How To Protect Your Social Media Data From Government Interception

0

Kevin Wells • August 2, 2016 • Internet Security

1

Social media sites such as Facebook, Twitter and Google Plus are extremely popular. It's estimated over a billion people use social media every day as a convenient way to communicate with others.

Social media is accessible, easy to use and in most cases free. We take it for granted that we can use social media to share posts, images, information, news and personal data with each other.

Yet social media is also a very useful source of data for many other people beyond your own circle of friends and acquaintances.

Social media is a marketing specialist's dream come true. It's also one of the first sources law enforcement agencies turn to when they're investigating a suspect or potential suspect. Government and law enforcement agencies now routinely access Facebook and other social networks when investigating criminal activity.

The rich potential of social media as a source of information about citizens also hasn't gone ignored by state intelligence authorities such as the Department of Homeland Security and the CIA.

The surveillance disclosures of Edward Snowden and others reported by The Guardian and Washington Post in 2013 identified social media as key assets in the U.S. National Security Administration's PRISM intelligence program.

Why Government Use of Social Media Monitoring Software is a Threat to Our Online Privacy

Of course, social media by its very nature is a form of open media.

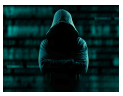
Latest articles


How to Use a VPN to Watch the 2016 Summer Olympics
Guides • no comments


The Threat of Social Hacking: Information and Defenses
Feature Articles • no comments


How To Protect Your Social Media Data From Government Interception
Internet Security • no comments


ExpressVPN the VPN for you? Our Review
Reviews • 17 comments


Know Your Enemy: Why Cybercriminals Do What They Do
Feature Articles • no comments

Recommended topics

- Internet Security
- Protect Your Information
- Phone and Tablet Security
- Protecting Your Children

Yet the American Civil Liberties Union (ACLU) has expressed concern about the increasing use by government agencies of a new and powerful surveillance tool called **Social Media Monitoring Software (SMMS).**

SMMS is an advanced online software tool which goes way beyond simple Google keyword searches. Originally developed as a marketing tool to help businesses identify potential customers, SMMS can be used to intensively monitor and analyze social media data.

But SMMS can also be deployed by governments as a tool for surveillance and intelligence to forecast future events, threats from individuals and groups, and even public opinion.

The CIA recognizes the importance of SMMS and now runs a venture capital fund called **In-Q-Tel**, specifically to invest in companies developing SMMS technology such as Geofeedia, Beware, SocioSpyder and Dataminr.

The Dangers of Social Media Monitoring Software for Our Liberty

The **ACLU recently reported that US law enforcement agencies are using SMMS** to keep tabs on "Black Lives Matter" activists.

Police monitoring of social media has been practiced for several years and the practice may not violate existing privacy laws. However, the sophisticated monitoring capabilities of SMMS take surveillance to a new level and raises many privacy concerns.

SMMS can trigger false alarms and incriminate innocent people. It can also lead to people being intimidated into practicing a form of self-censorship to avoid being flagged by social media monitoring systems.

For example, not tweeting or posting to social media about an issue or not attending a demonstration. It opens the potential for innocent people to be placed under suspicion without actual evidence of any wrongdoing.

How to Protect Your Social Media from SMMS

So how should we respond to the use of SMMS?

SMMS has serious implications for our freedoms. SMMS by itself is not a reliable indicator of wrongdoing and it shouldn't be regarded as such.

The **Electronic Frontier Foundation (EFF)** provides a useful Surveillance Self Defense Pack containing practical tips on how to protect your privacy on social networks.

There are a number of aspects you should pay attention to concerning your online data security when using social media.

Ask yourself who you want to allow access to your social media. Social media sites usually allow you to set the level of privacy for your account.

Don't forget Facebook and other social media operators often change their policies which means the effectiveness of your settings can change. So you need to regularly re-check your social media privacy settings.

Social media often permit you to login to third party sites using your social media account. While this is convenient for you, it comes at a risk. If your social media password gets intercepted, then all other sites that rely on this connection can also be compromised.

Using real data in your personal profile is always a security risk. Do you really need or want to use your real name, address, date of birth, phone number and email address for your social media? Do you have to use a full face photo on your social media accounts? You can an avatar if you prefer.

And what about the details of your interests, relationships, work, career and education? Where you've lived in the past? How much of this information do you want made public?

Check out the **practical advice for keeping your social media secure** provided by the **National Cyber Security Alliance** on their website.

The only sure way to fully protect yourself against digital surveillance is not to use any digital media or services anywhere at any time. But for nearly all of us nowadays that's practically impossible.

Another problem is that SMMS is extremely powerful surveillance technology. In that sense it's a bit like a

nuclear weapon. Once launched, there's not much you can do to intercept it.

Demand Accountability from the Government on the Use of SMMS

The best defense against blanket use of SMMS is awareness and prevention at the political level.

Insist that lawmakers and your representatives fully respect our civil rights about the indiscriminate use of SMMS.

Demand that government agencies regularly report back to the public about how SMMS is being used. You have a right to know whether this technology is achieving its public security purpose without encroaching on your privacy and liberty.

This is important because once freedoms and digital privacy are ceded, the new restricted state of affairs becomes the new norm and it can be all the harder to recover them.

One organization in the forefront of campaigning for the protection of digital freedoms is the **Electronic Frontier Foundation (EFF)**. You can find out more about the EFF and how to join and support their campaigns at www.eff.org

Like nuclear weapons, SMMS can't be wished away. Yet we can demand that our lawmakers restrict and control its usage by intelligence agencies.

What's your view on the use of SMMS technology by government? We're interested to hear your opinion on how we can best protect ourselves from the misuse of SMMS. Add your comments to the discussion below.

1

RELATED ARTICLES

The Best VPN for Dubai Of 2016

3 Best VPN's For Apple Mac Computers

3 Best VPNs for Australia

We will be happy to hear your thoughts

Latest Articles

How to Use a VPN to Watch the 2016 Summer Olympics

Feature Guides

Secure Thoughts is the industry leader in helping everyday people make sure their information and loved ones are protected online.

Your future and the future of those you love is too important to gamble with.

When you need the right advice, trust Secure Thoughts.