ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Digital Innovation Isn't Undermining Societal Trust; It's the Other Way Around

DAVID MOSCHELLA | FEBRUARY 2023

Defending Digital Series, No. 14: America's declining societal trust will harm its innovation ecosystem, because the next phase of digital growth will require collective confidence in technologies that operate in the public sphere.

Between the scandals of Theranos and FTX, the collapse of cryptocurrencies and NFTs, the chaos and content suppression at Twitter, steep share price declines, the voting machine malfunctions in Maricopa County, and the failure of the Federal Aviation Administration's computer systems, the last few months haven't been good ones for trust in digital technologies. These high-profile events have only added to long-standing security challenges for the technology industry such as denial-of-service attacks, malware, ransomware, fraud, scams, identity and intellectual property theft, misinformation, hacktivists, privacy violations, data loss, and more. As has often been noted, the Internet was not designed with digital trust in mind. Quite the opposite; it was optimized for the openness and decentralization needed for scientific collaboration and resiliency.

But we shouldn't exaggerate the impact or extent of these problems. Citizens around the world have become comfortable managing their finances, careers, health, and relationships through various online intermediaries, and this implies that there is a solid foundation of digital trust. To most Americans, digital products and services from companies such as Amazon, Google, Microsoft, and Apple have offered clear value and rarely seem to break or fail. Businesses also trust the Internet for everything from simple communications to complex global transactions.

Thus, while efforts to improve digital trust must continue, the bigger challenge is that declining *societal* trust will limit America's ability to innovate in digital technologies. Advanced applications such as autonomous vehicles, drones, smart grids, charging infrastructure, blockchains, digital cash, voting systems, digital IDs, facial recognition, robotics, and the like will operate in public spheres and thus will depend on collective confidence in the technology more than just consumer demand for it. Nations with high levels of societal trust therefore will have some distinct advantages in deployment and acceptance—and as a high-innovation, low-trust nation, America's position will be more strategically precarious than it currently appears.

Improving this situation will require both a digital trust and a societal trust agenda. But it's the latter that is more important and more difficult.

SNOWBALLING SOCIETAL DISTRUST

As many have noted, within just a few generations the United States has shifted from a relatively high-trust nation to a relatively low one, now ranking 30th according to *U.S. News and World Report*.[1] It's generally recognized that this shift began gathering significant momentum in the 1960's and '70s, driven by doubts about President Kennedy's assassination, false government claims about the Vietnam war, pervasive air and water pollution, the impeachment of President Nixon, oppressive race and gender norms, and a self-identified "counterculture" that openly questioned traditional sources of official and cultural authority. Much of this distrust was warranted and long overdue, so in this sense distrust can lead to needed improvements.

But America has lived through a series of events in the 21st century that have shaken just about every traditional pillar of societal trust: the false claims of weapons of mass destruction that were used to justify the Iraq war; the recklessness of the financial services industry and failure of regulators that led to the 2008 crash; the sickening child abuse covered up by the Catholic Church, the Boy Scouts, gymnastic coaches, and others; the NSA's mass surveillance of American citizens as revealed by Edward Snowden; the OxyContin scandal at Purdue Pharma; widespread questioning of both the 2016 and 2020 presidential elections; the George Floyd and other police abuse videos; an FBI seen by many as overly politicized and a Supreme Court seen by many others as overly conservative; teachers unions blamed for keeping K-12 schools closed for too long; a Congress that has run up more than $31 trillion in debt; a scientific community that suppressed and even demonized peers who challenged the official views regarding the origins and management of COVID-19; the chaotic military withdrawal from Afghanistan; ongoing failure at America's southern border; the weakening of academic standards at seemingly every educational level; a biased and polarized national media; and a citizenry increasingly wary and intolerant of those it disagrees with. The benefits of today's era of distrust are much harder to discern.

This erosion in institutional trust and deference has created much deeper problems than anything stemming from the digital world, and the challenge for America's next generation of leaders is to somehow reverse these trends. The Internet may have made it easier to talk about societal problems, but it did not cause them. Indeed, one thing is clear: The loss of societal trust has had very little to do with technology. While many commentators have blamed today's societal divisions on misinformation, the examples above show the opposite. The most serious losses of trust occur when people learn the truth about what has actually happened. Whether these truths emerge first from online or offline sources is a relatively minor factor.

IMPROVING DIGITAL TRUST

Compared to the challenge of making America a high-trust nation again, the task of increasing trust in digital technologies is much more straightforward. Whereas societal divisions can seem irreparable and often involve participants who fundamentally disagree about what should be done, there is a broad-based consensus that the digital world needs to be safer and more stable. The main debate is about how to do this, and whether industry evolution or government regulation is the best path forward, and if it's the latter, then how onerous and prescriptive it

should be. In order to systematically assess and enhance the state of digital trust today, it's useful to segment the challenge into relatively discrete categories:

1. **Product trust.** *Do digital products and services perform as advertised?* The industry tends to do pretty well here, but artificial intelligence presents new challenges going forward.
2. **Company trust.** *Do the leading technology companies behave in a socially responsible way?* The revelations of the *Twitter Files* have been damaging, but most established Internet businesses are trusted, especially in e-commerce.
3. **Transaction trust.** *Is there sufficient security, fraud detection, oversight, and recourse?* The FTX scandal is of historic and lasting proportions, but most digital transactions, especially with the major players, are trustworthy.
4. **Personal trust.** *Are citizens' digital property and accounts sufficiently secure and protected?* Ransomware remains particularly difficult to fully prevent.
5. **Technology trust.** *Are core technologies such as identification, encryption, backup, and recovery working effectively across systems?* Good progress has been made here.
6. **Privacy trust.** *Is there a right to correct or forget, and an effective range of settings and permissions?* There hasn't been much change here in recent years.
7. **Fairness trust.** *Are there accepted principles of data usage, fair use, fair compensation, and fair competition?* We think these concerns have been overblown, which is why we opposed the Journalism Competition and Preservation Act.[2] Indeed, given that many of the most valuable Internet services are free, fairness is at the core of the online world.
8. **Environmental trust.** *Is the technology industry sufficiently green?* There has generally been too much focus on the tech industry's energy usage and not enough on the environmental downsides of hi-tech manufacturing, what to do with billions and billions of obsolete tech products, and the many ways that the digitalization of society reduces energy use.[3]
9. **Global trust.** *Are the societal norms mentioned above undermined or reinforced by offshore players in today's increasingly multipolar world?* The Internet is clearly splintering along national and regional lines, meaning that trust in the above areas will vary significantly by geography.
10. **Ideation trust.** There is now a civil-society industrial complex funded by left-of-center foundations and amplified by a media that promotes an antitechnology, anti-big-business agenda. Many of these groups' raison d'etre is to paint the current techno-economic system in an unfavorable light and sow seeds of distrust.

It's important for the technology industry to effectively manage these issues as it goes through what could be an extended recessionary phase after the long boom of the last 20 years. Companies behave one way when times are good, and differently when financial pressures mount. Don't be surprised if popular services that are currently free begin to have charges, especially if EU-style privacy laws are adopted in the United States. But looking ahead, many tech services are becoming core components of working societies, and this means that key technologies must maintain relatively high levels of stability and trust. The incentives to

continually make technology safer are strong, and this provides grounds for long-term optimism. In contrast, improvements in societal trust seem much less certain.

CO-EVOLVING TRUST

For decades, the idea that businesses, science, the arts, culture, and society itself would increasingly *co-evolve* with information technology has been a useful guiding principle. In this sense, the largely separate evolution of digital and societal trust thus far seems like an aberration. But this anomaly won't continue. The first great phase of Internet industry growth was driven by consumers, who could decide for themselves whether a particular product or service was worth using. The next phase of opportunity will be much more collective in nature. From autonomous vehicles and drones to digital IDs and online voting, technologies that operate in the public sphere won't be driven by individual consumer choice alone. They must be developed and deployed in a trusted, cooperative way. It only makes sense that high-trust—often smaller—nations would have advantages in these areas, and from Singapore to Estonia there are many examples of this being the case.

It follows that America's declining national trust presents a direct challenge to its future technology leadership. Continually improving digital products and services is clearly important, but it's no longer a guarantee of leading-edge innovation. Building an advanced, intelligent economy will require a level of societal cohesion that is currently lacking, and without it antitechnology forces are much more likely to prevail. Digital innovation isn't undermining societal trust, but declining societal trust will eventually undermine digital innovation.

About This Series

ITIF's "Defending Digital" series examines popular criticisms, complaints, and policy indictments against the tech industry to assess their validity, correct factual errors, and debunk outright myths. Our goal in this series is not to defend tech reflexively or categorically, but to scrutinize widely echoed claims that are driving the most consequential debates in tech policy. Before enacting new laws and regulations, it's important to ask: Do these claims hold water?

About the Author

David Moschella is a non-resident senior fellow at ITIF. Previously, he was head of research at the Leading Edge Forum, where he explored the global impact of digital technologies, with a particular focus on disruptive business models, industry restructuring and machine intelligence. Before that, David was the worldwide research director for IDC, the largest market analysis firm in the information technology industry. His books include *Seeing Digital—A Visual Guide to the Industries, Organizations, and Careers of the 2020s* (DXC, 2018), *Customer-Driven IT* (Harvard Business School Press, 2003), and *Waves of Power* (Amacom, 1997).

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit us at www.itif.org.

ENDNOTES

1. *U.S. News & World Report*, "These Are the Most Trustworthy Countries," https://www.usnews.com/news/best-countries/rankings/trustworthy.
2. Daniel Castro, "Congress Should Not Break Big Tech to Fix Local News," *Innovation Files*, February 11, 2022, https://itif.org/publications/2022/02/11/congress-should-not-break-big-tech-fix-local-news/; Daniel Castro, "History Shows That the News Industry Does Not Need a Handout from Big Tech," *Innovation Files*, August 31, 2022, https://itif.org/publications/2022/08/31/history-shows-that-the-news-industry-does-not-need-a-handout-from-big-tech/.
3. Colin Cunliff, "Beyond the Energy Techlash: The Real Climate Impacts of Information Technology" (ITIF, July 2020), https://itif.org/publications/2020/07/06/beyond-energy-techlash-real-climate-impacts-information-technology/.