



Dear Friends of RSI

We are pleased to share the news that RSI has co-published a major new research report -- [*Dangerous Data: Police Abuse of Access to Personal Data in the United States and its Global Implications*](#) -- produced in partnership with [Privacy International](#). After years of meticulous research including examining over 130 federal civil rights lawsuits filed across the United States, we can now tell the stories of ordinary people whose lives have been turned upside down because of the largely unchecked access to and over-reliance on vast databases of personal information that US police have.

The picture is alarming. In the United States today, police officers can search enormous collections of personal data -- about millions of people never suspected of any wrongdoing -- without a warrant, without a court order, and with almost no legal accountability. These databases, many of them built up in the fearful immediate aftermath of 9/11, now contain everything from home addresses and Social Security numbers (akin to national ID numbers) to photographs, vehicle records, social media activity, financial information, and even details about people's family members and associates. Private data broker companies sell access to all of this directly to law enforcement -- openly and legally.

The consequences of these practices, as our report documents, can be devastating. One Pennsylvania man was arrested for a murder he had nothing to do with and spent more than 17 months behind bars - because of misuse of a database. A Minnesota TV broadcaster discovered that police officers and government workers across the state had secretly looked up her driver's licence photo and other personal information nearly 4,000 times. And a South Carolina woman was looked up in a police database by an officer who then allegedly sexually assaulted her; a jury eventually awarded her \$500,000. (The locality involved has always denied wrongdoing.)

These are not isolated incidents. Our research shows that there are patterns: women and people of colour are disproportionately harmed. Moreover, these problems span the entire country and have lasted through multiple presidential administrations.

Despite being a US-focused report, this matters for us here in the UK because Westminster passed laws in 2024 granting authorities access to bulk social media data, and there was pre-existing access to other bulk personal data. Governments around the world are expanding law enforcement's reach into personal information, often without the safeguards that international human rights law demands – or even basic safeguards to make sure the data is correct, which (our research suggests) it often isn't. The United States provides a powerful and troubling preview of what happens when those safeguards are absent.

Our report is a warning and a call to action for legislators everywhere to investigate these practices and put strong protections in place before the harms become entrenched. We are calling for government agencies in the US and elsewhere to be much more transparent about what data they hold or have access to, and what they use it for – and much stricter rules are needed to limit police access to records and ensure that any data held is accurate.

Yours sincerely

Sarah St Vincent
Executive Director



If you would like to unsubscribe, please [click here](#).

