

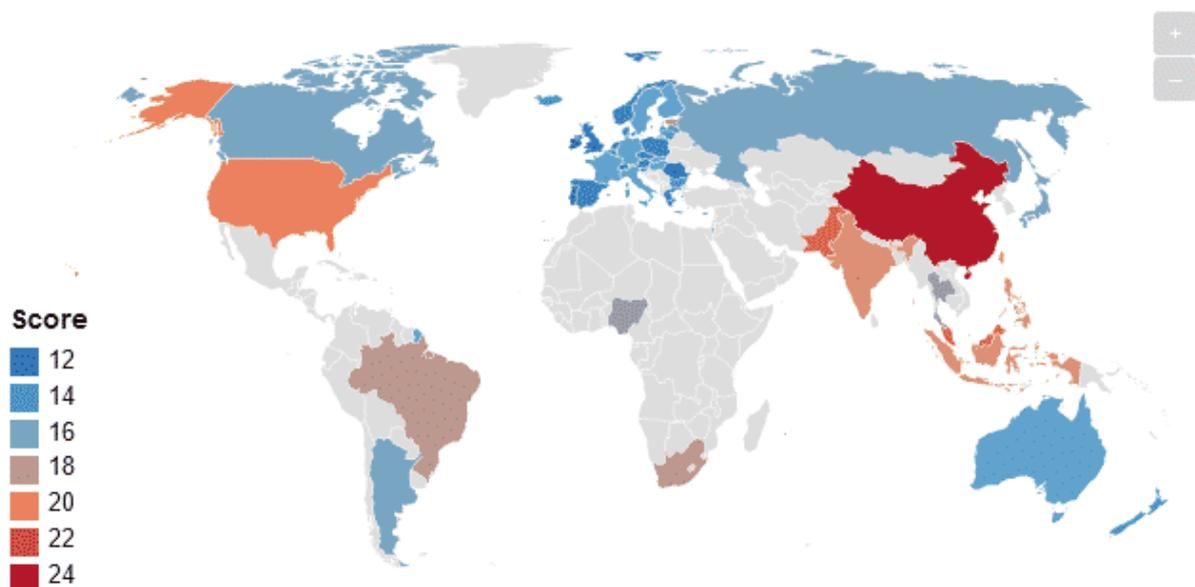


Shock: U.S. 4th Worst Abuser Of Biometric Privacy Rights

The Chinafication of America is well underway. The only three countries with a worse record than the U.S. are China, Malaysia and Pakistan. This should be a massive wake-up call for all Americans to demand that this madness be stopped. □ TN Editor

Does anyone really believe America is still the land of the free?

Collection and storage of biometrics by country



Map: Comparitech • [Get the data](#) • Created with [Datawrapper](#)

Since 9/11, DHS, the FBI, the CIA, and countless other alphabet soup agencies have turned the United States into a public surveillance monstrosity.

In 19 years, one terrorist attack has done what no one else could have dreamed of: turn America's freedoms into a distant memory.

Abusing citizen's rights and privacy used to be the hallmark of dictatorships and police states like the CCCP or North Korea.

A recent study conducted by Comparitech, rated 50 countries from best to worst at protecting citizen's biometric data.

The study found that America is one of the world's worst abusers of citizen's biometric privacy.

"While China topping the list perhaps doesn't come as too much of a surprise, residents of (and travelers to) other countries may be surprised and concerned at the extent of biometric information that is being collected on them and what is happening to it afterward."

This really should not come as a surprise, because last year Comparitech revealed that American and Chinese cities lead the world in spying on

their citizens. Last week, I wrote an article explaining how 2019 would go down as the year that facial recognition and corporate surveillance became commonplace in America.

Comparitech’s recent study on biometric privacy compared how 50 countries collect and use data to identify innocent people:

- Many countries collect travelers’ biometric data, often through visas or biometric checks at airports
- Every country we studied is using biometrics for bank accounts, e.g. fingerprints to access online app data and/or to confirm identities within the banks themselves
- Despite many countries recognizing biometric data as sensitive, increased biometric use is widely accepted
- Facial recognition CCTV is being implemented in a large number of countries, or at least being tested
- EU countries scored better overall than non-EU countries due to GDPR regulations protecting the use of biometrics in the workplace (to some extent)

The USA is the 4th worst abuser of citizen’s biometric privacy

Rank	Country	Score
#1	China	24/25
#2	Malaysia	21/25
#3	Pakistan	21/25
#4	USA	20/25
#5	India, Indonesia, The Philippines and Taiwan	19/25

Comparitech warns, “these 5 countries show a concerning lack of regard for the privacy of people’s biometric data.” That’s right, the former “land of the free” has become the land of the surveilled and tracked.

How can that be you ask?

According to Comparitech, the United States scores highly in most areas due to:

- Having biometrics in passports, ID cards, and bank accounts.
- Having a biometric voting system (optical scan equipment used in a large number of states).

- Not having a specific law to protect citizens' biometrics. While there is a handful of state laws that protect state residents' biometrics (as can be seen in our state privacy study), this does leave many US citizens' biometrics exposed as there is no federal law in place.
- Implementing the widespread use of facial recognition cameras with law enforcement pushing for further use in the identification of criminals. For example, the FBI and ICE have recently been criticized due to their use of facial recognition technology to scan drivers' license photos without gaining the citizens' consent beforehand. Equally, some city-level bans have been put in place with San Francisco (CA), Oakland (CA), Berkeley (CA), and Somerville (MA) banning government use of facial recognition technology.
- The growing use of biometrics in the workplace. Many companies use employees' biometrics for certain actions, e.g. using a fingerprint to gain access to a work computer. Again, some state laws offer a little more protection but this still leaves many employees' biometrics exposed.
- Fingerprints being required for most American visas and everyone's fingerprints being collected upon entry to the country.

Curiously, Comparitech failed to elaborate on DHS's national Real-ID program which forces everyone to provide biometric information to drive or fly in America. If they had included Real-ID in their study it is my opinion that America would be 2nd only to China in abusing citizen's biometric privacy.