BROOKINGS

TechTank

How technology and the world have changed since 9/11

Darrell M. West and Nicol Turner Lee Friday, August 27, 2021

On Sept. 11, 2001, one of us (Darrell) was teaching a political science course at Brown University, while the other (Nicol) was four days away from her wedding in Westchester County. The morning of those infamous terrorist attacks, Darrell had finished his lecture and while walking across campus encountered a fellow professor who said it was terrible what happened to those planes. "What planes?" Darrell asked, unaware of the attacks in New York City and Washington, D.C. This was the time before ubiquitous cell phones and social media platforms, where news traveled quickly inside classrooms and around the globe.

Nicol was getting ready for her wedding and had woken up after a long night preparing table tent cards for invited guests. When she was told to turn on the television at her parents' home, she witnessed one of the two planes hit the second of the former Twin Towers, which was located just 30 minutes away from her location. The phone calls from both worried and frenetic guests would be the beginning of her 9/11 experience as members of her bridal party were unable to fly, and the groom would drive more than 10

hours to ensure his attendance at the wedding. The ceremony ultimately took place with a far smaller crowd than the anticipated 500 guests that had confirmed, which would be mostly comprised of Nicol's relatives who were also from the New York area. For a while, it was not clear whether the officiating minister and even the groom—who would wait for hours to cross the George Washington Bridge—would make the event.

At the time, there were no smartphones to initiate a video call with loved ones. The active cell phone service was down after the Twin Towers were hit in New York City, which made it difficult to hear from family and friends who may have been in the vicinity of the plane crashes. Similar occurrences happened in the series of related terrorist events in Virginia and Pennsylvania. Neither of us also knew how dramatically technology and the world would change following the terrorist attacks. Substantial alterations in news transmission, technology innovation, telecommunications networks, disaster preparedness, personal privacy, digital inequity, and security levels arose after the tragic events of this day. From a virtual standpoint, so many things have shifted over the last two decades that it is hard to imagine the world as it existed in 2001.

INSTANT NEWS AND MISINFORMATION

Today, it is impossible to conceive a situation where something big happens and people don't know instantly what has occurred. News spread quickly through digital websites, social media platforms, mobile calls, and instant messages. Tweets fly around the world and people know about important events almost as soon as they take place. Back then, social media platforms were not widely adopted, and who even knew what a tweet was during a time when most people were still reliant on their home telephone services.

The upside of the rapidity of news transmission is that people are aware of new developments far more quickly and in cases of such terrorist attacks are in a position to protect themselves. We can see events unfold and react in whatever manner makes sense for individuals and organizations. Back then, we both watched the 9/11 events on television, but broadcast did not particularly enable us to quickly share what was happening from our corners of the world with others. Instead, we had to wait until the reporter shared more as the events transpired over the course of the day.

While having the ability to rapidly transmit our versions of the story seemed constructive at the time, the current realities of misinformation and disinformation reveal the downside of instant news, especially the pressure to react immediately to unfolding events that can lead to overreactions, false interpretations, or premature conclusions. Nicol recalls trying to assess whether she should immediately cancel the wedding after witnessing the devastation, but she didn't after hearing the voices of loved ones who desired to come just to be closer to other family members in the midst of this dramatic event. In a contemporary world of fast news transmission and speedy reactions, technology's enablement of skewed truths can lead to misinterpretations, quick judgments, and outright falsehoods about what happens. Both events and people become easy to manipulate when information is quickly forming and incomplete.

Just imagine the mischief that could have been created in a 9/11-style attack during a time of social media. Immediately, there would be speculation over what happened and who was responsible. If recent events are any indication, there likely would be a wide range of possible suspects: foreign terrorists, domestic agents, political opponents, immigrants, or racial, religious, or ethnic minorities. On the day, social media algorithms will likely promote automatic posts with the most engagement: the incendiary and the controversial. This could lead to real-life acts of violence and mobilization in short amounts of time. Many people would not trust experts during a highly polarized time and there likely would be no bipartisan commission to investigate what happened. Conspiracy theories would flourish, and false accounts would circulate among digital echo chambers, leading to widespread misunderstandings of what transpired and who was responsible.

The same echo chambers created by the current information ecosystem have also left many intensely concerned regarding how technology has fueled extremism, polarization, and radicalization. Many observers worry that today's technology is tearing communities apart, not building bridges or enabling constructive civic discourse. In 2001, it is probable that contemporary technology would have made it far more difficult to define, address, and even heal from the tragic events of 9/11.

MORE ROBUST but Vulnerable networks

One positive contemporary feature is that our communications networks are more broad-based and robust today than 20 years ago. Government agencies and private companies have beefed up their disaster preparedness and telecommunications providers have strengthened their digital infrastructure. We have wired and wireless networks that can withstand the possible interruptions caused by downed antennae, or damaged wiring. Following 9/11 and Hurricane Katrina, the United States realized the importance of mobile communications during terrorist attacks and natural disasters. Steps have been taken to safeguard vital networks, which is a huge advancement since 9/11 when thousands of people in New York, and in the area of the Pentagon bombing had to run and walk for miles to what appeared to be a safe space for shelter. Back then, we didn't even have voice-activated internet-enabled navigational tools that could advise pedestrians and drivers of road closures, or other potential road or walking hazards.

But even with our improved communications capabilities, we now face different kinds of threats. Back then, they were the planes crashing into buildings or individuals detonating explosive devices. Now, government, business, and nonprofits encounter cyber threats, ransomware attacks, and unwanted digital intrusions. These attacks can occur from state-sponsored sources or criminal enterprises that operate with impunity.

These are different problems than those encountered during 9/11 and require different societal and global responses. Could 9/11 have been diverted if the technology had forecasted such an event? How could more effective cybersecurity measures and online surveillance reveal the events that shook the world? It has become increasingly clear that everyone—from government to the average citizen—must take cybersecurity far more seriously and implement steps that safeguard their networks and personal devices. Some of this means better digital hygiene, password protection, and two-factor authentication. But it also involves stronger systems that protect critical infrastructure, financial networks, and health care facilities, among others.

Privacy versus national security

The balance between privacy and national security shifted markedly following 9/11. With the passage of the U.S. Patriot Act in October 2001, government officials gained new authority to surveil possible threats. For American citizens, administrators could go to a Foreign Intelligence Surveillance (FISA) Court and request permission to monitor phone calls, emails, and/or text messages. With the advent of smartphones and the prevalence of electronic communications, public authorities also developed new tools for monitoring particular individuals and tracking their physical whereabouts via geolocation data.

Taken together, these actions dramatically expanded government power to engage in mass surveillance. Yet at the same time, the moves alarmed civil liberties advocates who worried about privacy invasions and unwarranted oversight of people's activities. Those fears eventually led to some curtailment of government activities via the U.S. Freedom Act of 2015, but we still face a policy environment where there is no national privacy law and considerable government power for monitoring national security threats. Twenty years after the attack, the country continues to debate where to draw the line between promoting personal privacy and protecting national security.

Digital inequity

Technology innovation has flourished, but many are still not able to access the benefits of the digital revolution. They either have no meaningful broadband access from their home, or they have such slow broadband speeds that their ability to take advantage of digital connectivity is quite limited. They are not able to apply for jobs, shop online, use video streaming services, take advantage of telemedicine, or enroll in online courses.

Without reasonable access, they are shut out of the digital economy and left behind. They face limits in terms of jobs, economic opportunity, and social connectedness. Twenty years ago, they were probably more normal in a society with limited technological tools. Today, these same populations are at the most risk of being digitally invisible and excluded if a new national attack were to be waged. They wouldn't read, hear, or see it because they do not partake or benefit from internet access. Unfortunately, those on the wrong side of digital opportunities find themselves suffering long-term harms and difficulties in dealing with many forms of trauma.

Retaining hope during a time of digital insecurity

When you add all these digital innovations together since 9/11, we have undergone a dramatic revolution. We spend more and more of our lives online, which gives us access to the latest developments, the ability to communicate quickly with one another, and the capacity to access a broad range of digital services and products. During the pandemic, our increasing reliance on technology became more pointed, as in-person services were shut down to manage social distancing.

Yet the extraordinary increase in change at all levels has generated a parallel increase in anxiety, insecurity, and nervousness. According to the Edelman Trust Barometer, two-thirds of people are concerned about the pace of digital change and feel they are not always able to distinguish real from fake realities. Many also worry about technology and can see how it has fueled a variety of social, economic, and political problems. As Nicol watched the explosion on her television on that fretful day, she kept saying that this experience was not real and that the state of New York was resilient, and this could possibly not be happening to their strong and sharp-edged residents before her wedding. But it was and she watched it in horror, along with others who had seen or heard about what was transpiring. Even Darrell had to confirm what he just heard about the planes that took down America's morale and sense of safety in a few short minutes and found it impossible to fathom the destructiveness of the attack.

As we move beyond the 9/11 commemoration, our challenge is to find a positive path forward with the use of technology. Technology innovation is not likely to slow and indeed digital advances are likely to accelerate. Super-computing and quantum computing will push change ahead and enable even more powerful digital applications. But figuring out how to retain hope and humanity through the use of technological advances will be crucial, especially in efforts to minimize problems of misinformation, personal privacy, cybersecurity, inequity, and civic toxicity.

Acknowledgments:

The authors would like to thank Samantha Lai for her research assistance.