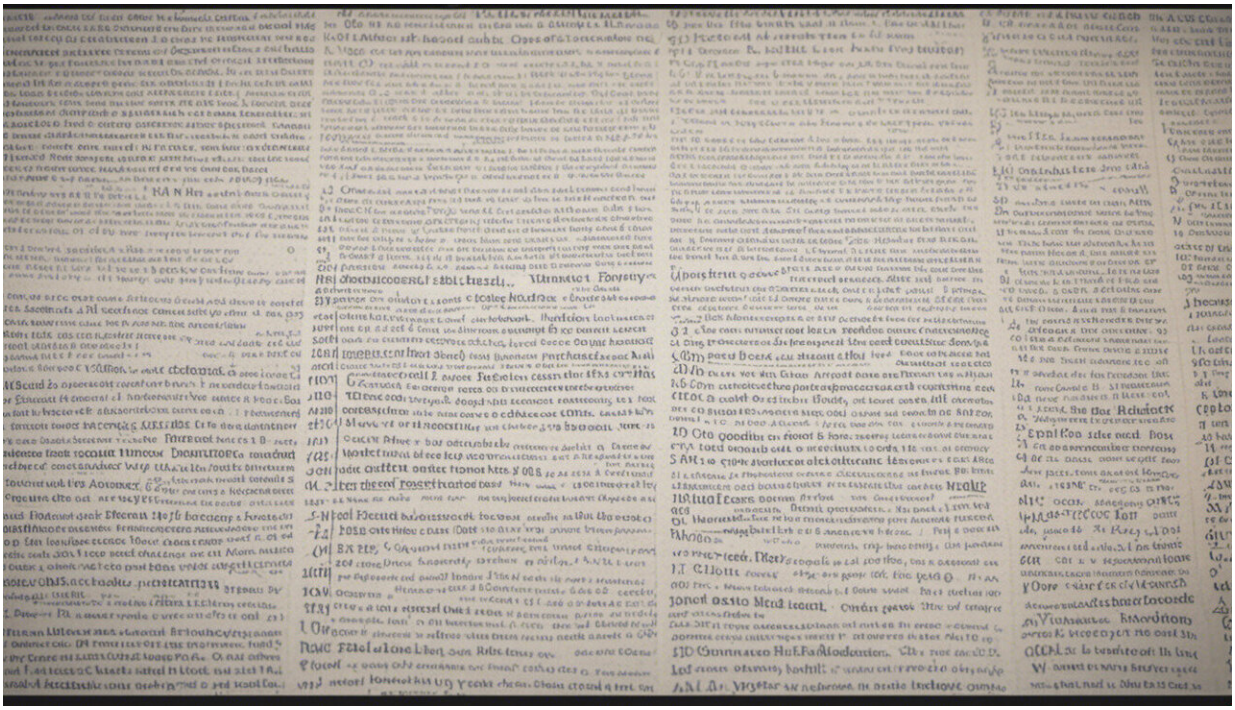
Feds can read all your email, and you'll never know

September 22 2016, by Clark D. Cunningham



Credit: AI-generated image (disclaimer)

Fear of hackers reading private emails in cloud-based systems like Microsoft Outlook, Gmail or Yahoo has recently sent regular people and public officials scrambling to delete entire accounts full of messages dating back years. What we don't expect is our own government to hack our email – but it's happening. Federal court cases going on right now

are revealing that federal officials can read all your email without your knowledge.

As a scholar and lawyer who started researching and writing about the history and meaning of the Fourth Amendment to the Constitution more than 30 years ago, I immediately saw how the FBI versus Apple controversy earlier this year was bringing the founders' fight for liberty into the 21st century. My study of that legal battle caused me to dig into the federal government's actual practices for getting email from cloud accounts and cellphones, causing me to worry that our basic liberties are threatened.

A new type of government search

The federal government is getting access to the contents of entire email accounts by using an ancient procedure – the search warrant – with a new, sinister twist: secret court proceedings.

The earliest search warrants had a very limited purpose – authorizing entry to private premises to find and recover stolen goods. During the era of the American Revolution, British authorities abused this power to conduct dragnet searches of colonial homes and to seize people's private papers looking for evidence of political resistance.

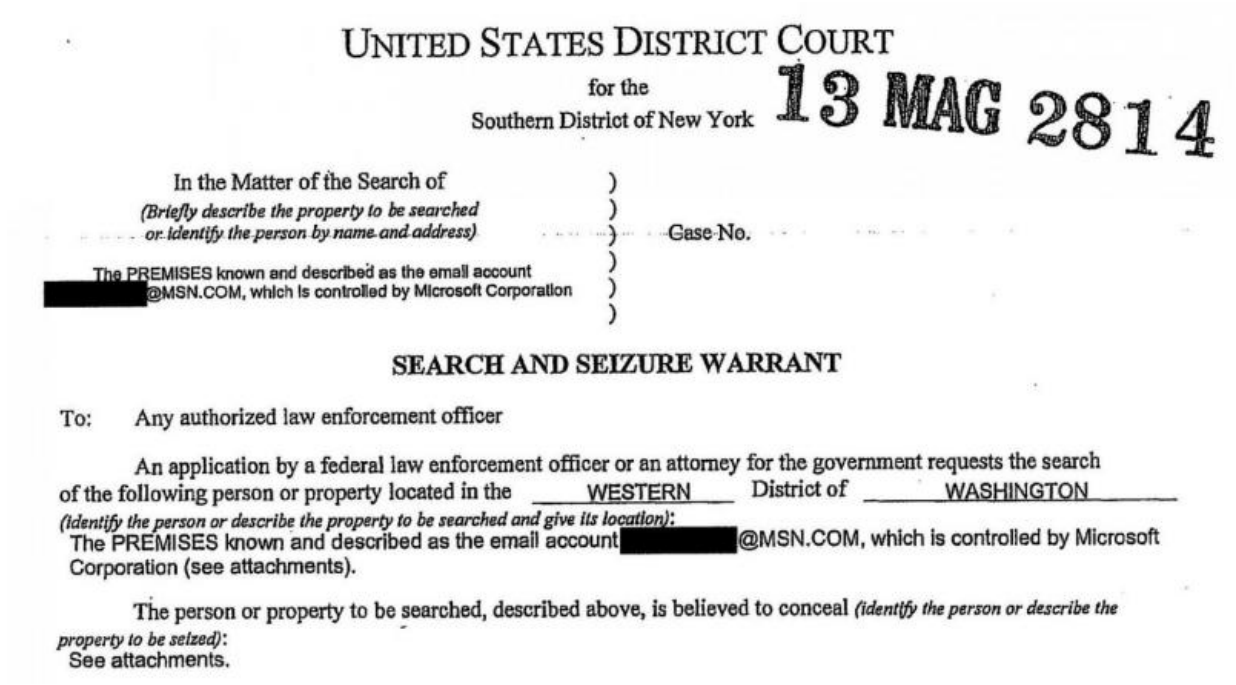
To prevent the new federal government from engaging in that sort of tyranny, special controls over search warrants were written into the Fourth Amendment to the Constitution. But these constitutional provisions are failing to protect our personal documents if they are stored in the cloud or on our smartphones.

Fortunately, the government's efforts are finally being made public, thanks to legal battles taken up by Apple, Microsoft and other major companies. But the feds are fighting back, using even more subversive

legal tactics.

Searching in secret

To get these warrants in the first place, the feds are using the Electronic Communications Privacy Act, passed in 1986 – long before widespread use of cloud-based email and smartphones. That law allows the government to use a warrant to get electronic communications from the company providing the service – rather than the true owner of the email account, the person who uses it.



UNITED STATES DISTRICT COURT

for the

Southern District of New York

13 MAG 2814

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

This search warrant clearly spells out who the government thinks controls email accounts – the provider, not the user. Credit: U.S. District Court for the Southern District of New York

And the government then usually asks that the warrant be "sealed," which means it won't appear in public court records and will be hidden from you. Even worse, the law lets the government get what is called a "gag order," a court ruling preventing the company from telling you it got a warrant for your email.

You might never know that the government has been reading all of your email – or you might find out when you get charged with a crime based on your messages.

Microsoft steps up

Much was written about Apple's successful fight earlier this year to prevent the FBI from forcing the company to break the iPhone's security system.

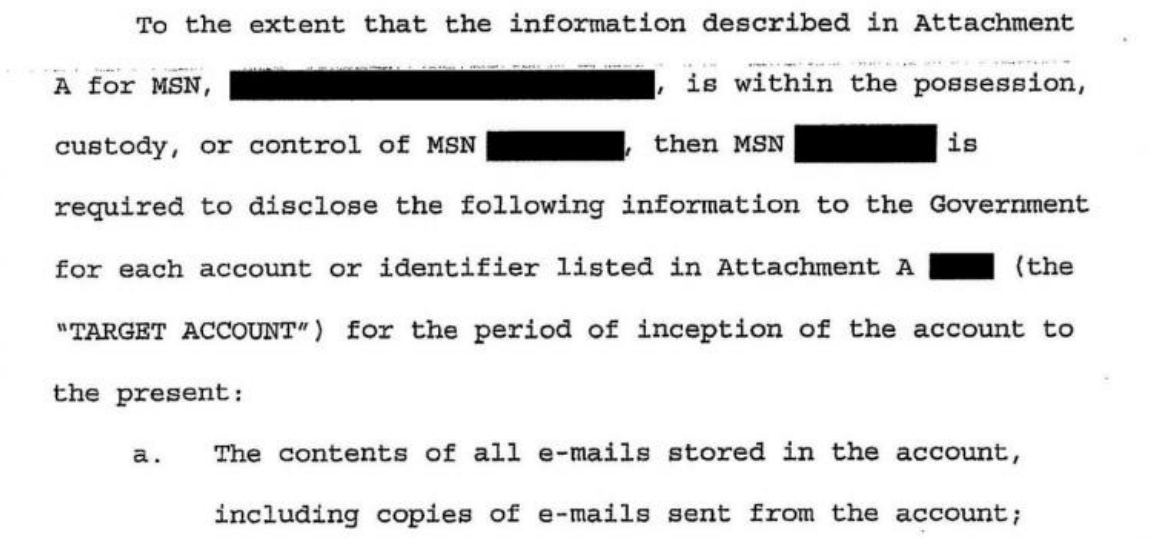
But relatively little notice has come to a similar Microsoft effort on behalf of customers that began in April 2016. The company's suit argued that search warrants delivered to Microsoft for customers' emails are violating regular people's constitutional rights. (It also argued that being gagged violates Microsoft's own First Amendment rights.)

Microsoft's suit, filed in Seattle, says that over the course of 20 months in 2015 and 2016, it received more than 3,000 gag orders – and that more than two-thirds of the gag orders were effectively permanent, because they did not include end dates. Court documents supporting Microsoft describe thousands more gag orders issued against Google, Yahoo, Twitter and other companies. Remarkably, three former chief federal prosecutors, who collectively had authority for the Seattle region for every year from 1989 to 2009, and the retired head of the FBI's Seattle office have also joined forces to support Microsoft's position.

The feds get everything

It's very difficult to get a copy of one of these search warrants, thanks to orders sealing files and gagging companies. But in another Microsoft lawsuit against the government a redacted warrant was made part of the court record. It shows how the government asks for – and receives – the power to look at all of a person's email.

On the first page of the warrant, the cloud-based email account is clearly treated as "premises" controlled by Microsoft, not by the email account's owner:



To the extent that the information described in Attachment A for MSN, [redacted], is within the possession, custody, or control of MSN [redacted], then MSN [redacted] is required to disclose the following information to the Government for each account or identifier listed in Attachment A [redacted] (the "TARGET ACCOUNT") for the period of inception of the account to the present:

a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;

The warrant orders Microsoft to turn over every email in an account – including every sent message. Credit: U.S. District Court for the Southern District of New York

"An application by a federal law enforcement officer or an attorney for

the government requests the search of the following … property located in the Western District of Washington, the premises known and described as the email account [REDACTED]@MSN.COM, which is controlled by Microsoft Corporation."

The Fourth Amendment requires that a search warrant must "particularly describe the things to be seized" and there must be "probable cause" based on sworn testimony that those particular things are evidence of a crime. But this warrant orders Microsoft to turn over "the contents of **all** e-mails stored in the account, including copies of e-mails sent from the account." From the day the account was opened to the date of the warrant, everything must be handed over to the feds.

Reading all of it

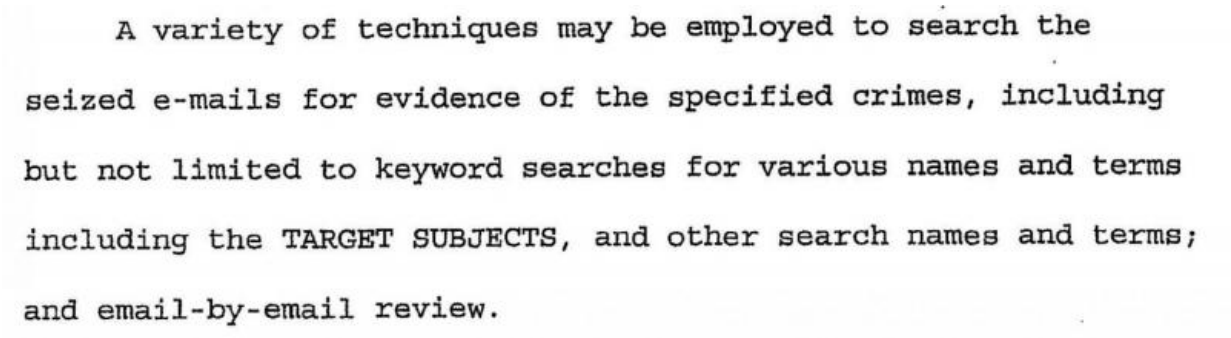
In warrants like this, the government is deliberately not limiting itself to the constitutionally required "particular description" of the messages it's looking for. To get away with this, it tells judges that incriminating emails can be hard to find – maybe even hidden with misleading names, dates and file attachments – so their computer forensic experts need access to the whole data base to work their magic.

If the government were serious about obeying the Constitution, when it asks for an entire email account, at least it would write into the warrant limits on its forensic analysis so only emails that are evidence of a crime could be viewed. But this Microsoft warrant says an unspecified "variety of techniques may be employed to search the seized emails," including "email by email review."

As I explain in a forthcoming paper, there is good reason to suspect this type of warrant is the government's usual approach, not an exception.

Former federal computer-crimes prosecutor Paul Ohm says almost every

federal computer search warrant lacks the required particularity. Another former prosecutor, Orin Kerr, who wrote the first edition of the federal manual on searching computers, agrees: "Everything can be seized. Everything can be searched." Even some federal judges are calling attention to the problem, putting into print their objections to signing such warrants – but unfortunately most judges seem all too willing to go along.



A variety of techniques may be employed to search the seized e-mails for evidence of the specified crimes, including but not limited to keyword searches for various names and terms including the TARGET SUBJECTS, and other search names and terms; and email-by-email review.

The right to read every email. Credit: U.S. District Court for the Southern District of New York

What happens next

If Microsoft wins, then citizens will have the chance to see these search warrants and challenge the ways they violate the Constitution. But the government has come up with a clever – and sinister – argument for throwing the case out of court before it even gets started.

The government has asked the judge in the case to rule that Microsoft has no legal right to raise the Constitutional rights of its customers. Anticipating this move, the American Civil Liberties Union asked to join the lawsuit, saying it uses Outlook and wants notice if Microsoft

were served with a warrant for its email.

The government's response? The ACLU has no right to sue because it can't prove that there has been or will be a search warrant for its email. Of course the point of the lawsuit is to protect citizens who can't prove they are subject to a search warrant because of the secrecy of the whole process. The government's position is that no one in America has the legal right to challenge the way prosecutors are using this law.

Far from the only risk

The government is taking a similar approch to smartphone data.

For example, in the case of U.S. v. Ravelo, pending in Newark, New Jersey, the government used a search warrant to download the entire contents of a lawyer's personal cellphone – more than 90,000 items including text messages, emails, contact lists and photos. When the phone's owner complained to a judge, the government argued it could look at everything (except for privileged lawyer-client communications) before the court even issued a ruling.

The federal prosecutor for New Jersey, Paul Fishman, has gone even farther, telling the judge that once the government has cloned the cellphone it gets to keep the copies it has of all 90,000 items even if the judge rules that the cellphone search violated the Constitution.

Where does this all leave us now? The judge in Ravelo is expected to issue a preliminary ruling on the feds' arguments sometime in October. The government will be filing a final brief on its motion to dismiss the Microsoft case September 23. All Americans should be watching carefully to what happens next in these cases – the government may be already watching you without your knowledge.

This article was originally published on The Conversation. Read the original article.

Source: The Conversation