paper.pdf.

38. Chris Inglis, "National Cyber Policy Will Disrupt Crime and Instill Hope," *The Wall Street Journal*, October 28, 2021 (last accessed Nov. 23, 2021); available at: https://www.wsj.com/articles/national-cyber-policy-will-disrupt-crime-and-instill-hope-cyberattack-cyberspace-11635367439.

39. *For traffic flow*, James Manyika et al, Unlocking the Potential of the Internet of Things, McKinsey Global Institute, June 1, 2015 (last accessed Nov. 24, 2021); available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world, *for electricity,* Estimating the Costs and Benefits of the Smart Grid: A Preliminary Estimate of the Investment Requirements and Resultant Benefits of a Fully Functional Smart Grid, The Electric Power Research Institute, February 28, 2011 (last accessed Nov. 24, 2021); available at: https://www.smartgrid.gov/document/estimating_costs_and_benefits_smart_grid_preliminary_estimate_investment_requirements_and_r, *for air traffic*, Prachi Dhariwal, "Air Traffic Control Using Big Data Analysis and Machine Learning," May 4, 2020 (last accessed Nov. 24, 2021); available at SSRN: https://ssrn.com/abstract=3592705.

40. Trust in Smart City Systems: Characteristics and Key Considerations, Cybersecurity and Information Security Agency, January 2020 (last accessed Nov. 24, 2021); available at: https://ssrn.com/abstract=3592705.

41. Trust in Smart City Systems, CISA.

42. Bianca Wylie, "Civic Tech: A List of Questions We'd Like Sidewalk Labs to Answer," Torontoist (blog), October 30, 2017 (last accessed Nov. 24, 2021); available at: https://torontoist.com/2017/10/civic-tech-list-questions-wed-like-sidewalk-labs-answer/.

43. Guiding Principles: Equity Priorities and Privacy Principles Guide the Smart PDX Program, Smart City PDX, (last accessed Nov. 24, 2021) available at: https://www.smartcitypdx.com/guiding-principles/.

44. For development time, James Manyika et al, Big Data: The Next Frontier for Innovation, Competition, and Productivity, McKinsey Global Institute, May 1, 2011 (last accessed Nov. 24, 2021); available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation, *for time to market, energy efficiency, and safety incidents*, Economic Benefit Report, Smart Manufacturing Leadership Consortium, 2021 (last accessed Nov. 24, 2021); available at: https://smlconsortium.org/economic-benefit, *for factory productivity*, Manyika et al, Unlocking the Potential.

45. *For disrupting manufacturing plants*, Dan Goodin, "How a VPN Vulnerability Allowed Ransomware to Disrupt Two Manufacturing Plants," arstechnia (blog), April 7, 2021 (last accessed Nov. 24, 2021); available at: https://arstechnica.com/information-technology/2021/04/ransomware-shuts-down-production-at-two-manufacturing-plants/, *for ransomware on the rise*, Jenny Darmody, "Ransomware Attacks in Manufacturing Tripled in 2020," Silicon Report (blog), March 2, 2021 (last accessed Nov. 24, 2021); available at: https://www.siliconrepublic.com/enterprise/ransomware-attacks-manufacturing-sector.

46. The State of Ransomware 2021, Sophos, April 2021 (last accessed Nov. 24, 2021); available at: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

47. *For electricity demand and impacts on electric grid*, How Technology Could Change the Way Energy is Produced and Consumed, BP Technology Outlook, BP, 2018 (last accessed Nov. 24, 2021); available at: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/what-we-do/bp-technology-outlook-2018.pdf, *for greenhouse gas reductions and other climate impacts*, Machine to Machine Technologies: Unlocking of a $1 Trillion Industry, The Carbon War Room, 2013 (last accessed Nov. 24, 2021); available at: http://www.carbonwarroom.com/what-we-do/research-publications/M2MReport.

48. Digitalization and Energy, International Energy Agency, 2017 (last accessed Nov. 24, 2021); available at: https://iea.blob.core.windows.net/assets/b1e6600c-4e40-4d9c-809d-1d1724c763d5/DigitalizationandEnergy3.pdf.

49. Cathy Hilborn Feng, "How a Smartwatch Literally Saved This Man's Life and Why He Wants More People To Wear One," *South China Morning Post*, May 11, 2018 (last accessed Nov. 24, 2021); available at: http://www.scmp.com/lifestyle/health-wellness/article/2145681/how-apple-watch-literally-saved-mans-life-and-why-he-wants

50. Sarah Buhr, "The Apple Watch Can Detect Diabetes With an 85% Accuracy, Cardiogram Study Shows," TechCrunch (blog), February 7, 2018 (last accessed Nov. 24, 2021); available at: https://techcrunch.com/2018/02/07/the-apple-watch-can-detect-diabetes-with-an-85-accuracy-cardiogram-study-says/.

51. Manyika et al, Unlocking the Potential.

52. Corey Stern, "Goldman Sachs Says that a Digital Healthcare Revolution is Coming - and it Could Save American $300 Billion," *Bloomberg Insider*, June 29, 2015 (last accessed Nov. 24, 2021); available at: http://www.businessinsider.com/goldman-digital-healthcare-is-coming-2015-6.

53. Jane Sarasohn-Kahn, "For Health Consumers, Trust, Privacy, and Good Experience Must Be Baked Into Digital Health Care," Health Populi (blog), August 24, 2020 (last accessed Nov. 24, 2021); available at: https://www.healthpopuli.com/2020/08/24/for-health-consumers-trust-privacy-good-experience-must-be-baked-into-digital-health-care/.

54. How Can Leaders Make Recent Digital Health Gains Last: Re-Examining the Accenture 2020 Digital Health Consumer Survey, Accenture, 2020 (last accessed Nov. 24, 2021); available at: https://www.accenture.com/_acnmedia/PDF-130/Accenture-2020-Digital-Health-Consumer-Survey-US.pdf.

55. Mark Rosegrant et al, Food Security in a World of Natural Resource Scarcity: The Role of Agricultural Technologies, International Food Policy Research Institute (Washington, D.C.), 2014 (last accessed Nov. 24, 2021); available at: http://dx.doi.org/10.2499/9780896298477.

56. *For cutting water use*, Aaron Tilley, "The Internet Versus The Great California Drought," Forbes, July 20, 2015 (last accessed Nov. 24, 2021); avaialabel at: https://www.forbes.com/sites/aarontilley/2015/07/01/the-internet-versus-the-great-california-drought/, *for herbicide and fuel use*, "Here Come the Robots: Precision and Regenerative Farming," *The Futures Center*, April 12, 2021 (last accessed Nov. 24, 2021); available at: https://www.thefuturescentre.org/here-come-the-robots-precision-and-regenerative-farming/, *for food price reduction*, Rosengrant et al, Food Security.

57. Threats to Precision Agriculture, 2018 Public-Private Analytic Exchange Program, Department of Homeland Security, 2018 (last accessed Nov. 24, 2021); available at: https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf.

58. *For smartphone use*, John Walter, "There's an Ag App for That," *Successful Farming*, November 16, 2016 (last accessed Nov. 24, 2021); available at: https://www.agriculture.com/technology/crop-management/there-s-an-ag-app-for-that, *for decision support systems*, Zhaoyu Zhai et al, "Decision Support Systems for Agriculture 4.0: Survey and Challenges," *Computers and Electronics* in Agriculture, Vol. 170, March 2020 (last accessed Nov. 24, 2021); available at: https://www.sciencedirect.com/science/article/pii/S0168169919316497.

59. Blackmatter Ransomware, Joint Cybersecurity Advisory, The Federal Bureau of Investigation, Cybersecurity and Information Security Agency, and The National Security Agency, October 18, 2021 (last accessed Nov. 24, 2021); available at: https://us-cert.cisa.gov/sites/default/files/publications/Joint-CISA-FBI-NSA_CSA_AA21-291A_BlackMatter_Ransomware.pdf.

60. "Prepared Floor Remarks of Sen. Chuck Grassley of Iowa: Combatting Cyberattacks in America's Food Supply Chain," November 1, 2021 (last accessed Nov. 24, 2021); available at: https://www.grassley.senate.gov/news/remarks/grassley-combatting-cyberattacks-in-americas-food-supply-chain.

61. Shane Tews, "Cybersecurity in Agriculture: Don't Forget About Mobile," AEIdeas (blog), November 9, 2021 (last accessed Nov. 24, 2021); available at: https://www.aei.org/technology-and-innovation/cybersecurity-in-agriculture-dont-forget-about-mobile/.

62. Automated Vehicles for Safety, National Highway Traffic Safety Administration, Department of Transportation, 2020 (last accessed Nov. 24, 2021); available at: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety#:~:text=What%20are%20the%20safety%20benefits,to%20human%20error%20or%20choices.

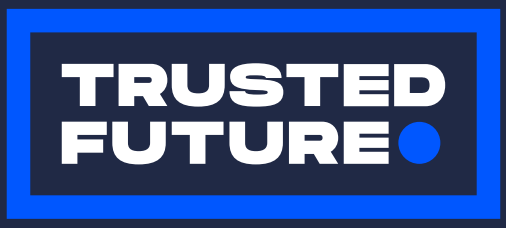
63. *For distrust*, Matthew Hutson, "People Don't Trust Driverless Cars. Researchers Are Trying to Change That," Science, December 14, 2017 (last accessed Nov. 24, 2021); available at: https://www.science.org/content/article/people-don-t-trust-driverless-cars-researchers-are-trying-change, *for cyberattacks*, 2017 Connected Cars and Autonomous Vehicles Survey, Foley and Lardner LLP, 2017 (last accessed Nov. 24, 2021); available at: https://www.science.org/content/article/people-don-t-trust-driverless-cars-researchers-are-trying-change.

64. Michael Mandel and Bret Swanson, "The Coming Productivity Boom: Transforming the Physical Economy with Information, The Technology CEO Council, March 2017 (last accessed Nov. 24, 2021); available at: http://www.techceocouncil.org/clientuploads/reports/TCC%20Productivity%20Boom%20FINAL.pdf.

65. The Impact of 5G on the United States Economy, Accenture Strategy, February 2021 (last accessed Nov. 24, 2021); available at: https://www.accenture.com/_acnmedia/PDF-146/Accenture-5G-WP-US.pdf.

66. Josh Hendel, "The 5G World: What People Care About," *Politico*, February 25, 2020 (last accessed Nov. 24, 2021); available at: https://www.politico.com/news/agenda/2020/02/25/poll-5g-what-do-people-really-want-110831.

67. Hayden, "Changing How App Stores Operate."


TRUSTED
FUTURE