

UK surveillance could yield window into lives

May 18 2012, RAPHAEL SATTER , Associated Press



In this Friday, Sept. 23, 2011 file photo a man talks on a mobile phone as the hi-rise buildings of the banks based in the Canary Wharf business district are seen in the distance from Parliament Hill on Hampstead Heath in London. British officials have given their word: 'We won't read your emails.' But experts say that its proposed new surveillance program, unveiled last week as part of the government's annual legislative program, will gather so much data that spooks won't have to read your messages to guess what you're up to. (AP Photo/Matt Dunham)

(AP) -- British officials have given their word: "We won't read your emails."

But experts say that its proposed new surveillance program, unveiled last week as part of the government's annual legislative 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 that it is not seeking to read the content of every Britons' communications, saying the data it was seeking "is NOT the content of any communication." It is, however, seeking information on who's sending the message, whom it's sent to, where it's sent from, and potentially other details including a message's length and its format.

The government's proposal is just a draft bill, so it could be modified or scrapped. But if passed in its current form, it would put a huge amount of [personal data](#) at the government's disposal, which it could potentially use to deduce a startling amount about Britons' private life - 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 telephony services such as Skype, chat rooms, and in-game services liked those used by [World of Warcraft](#).

[Communications service](#) providers, who would log the details of all that back-and-forth, believe that the government's program would force them to process petabytes (1 quadrillion bytes) of information every day. It's a mind-bogglingly large amount of data on the scale of every book, every movie, and every 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

Do you know how fast you were going?

Your phone does.

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

Crunching location data and communications patterns gives a remarkable rich view of a person's lives - and their misadventures.

Ken Altshuler, of the American Academy of Matrimonial Lawyers, raves about the benefits which 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 HOW 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 machine learning

expert. 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 between 9 and 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 redundancy.

"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 described as "automated social hierarchy detection," a technique which 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 four of them analyzed traffic taken 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 are your friends.

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 the 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 the mass surveillance program for years, but civil libertarians are perturbed, branding the proposal a "snooper's charter."

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

"There's no sense in getting all Big Brother-ish that there are legitimate safeguards in place," 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."

©2012 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: UK surveillance could yield window into lives (2012, May 18) retrieved 24 April 2024 from <https://phys.org/news/2012-05-uk-surveillance-yield-window.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.