

COSTS OF WAR



Total Information Awareness: The High Costs of Post-9/11 U.S. Mass Surveillance

The Bottom Line: Since the 9/11 attacks, the United States has witnessed an unprecedented expansion of mass surveillance, built upon older legacies of institutionalized racism, yet much different in scale and technology from what existed before. Today, our ever-expanding surveillance systems may seem inevitable, but they must be understood as policy choices driven by the fear, Islamophobia, xenophobia, weakened civil liberties protections, and exponentially increased funding of the post-9/11 era. While mass surveillance affects all Americans, it has particularly impacted Muslims, immigrants, and protesters for racial and labor justice. Surveillance programs have cost untold taxpayer dollars, normalized an erosion of privacy, and entrenched an expanding surveillance infrastructure that grows ever more difficult to track and control.



Today's U.S. Mass Surveillance Includes:

- **Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act:** A provision up for Congressional reauthorization this year, Section 702 legalizes warrantless wiretapping and retaining data on foreigners abroad, with U.S.

residents' data swept up "incidentally." The FBI has often misused the 702 database to target political dissenters, racial justice activists, others.

- **Executive Order 12333:** Originally issued by President Reagan during the Cold War and expanded by later presidents, EO 12333 allows the government to conduct warrantless bulk data collection abroad without judicial or congressional oversight, and has been used for dragnet programs that siphon the contents of text messages and phone calls made abroad, including those of Americans.
- **Department of Homeland Security's "Extreme Vetting" Programs:** In collaboration with private companies and unregulated data brokers, DHS collects social media information from nearly all travelers to the U.S.—including visa and Green Card holders and naturalized citizens. The data can be indefinitely retained and shared with foreign governments. DHS's electronic surveillance of immigrants, known as Alternatives to Detention (ATDs), includes tracking ankle monitors and mobile technology with voice and facial recognition.
- **Increased Local Law Enforcement Surveillance:** Private companies sell raw location data from personal devices to local police departments, which has led to increased monitoring of racial justice protesters. Police departments have expanded their surveillance of Black, Latinx, and Muslim communities using technology developed for war zones, including tools such as the Domain Awareness System. Local police departments have entered into agreements to participate in federal immigration enforcement projects, such as Immigration and Customs Enforcement's (ICE) 287(g) program.
- **Inflated Government Budgets for Surveillance:** Untold taxpayer dollars have been spent developing surveillance infrastructure and technology. The annual U.S. intelligence budget has doubled from approximately \$40 billion per year in the late 1990s to \$80 billion per year in 2020. The government has rarely been able to demonstrate that such funding has created public safety at a scale that merits the cost. These billions, if not trillions, of dollars could be spent addressing pressing social issues, such as poverty, climate crises, and racial disparities.
- **Complex Infrastructure and Lack of Transparency:** The infrastructure built to sustain intensified mass surveillance has grown dizzyingly large and complex and proven very difficult to roll back. This complexity, along with the government's lack of transparency, make it nearly impossible to disentangle mass surveillance from the tightly interlinked areas of intelligence, counterterrorism, and homeland security.

[The full report is available here.](#) For more information, please contact costsofwar@brown.edu.