CHICAGO POLICE DEPARTMENT

# PAX 501

Garry F. McCarthy, *Superintendent of Police*

**VOLUME 12** **01 June 2012** **NUMBER 6**

There have been several recent incidents in the wake of the NATO Summit in which Department members' personal information has been made public. In the most serious occurrence, an anonymous phone call threat was made to the family member of an officer as the result of personal information that was obtained about the Department member.

While we continue to investigate this outrageous incident, it serves as an urgent reminder that we as law enforcement officers must take every precaution to ensure our personal information is safeguarded and our privacy, particularly our online privacy, is protected.

The use of social media has grown at a dynamic rate in recent years. Many law enforcement officers have kept apace with this trend, participating on sites such as Facebook and Twitter. Social media sites are communities just as real as the neighborhoods we patrol every day; there are victims, offenders, and crimes in these venues. As a matter of officer safety, we must be cognizant that social media sites may share personal information with outside parties that can make an officer susceptible to a security breach.

The same discretion and responsibility we bring to our law enforcement duties will go a long way in ensuring an officer's personal information is not violated while using social media. Maintaining online connections with only the people you know and trust, and being mindful of the messages and photos you post and share, are advisable for social networking.

Privacy settings also can be customized to limit the personal information that is accessible from various social media sites. It is recommended that members enable the highest level possible to minimize the extent of private data that can be obtained by a third party. Encourage family members who maintain social media profiles to take similar precautions, as privacy gaps at these accounts may unknowingly reveal your personal information as well.

Technological advances, such as GPS and facial recognition applications, further expose what can be learned about members who utilize social media and other websites on computers or smart phones. Extra measures, such as deactivating data and opting out of databases that compile and retain personal information tracked from online user activity, insure against risks that might compromise an officer's security.

Our line of work means we are the police 24 hours a day. For your safety, review Information Bulletin #2012-INF-047 from the Crime Control Strategies Deployment Operations Center for guidance on how to protect yourself in the unique ways demanded of us by current trends. As always, keep up the great work and stay safe out there.

Garry F. McCarthy
Superintendent of Police