

Able To 'Tap' Skype, Facebook and BlackBerry Emails

It appears that law enforcement officers are finding it too difficult to track the Facebook messages going back and forth between drug dealers. Charlie Savage at the [New York Times](#) reports today that “federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is ‘going dark’ as people increasingly communicate online instead of by telephone.”

It may be shocking to many to hear that the po-po are facing more obstacles from Facebook and Skype than from disposable cell phones. But the FBI, NSA, Justice Department and other agencies are feeling stymied and are hoping that a bill will be passed next year to enhance their ability to dip their hands into digital communications in real time...

Essentially, officials want Congress to require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct “peer to peer” messaging like Skype — to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.

via [U.S. Wants to Make It Easier to Wiretap the Internet – NYTimes.com](#).

Research in Motion is still resolving [threatened bans](#) by the Indian and United Arab Emirates governments over their inability to monitor encrypted email sent by BlackBerrys. We'll see how it stands up against this U.S. request.

Declan McCullagh at [CNet](#) wrote about the police desire to conduct online investigations more efficiently a few months back, explaining that



42

Share

16 tweets

retweet

Res
the



MY A

Show a

K

K

L

C

K

L

A

E

K

F

E

by

law enforcement wants a private Web interface to make interception of electronic messages easier. Maybe we can call it PoliceBook.com?

The police already have a very cozy relationship with the phone companies, thanks to the 1994 Communications Assistance to Law Enforcement Act. To comply with that act, Sprint Nextel has already created a [private interface for law enforcement](#). Sometimes the relationship is too cozy, as I've [mentioned here before](#); a Department of Justice investigation determined that law enforcement officers were too easily getting phone records from Verizon and AT&T — sometimes by just handing a phone employee a post-it note.

Julian Sanchez of the Cato Institute has previously pointed out that a downside to creating an easy access key for the feds, is that an easy access key then exists and can be stolen by hackers. Check out his piece for The Nation [here](#).

For now, enjoy the fact that your Facebook communications are relatively private when it comes to law enforcement monitoring, so you can poke people as you please without worrying too much about the police watching.

[U.S. Wants to Make It Easier to Wiretap the Internet \[New York Times\]](#)

[Police want backdoor to Web users' private data \[CNet\]](#)

[Surveillance Can't Make Us Secure \[The Nation\]](#)

Recommend



Buzz Up!



Reddit



StumbleUpon



Facebook



Twitter



Email this

Previous Post:

[Facebook Engineer Discussed
'Hypothetical' Outage Last Week](#)

More on Forbes Right Now

LIVE STREAMS ▶

Related streams

Tech