http://www.guardian.co.uk/commentisfree/2013/jan/24/google-ecpa-fbi-warrantless-email-snooping

Google's ECPA report reveals the extent of the FBI's warrantless email snooping

Guess who's reading your email? Thanks to a legal loophole that nixes your constitutional rights, the Feds can help themselves

Dominic Rushe

1/24/2013

Right now, as you read this, the US government may be snooping through your emails, looking at your photos, poring over your online life. Maybe, one day, there'll be a knock on your door.

More than likely, though, you'll never know that the Feds have been right through your inbox. This may sound like the paranoid fantasies of Big Government-hating Tea Party activists, but thanks to a 1986 law, your privacy means pretty much nothing to the Feds online.

Ronald Reagan signed off on the electronic communications privacy act (ECPA) in an early, and prescient, attempt to extend the fourth amendment's right to privacy in people's private communications to the electronic age. The bill was passed when only a handful of campus-dwelling computer geeks used email. Technology has moved on since; the ECPA has not.

This week, Google revealed that the US government made 8,438 requests for user data between July and December, up 136% from the last half of 2009 when the search firm started compiling data. More worryingly still, Google's Transparency Report revealed for the first time just how the US authorities go about collecting this information. In 68% of cases, the requests for information are made using ECPA subpoenas, which do not need a court order.

As anyone who has watched Law and Order will know, getting a wiretap for a phone line is a piece of work. The same goes for the letters in your mailbox, or the chance to rifle through your office draws. But the vast majority of ECPA investigations go ahead without a court hearing. The government needs to show only that it has "reasonable grounds" to believe the information would be useful in an investigation.

As the law stands, we are in the bizarre situation where the J Crew catalogue in your mailbox has more legal protection than the email from your accountant or the medical notifications from your health insurer in your electronic inbox. Part of the reason for this is a change in technology. When the act was drawn up, email stored on a server for more than 180 days was considered "abandoned", allowing the government to get at it without a warrant. But back then, email – what little there was of it – was downloaded from the server and stored on the consumer's hard drive.

We live in a different world today. In 1990, the number of households owning a computer was 15%; last year, 81% of US households had a computer and, according to a Pew report, 45% of adults and two-thirds of young adults owned smart phones. All those people are storing their email in "the cloud", often for a lot longer than 180 days.

We file our taxes online, get divorced, start dating, find new jobs, bitch and gossip about our current ones. Our inboxes are a treasure trove of our most personal information. More and more people use cloud services to store their documents, their photos. Information we used to think of as private is commonly posted on Facebook.

Search histories are a depository of our deepest fears. From the personal (body weight, hair loss, children's drug habits, infidelity) to the political (your views about the environmental impact of that local chemicals factory, Obama's plans for gun control), Google knows what you are thinking.

Thanks to its origins and some legal challenges, the ECPA is now a confusing mess when it comes to the government's right to access this information. What is certain is that, says Chris Calabrese, legislative counsel for privacy-related issues in the American Civil Liberties Union (ACLU):

"People don't know how little their rights are being protected online."

The fourth amendment is anything but muddled on the issue:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

I doubt the founding fathers would have approved of unwarranted government snooping. And yet, the shadow of 9/11 continues to erode our right to privacy, while the Obama administration has shown little interest in reforming the ECPA for the digital age.

Democratic Senator Patrick Leahy has been campaigning for the ECPA to be reformed for a number of years and is set to make another push this year. He has the support of the ACLU and digital rights organisations, including the Electronic Frontier Foundation and Fight For the Future. Even tax reformer Grover Norquist, no woolly liberal he, has called for change.

But so far, the demands of law enforcement have trumped privacy. The last time reform of the bill got a full airing was 2011, when James Baker, the associate deputy attorney general, was quick to tell a Senate committee about the risks of reform:

"Speed is essential. If Congress slows down the process, this would have real-life consequences, particularly where human life is involved."

There are signs of change. The Senate judiciary committee passed Leahy's proposals to eliminate the 180 day rule late last year. It was the first time since 9/11 that Congress had acted on a privacy bill that *protected* people's rights, rather than took them away.

It's just a first step: far more needs to be done before the proposal becomes legislation. In the meantime, if you really want to keep something private, commit it to paper and use snail-mail.