Holding law enforcement accountable for electronic surveillance

8 August 2018

AUDIT's senior authors, MIT professor Shafi Goldwasser and principal research scientist Daniel J. Weitzner. Credit: MIT CSAIL

When the FBI filed a court order in 2016 commanding Apple to unlock the San Bernandino shooter's iPhone, the news made headlines across the globe. Yet every day there are tens tens of thousands of of other court orders asking tech companies to turn over Americans' private data. Many of these orders never see the light of day, leaving a whole privacy-sensitive aspect of government power immune to judicial oversight and lacking in public accountability.

To protect the integrity of ongoing investigations, these data requests require some secrecy: companies usually aren't allowed to inform individual users that they're being investigated, and the court orders themselves are also temporarily hidden from the public.

In many cases, though, charges never actually materialize, and the sealed orders usually end up forgotten by the courts that issue them, resulting in a severe accountability deficit.

To address this issue, researchers from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) and Internet Policy Research Initiative (IPRI) have proposed a new cryptographic system to improve the accountability of government surveillance while still maintaining enough confidentiality for the police to do their jobs.

"While certain information may need to stay secret for an investigation to be done properly, some details have to be revealed for accountability to even be possible," says CSAIL graduate student Jonathan Frankle, one of the lead authors of a new paper about the system, which they've dubbed "AUDIT" ("Accountability of Unreleased Data for Improved Transparency"). "This work is about using modern cryptography to develop creative ways to balance these conflicting issues."

Many of AUDIT's technical methods were developed by one of its co-authors, MIT professor Shafi Goldwasser. AUDIT is designed around a public ledger on which government officials share information about data requests. When a judge issues a secret court order or a law enforcement agency secretly requests data from a company, they have to make an iron-clad promise to make the data request public later in the form of what's known as a "cryptographic commitment." If the courts ultimately decide to release the data, the public can rest assured that the correct documents were released in full. If the courts decide not to, then that refusal itself will be made known.

AUDIT can also be used to demonstrate that actions by law-enforcement agencies are consistent with what a court order actually allows. For example, if a court order leads to the FBI going to Amazon to get records about a specific customer, AUDIT can prove that the FBI's request is above board using a cryptographic method called "zero-knowledge proofs." First developed in the 1980s by Goldwasser and other researchers, these proofs counterintuitively make it possible to prove that surveillance is being conducted properly without revealing any specific information about the surveillance.

AUDIT's approach builds on privacy research in

accountable systems led by paper co-author Daniel J. Weitzner, director of IPRI.

"As the volume of personal information expands, better accountability for how that information is used is essential for maintaining public trust," says Weitzner. "We know that the public is worried about losing control over their personal data, so building technology that can improve actual accountability will help increase trust in the Internet environment overall."

As a further effort to improve accountability, statistical information from the data can also be aggregated so that that the extent of surveillance can be studied at a larger scale. This enables the public to ask all sorts of tough questions about how their data is being shared. What kinds of cases are most likely to prompt court orders? How many judges issued more than 100 orders in the past year, or more than 10 requests to Facebook this month? Frankle says the team's goal is to establish a set of reliable, court-issued transparency reports, to supplement the voluntary reports that companies put out.

"We know that the legal system struggles to keep up with the complexity of increasing sophisticated uses of personal data," says Weitzner. "Systems like AUDIT can help courts keep track of how the police conduct surveillance and assure that they are acting within the scope of the law, without impeding legitimate investigative activity."

Importantly, the team developed its aggregation system using an approach called multi-party computation (MPC), which allows courts to disclose relevant information without actually revealing their internal workings or data to one another. The current state-of-the-art MPC would normally be too slow to run on the data of hundreds of federal judges across the entire court system, so the team took advantage of the court system's natural hierarchy of lower and higher courts to design a particular variant of MPC that would scale efficiently for the federal judiciary.

"[AUDIT] represents a plausible way, both legally and technologically, for increasing public accountability through modern cryptographic proofs of integrity," says Eli Ben-Sasson, a professor in the computer science department at the Technion Israel Institute of Technology.

According to Frankle, AUDIT could be applied to any process in which data must be both kept secret but also subject to public scrutiny. For example, clinical trials of new drugs often involve private information, but also require enough transparency to assure regulators and the public that proper testing protocols are being observed.

"It's completely reasonable for government officials to want some level of secrecy, so that they can perform their duties without fear of interference from those who are under investigation," Frankle says. "But that secrecy can't be permanent. People have a right to know if their personal data has been accessed, and at a higher level, we as a public have the right to know how much surveillance is going on."

Next the team plans to explore what could be done to AUDIT so that it can handle even more complex data requests—specifically, by looking at tweaking the design via software engineering. They also are exploring the possibility of partnering with specific federal judges to develop a prototype for real-world use.

"My hope is that, once this proof of concept becomes reality, court administrators will embrace the possibility of enhancing public oversight while preserving necessary secrecy," says Stephen William Smith, a federal magistrate judge who has written extensively about government accountability. "Lessons learned here will undoubtedly smooth the way towards greater accountability for a broader class of secret information processes, which are a hallmark of our digital age."

Frankle co-wrote the paper with Goldwasser, Weitzner, CSAIL Ph.D. graduate Sunoo Park and undergraduate Daniel Shaar, The paper will be presented at the USENIX Security conference in Baltimore August 15 to 17.

IPRI team members will also discuss related surveillance issues in more detail at upcoming

workshops for both USENIX and this month's International Cryptography Conference (Crypto 2018) in Santa Barbara.

Provided by Massachusetts Institute of Technology