Digital security and due process: A new legal framework for the cloud era

Kent Walker
SVP & GENERAL COUNSEL

Editor's note: This is an abbreviated version of a speech Kent delivered today at The Heritage Foundation in Washington, D.C.

For as long as we've had legal systems, prosecutors and police have needed to gather evidence. And for each new advance in communications, law enforcement has adapted. With the advent of the post office, police got warrants to search letters and packages. With the arrival of telephones, police served subpoenas for the call logs of suspects. Digital communications have now gone well beyond the Postal Service and Ma Bell. But the laws that govern evidence-gathering on the internet were written before the Information Revolution, and are now both hindering the flow of information to law enforcement and jeopardizing user privacy as a result.

and communities, and the expectations of privacy that internet users have in their communications.

Today, we're proposing a new framework that allows countries that commit to baseline privacy, human rights, and due process principles to gather evidence more quickly and efficiently. We believe these reforms would not only help law enforcement conduct more effective investigations but also encourage countries to improve and align on privacy and due process standards. Further, reducing the amount of time countries have to wait to gather evidence means would reduce the pressure to pursue more problematic ways of trying to gather data.

Current laws hinder law enforcement and user privacy

The U.S. Electronic Communications Privacy Act (ECPA) governs requests for content from law enforcement. Under ECPA, foreign countries largely have to rely on diplomatic mechanisms such as Mutual Legal Assistance Treaties (MLAT) to obtain content that is held by a company in the United States. The last data we've seen suggests that the average wait to receive content through the MLAT process is 10 months, far too long for most criminal cases. While law enforcement waits for this data, crimes could remain unsolved or a trial might happen missing key evidence.

The current legal framework poses a threat to users' privacy as well. Faced with the extended delays under the MLAT process, some countries are now asserting that their laws apply to companies and individuals outside of their borders. Countries asserting extraterritorial authority potentially put companies in an untenable situation where we risk violating either the law of the requesting country or the law of the country where we are headquartered.

We are also seeing various proposals to require companies to store data within local borders as a means to gain easier access. There are a host of problems with this: small, one-off data centers are easier targets for attackers and jeopardize

smaller companies.

The legal ambiguity concerning cross-border law enforcement requests has also created complications for law enforcement in the United States. Last year, the Second Circuit Court of Appeals was asked to determine the reach of ECPA search warrants issued under the now out-of-date statute. The Court ruled that under existing law, an ECPA search warrant cannot be used to compel service providers to disclose user data that is stored outside of the U.S. But even those judges agreed that ECPA should be updated by Congress to reflect the new reality of today's global networks.

Principles for reform

Our proposal to address these challenges for domestic and international law enforcement, for companies, and for users has two core principles:

First, countries that honor baseline principles of privacy, human rights, and due process should be able to make direct requests to service providers for user data that pertains to serious crimes that happen within their borders and users who are within their jurisdiction.

While the U.S. cannot solve the problem on its own, and many countries have blocking regulations, policy reform in the US is a necessary first step. We've been pleased to see serious debate around ways to update digital evidence laws in Washington on this issue.

In May, the U.S. Department of Justice presented legislation that would amend ECPA and authorize U.S. providers to disclose records and communications content to foreign governments that adhere to baseline due process, human rights, and privacy standards. This legislation would be the critical starting point for the new framework of direct requests.

enforcement requests for digital evidence should be based on the location and nationality of users, not the location of data. A key component of this reform is the International Communications Privacy Act (ICPA), which Google supports. ICPA provides a unique opportunity for Congress to update laws governing digital evidence both for investigations in the U.S. and abroad. While refinements to ICPA may be necessary, we believe the principles upon which ICPA is based are sound.

Second, provided that countries can meet baseline standards and the U.S. amends ECPA, the next step would be for the United States and foreign governments to sign new agreements that could provide an alternative to the MLAT process. The bilateral agreements that could be authorized by the legislation put forward by the Department of Justice provide a promising avenue to improve global privacy standards and create a pathway for foreign governments to obtain digital evidence for investigations.

We're ready to do our part

We know that this will be an involved process. It'll require action here in Washington and in capitals around the world. However, we can't accept the complexity of action as a reason for inaction in addressing an important and growing problem.

Our proposal asks for a lot of movement from governments. But we recognize our role as well. Google is ready to work with legislators, regulators, civil society, academics, and other companies to progress these proposals and make sure that we get this right. And I look forward to conversations that we'll have in Washington, D.C. and beyond in the months to come.

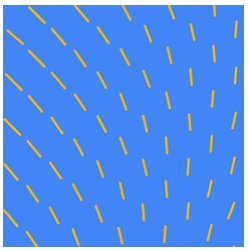
POSTED IN: PUBLIC POLICY

Up next

JUL 28 — PUBLIC POLICY

A significant step toward modernizing our surveillance laws

JUL 20 — GOOGLE IN EUROPE



Applications now open for the Google Policy Fellowship in Europe and Africa

Google policy fellowship programs launching in Europe and Africa

JUL 18 — PUBLIC POLICY

A new look for our Transparency Report

Today we're introducing the completely revamped Transparency Report, with clearer charts, more context for the data, a Recent Updates section, a better way to download data, and a fresh design.