

Army of Fake Social Media Friends to Promote Propaganda

By [Darlene Storm](#)

Theme: [Intelligence](#), [Media Disinformation](#)

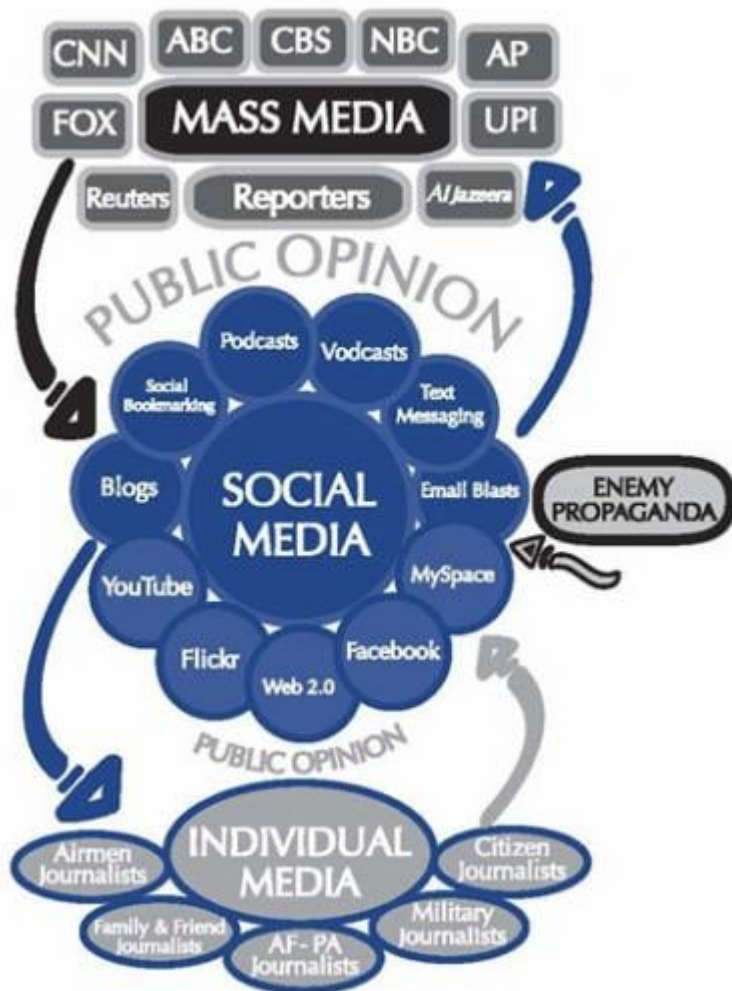
Global Research, February 28, 2011

[Computerworld](#) 22 February 2011

It's recently been revealed that the U.S. government contracted HBGary Federal for the development of software which could create multiple fake social media profiles to manipulate and sway public opinion on controversial issues by promoting propaganda. It could also be used as surveillance to find public opinions with points of view the powers-that-be didn't like. It could then potentially have their "fake" people run smear campaigns against those "real" people. As disturbing as this is, it's not really new for U.S. intelligence or private intelligence firms to do the dirty work behind closed doors.

[EFF previously warned that Big Brother wants to be your friend](#) for social media surveillance. While the [FBI Intelligence Information Report Handbook](#) (PDF) mentioned using "covert accounts" to access protected information, other government agencies endorsed using [security exploits](#) to access protected information.

It's not a big surprise that the U.S. military also wants to use social media to its benefit. Last year, Public Intelligence published the [U.S. Air Force social media guide](#) which gave 10 tips for social media such as, "The enemy is engaged in this battlespace and you must engage there as well." Number three was "DON'T LIE. Credibility is critical, without it, no one cares what you have to say...it's also punishable by the UCMJ to give a false statement." The Air Force used the chart below to show how social media influences public opinion.



The 6th Contracting Squadron at MacDill Air Force Base sought the development of [Persona Management Software](#) which could be used for creating and managing fake profiles on social media sites to distort the truth and make it appear as if there was a generally accepted agreement on controversial issues. “Personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms.” What happened to don’t lie and the Uniform Code of Military Justice?

Everything revealed after Anonymous leaked emails from private security firm [HBGary](#) Federal is disturbing on many levels. However, the [Daily Kos said](#) with the Persona Management Software it would take very few people to create “an army of sockpuppets” which could distort the truth while appearing to be “an entire Brooks Brothers riot online.”

So again I ask, what happened to number three . . . the rule about not lying that was also “punishable by the [UCMJ](#) to give a false statement”?

President and CEO of Plessas Experts Network, Inc, [Kirby Plessas pointed out](#) some of the unethical and potentially illegal activities that Aaron Barr’s leaked emails suggested like “Chumming and baiting” which sounded like “entrapment of some sort.” There would be no warrant for the data collected on individuals which could then be stored for how long? “THIS is the entire reason Intelligence Oversight was created – to avoid this sort of thing from ever happening again.”

[According to Redacted News](#), the leaked emails showed how names can be cross-referenced

across social media sites to collect information on people and then used to gain access to those social circles. The emails also talked of how Facebook could be used to spread government messages:

Even the most restrictive and security conscious of persons can be exploited. Through the targeting and information reconnaissance phase, a person's hometown and high school will be revealed. An adversary can create a classmates.com account at the same high school and year and find out people you went to high school with that do not have Facebook accounts, then create the account and send a friend request.

Under the mutual friend decision, which is where most people can be exploited, an adversary can look at a targets friend list if it is exposed and find a targets most socially promiscuous friends, the ones that have over 300-500 friends, friend them to develop mutual friends before sending a friend request to the target. To that end friend's accounts can be compromised and used to post malicious material to a targets wall. When choosing to participate in social media an individual is only as protected as his/her weakest friend.

Lots of people have multiple online aliases, Facebook or Twitter accounts for both business and private life. What most bothers me is the lying and seemingly unethical means to an end. Although the government says it doesn't approve of censorship, etc, when its [secrets come to light](#), it seems to be Okay with recommending underhanded tactics.

Secretary Clinton [delivered](#) a speech called, "Internet Rights and Wrongs: Choices and Challenges In A Networked World." To help promote and support Internet freedom, the State Department intends to award \$25 million in grants. While that is great news, the [EFF reported](#), "For every strong statement about preserving liberty, freedom of expression, and privacy on the global Internet, there exists a countervailing example of the United States attempting to undermine those same values."

[Secretary Clinton later told](#) "This Week" anchor Christiane Amanpour that most Americans "are in favor of human rights, freedom, democracy. We know that ultimately the most progress that can be made on behalf of human beings anywhere is when those individuals are empowered, when they have governments that are responsive." Clinton added, "At the same time, we recognize that this process can be hijacked. It can be hijacked by both outside and inside elements within any country."

So while the U.S. government can talk a good talk, what it does and what it says often doesn't seem to jive. Gasp, I know, it's not a big shocker but sometimes I find that utterly frustrating. The President wanted an Internet Kill Switch, the FBI keeps pushing for backdoors on all-things-Net. What happened to a code of ethics? Does it disappear behind closed doors, dirty deeds done in the dark and used against the American people who are supposed to be free to express themselves?

The original source of this article is [Computerworld](#)
Copyright © [Darlene Storm](#), [Computerworld](#), 2011

[Comment on Global Research Articles on our Facebook page](#)

Become a Member of Global Research

Articles by: **Darlene Storm**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca