Unsplash © Jesse Mills

On the 20th anniversary of 9/11, here’s what you need to know about what technology has contributed to its legacy

Every week, Maddyness curates articles from other outlets on a topic that is driving the headlines. On the week of the 20th anniversary of the 9/11 attacks, we're talking about how technology has developed since 2001, and how digital tools have been used to identify victims to the present day and expand U.S. surveillance capabilities.

New York’s medical examiner’s office has been approved to use new technology to identify remaining victims of the 9/11 attacks. The forensic methodology known as Next Generation Sequencing is more sensitive and can be used to identify victims who cannot be identified by conventional DNA detection techniques.

The technology has been studied by the medical examiner’s office since 2018, but approval for use was delayed by the pandemic. It has been used this week to identify two more victims just a week ahead of the 20th anniversary of the

attacks. Read more via *AP News* and *The Guardian*.

Surge of the surveillance state

Technology has developed since the attacks to identify victims but also to expand security. The digital surveillance state surged in the years after 2001, starting with the Patriot Act passed less than two months after the attack. It gave the U.S. government significant powers to monitor citizens behaviour through warrantless searches of mobile phones and digital correspondence.

Read more via *The Washington Post.*

Digital security subjects ordinary New Yorkers to surveillance

Digital surveillance technology has also altered the way investigations are carried out on the ground. Technology developed since the attacks in 2001 have changed the way New York's Police Department handles street crime and terrorist threats.

The New York Times revealed that New Yorkers have frequently encountered surveillance equipment including facial recognition software, mobile X-ray vans, licence plate readers and drones which have also been spotted hovering over demonstrations.

The clamp down on security across the New York Police Department has been funded by a growing intelligence budget which has more than quadrupled since the attacks.

Though the department is confident digital security has been responsible for combatting would be attacks, surveillance has also received criticism from activists and NGOs such as Amnesty International for invading the privacy of ordinary citizens and disproportionately targeting New York's black community.

People can be targeted using facial recognition tools which can be applied to social media profiles, intercepted phone calls and drones.

Read more via *The New York Times*.

Digital security has changed air travel

Technology has also changed pre-flight security. In the wake of the attacks, the

Transportation Security Administration (TSA), a federal airport security force replaced private security companies hired by airlines.

But stricter security checks and longer waiting lines meant more support has gathered for “trusted traveller programs,” meaning people can pay extra and agree to provide additional information, and consent to background checks so they do not have to go through additional security checks such as removing shoes and electrical items from carry ons.

The programme currently uses private vendors to gather pre-flight information on applicants and hopes to work with more vendors by the end of the year. The TSA is trialling kiosks equipped with facial recognition technology to check photo IDs. But critics are concerned that connecting tools to the internet would leave the information vulnerable to hackers.

The TSA have also be criticised in the past for using full body scanners which produced images likened to “virtual strip searches.” The scanners were quickly removed. Read more via *AP News.*

Article by ABBY WALLACE