

Britain's surveillance program could cut down on citizens' privacy

Published: Saturday, May 19, 2012, 7:45 AM



By **The Associated Press**

[Follow](#)



15 people recommend this. Be the first of your friends.

[Share](#)

[Email](#)

[Print](#)

[Tweet](#)

7

0

LONDON — British officials have given their word: "We won't read your emails."

But experts say the government's proposed new surveillance program will gather so much data that spooks won't have to read your messages to guess what you're up to.

The U.K. Home Office stresses it won't be reading the content of every Briton's communications, saying the data it seeks "is NOT the content of any communication."

It is, however, looking for information about who's sending the message and to whom, where it's sent from and other details, including a message's length and its format.

The proposal, unveiled last week as part of the government's annual legislative program, is just a draft bill, so it could be modified or scrapped. But if passed in its current form, it



AP Photo

The U.K. has proposed a new surveillance program that would put a huge amount of personal data at the government's disposal.

would put a huge amount of personal data at the government's disposal, which it could use to deduce a startling amount about Britons' private lives — from sleep patterns to driving habits or even infidelity.

"We're really entering a whole new phase of analysis based on the data that we can collect," said Gerald Kane, an information systems expert at Boston College. "There is quite a lot you can learn."

The ocean of information is hard to fathom. Britons generate 4 billion hours of voice calls and 130 billion text messages annually, according to industry figures. In 2008, the BBC put the annual number of U.K.-linked emails at around 1 trillion.

Then there are instant messaging services run by companies such as BlackBerry, Internet telephone services such as Skype, chat rooms, and in-game services like those used by World of Warcraft.

Communications service providers, who would log all that back-and-forth, believe the government's program would force them to process petabytes (1 quadrillion bytes) of information every day. It's a mind-boggling amount of data, on the scale of every book, movie and piece of music ever released.

So even without opening emails, how much can British spooks learn about who's sending them?

THEY'LL SEE THE RED FLAGS

Did you know how fast you were going?

Your phone does.

If you sent a text from London before stepping behind the wheel, and a second one from a service station outside Manchester three hours later, authorities could infer that you broke the speed limit to cover the roughly 200 miles that separate the two.

Crunching location data and communications patterns gives a remarkably rich view of people's lives — and their misadventures.

Ken Altshuler, of the American Academy of Matrimonial Lawyers, raves about the benefits smartphones and social media have brought to savvy divorce attorneys. Lawyers don't need sophisticated data mining software to spot evidence of infidelity or hints of hidden wealth when they review phone records or text traffic, he said.

"One name, one phone number that's not on our client's radar, and our curiosity is piqued," he said. The more the communication — a late-night text sent to a work colleague, an unexplained international phone call — is out of character, "the more of a red flag we see."

THEY'LL KNOW WHEN YOU'RE SLEEPING

The ebb and flow of electronic communication —that call to your mother just before bed, that early-morning email to your boss saying you'll be late — frames our waking lives.

"You can figure somebody's sleep patterns, their weekly pattern of work," said Tony Jebara, a Columbia University expert on artificial intelligence. In 2006, he helped found New York-based Sense Networks, which crunches phone data to do just that.

Jebara said that calls made from the same location from 9 to 5 are a good indication of where a person works; the frequency of email traffic to or from a person's work account is a good hint of his or her work ethic; dramatic changes to a person's electronic routine might suggest a promotion — or a layoff.

"You can quickly figure out when somebody lost their job," Jebara said, adding: "Credit card companies have been interested in that for a while."

THEY'LL KNOW WHO'S THE BOSS

Drill down, and communication can reveal remarkably rich information. For example, does office worker A answer office worker B's missives within minutes of the message being sent? Does B often leave colleagues' emails unanswered for hours on end? If so, B probably stands for "boss."

That's an example of what Jebara's Columbia colleagues call "automated social hierarchy detection," a technique that can infer who gives the orders, who's respected and who's ignored based purely on whose emails get answered and how quickly. In 2007, they analyzed traffic from the Enron Corporation's email archive to correctly guess the seniority of several top-level managers.

Intelligence agencies may not need such tools to untangle corporate flowcharts, but identifying ringleaders becomes more important when tracking a suspected terrorist cell.

"If you piece together the chain of influence, then you can find the central authority," he said. "You can figure that out without looking at the content."

THEY'LL KNOW WHO YOU'RE TALKING TO

Seeing how networks of people communicate isn't just about finding your boss. It's about figuring out who your friends are.

Programs already exist to determine the density of communications — something that can identify close groups of friends or family without even knowing who's who. If one user is identified as suspicious, then users closest to him or her might get a second look as well.

"Let's say we find out somebody in the U.K. is a terrorist," said Kane. "You know exactly who he talks to on almost every channel, so BOOM you know his 10 closest contacts. Knowing that information not only allows you to go to his house, but allows you to go to their houses as well."

A SNOOPER'S CHARTER?

Detective work at the stroke of a key is clearly attractive to spy agencies. British officialdom has been pushing for a mass surveillance program for years. But civil libertarians are perturbed, branding the proposal a "snooper's charter."

Kane says the surveillance regime has to be seen in the context of social networks such as Facebook and LinkedIn, where hundreds of millions of people are constantly volunteering information about themselves, their friends, their family and their colleagues.

"There's no sense in getting all Big Brother-ish," he said. "The bottom line is that we're all leaving digital trails, everywhere, all the time. The whole concept of privacy is shifting daily."