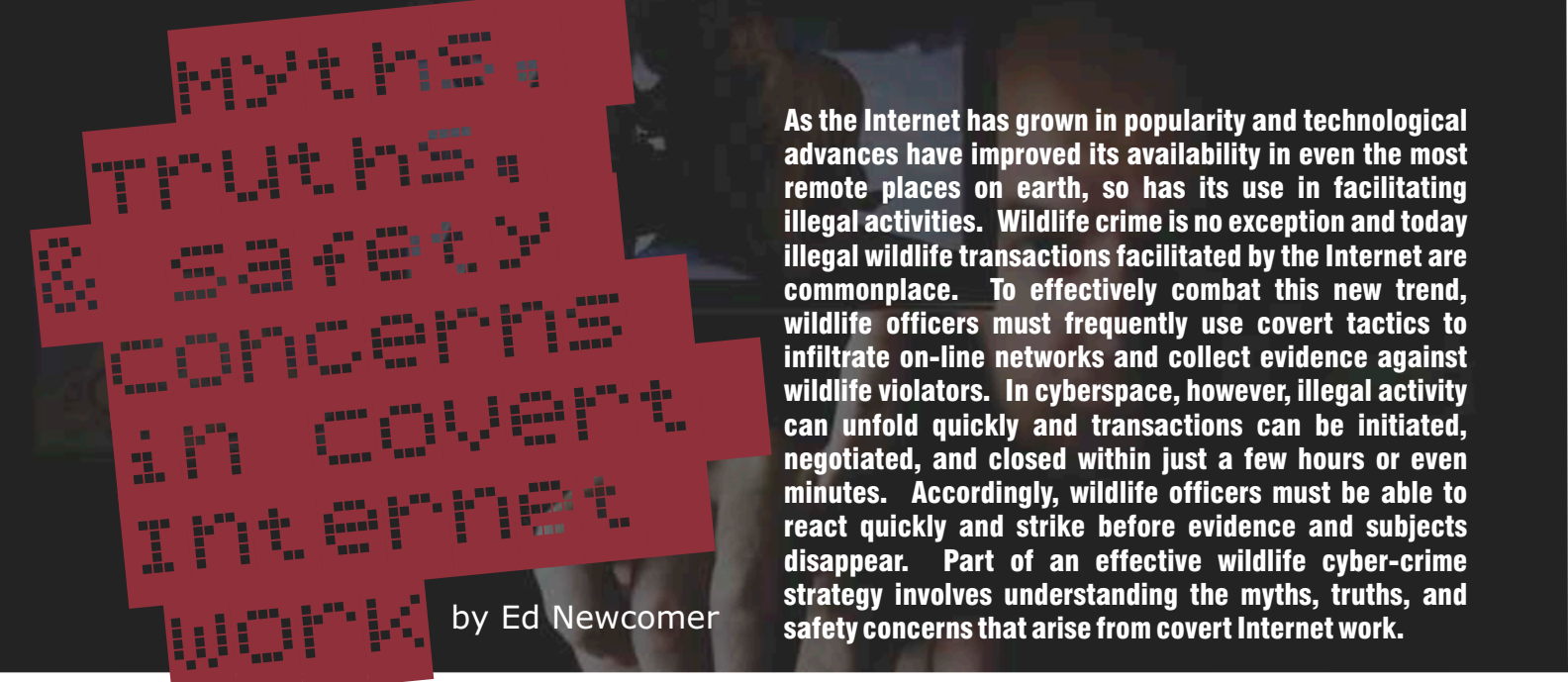

Myths, Truths & Safety Concerns in Covert Internet Work

by Ed Newcomer

As the Internet has grown in popularity and technological advances have improved its availability in even the most remote places on earth, so has its use in facilitating illegal activities. Wildlife crime is no exception and today illegal wildlife transactions facilitated by the Internet are commonplace. To effectively combat this new trend, wildlife officers must frequently use covert tactics to infiltrate on-line networks and collect evidence against wildlife violators. In cyberspace, however, illegal activity can unfold quickly and transactions can be initiated, negotiated, and closed within just a few hours or even minutes. Accordingly, wildlife officers must be able to react quickly and strike before evidence and subjects disappear. Part of an effective wildlife cyber-crime strategy involves understanding the myths, truths, and safety concerns that arise from covert Internet work.

The Safety Concerns:

You have probably been cautioned about not using government owned computers or computers connected to the Internet through government servers for covert Internet work. Generally, it's good advice. The concern, of course, is that a cyber-criminal will be able to use your IP address or your computer registration information to identify you as a law enforcement officer. This could compromise your case and even your personal safety.

However, purchasing cold computers and cold high speed Internet services can be expensive and complicated since it normally has to be done outside the usual bill paying methods used by the government. Bureaucratic necessities can make it difficult to get approval or can delay the purchase and installation of appropriate undercover equipment. In this article, I'll discuss what I believe are some of the myths about using government computers to do undercover work over the Internet and how I have attempted to verify my opinions.

A True Story:

In 1989, when computers were quickly gaining a foothold in American business and public use of the Internet was in its infancy, we started to hear news stories about viruses spreading to computer hard drives through floppy drives. The regional supervisor of the private company I worked for at the time held an office-wide meeting where he announced that we should be sure to keep all desktop computers in separate rooms and never place them next to each other for any reason. By doing this, he was confident we could avoid the transmission of any computer viruses. It's funny now but at the time he was very serious and there were more than a few people in the room who thought it was a reasonable precaution to take. Because so many people are unfamiliar with the technical workings of a computer, its software, and Internet connections, it is easy for half-truths and myths to be spread, grow, and become more credible with every telling.

Separating Myth from Reality:

1. Using your government computer or government Internet server to covertly visit a suspect website = High Risk

Concerns over this are no myth. This is where your IP address or your computer's registration information can burn your undercover identity. Assume you suspect a website of illegally selling protected wildlife and you want to look at the website to see what they're selling. You use your government computer and government Internet server to log onto www.illegalwildlife.com. Using simple tools, the owner of the website will be able to see that someone at your agency accessed his website and he will be able to see exactly what pages and items were looked at. Or, let's suppose that you log onto a suspect's website and then use a function built into the website to send a message or e-mail to the owner of the website or someone else through the website. There's a very good chance that the owners of the website will be able to identify you as a government agent through your IP address and, possibly, through your computer registration information.

2. Using your government computer or government Internet server to send e-mails to a suspect through a third party e-mail provider = Low Risk / No Risk

It's a myth that your identity will be easily compromised if you do this. Many law enforcement officers and their supervisors are overly concerned about this and tend to say, "Well, I'm not really sure so we're just going to use cold computers and Internet connections for everything." Generally, you can't ever go wrong being overly cautious but, at the same time, a blanket approach limits an undercover officer's speed, flexibility and creativity. Plus, depending on how your office is set up, you may not have the luxury of having a cold computer and cold Internet connection set up just for your case or at your desk. You may have to go to another physical location to use a cold computer and Internet connection and you may have to share that computer and line with other officers.

In the reality of day-to-day contacts with suspects, it just might not be feasible to always use a cold computer and connections. As long as you are using a reputable third party e-mail provider, it is safe to send covert e-mails. For example, if I log into the covert e-mail account I previously set up at www.yahoo.com, I am using the Yahoo owned computer servers to send e-mail through the Internet. My e-mail will be addressed to the suspect and when I click "send", it will be sent to a main Yahoo server before it is sent through the Internet to the suspect. If the suspect attempts to trace the source of the e-mail, the closest he can get to me will be a Yahoo server most likely located in the state or geographic region where I'm located. I have taken many steps to verify this information

and to test my security on this issue. If you have any concerns, you can do the same. I contacted several people familiar with computers and Internet security and told them that I would be sending them a series of e-mails from a Yahoo account name. I told them that one or more of the e-mails would be sent from my government computer connected to a government Internet server. I challenged them to tell me which were sent from the government equipment. No one could. The closest they could come was to tell me that my e-mail originated from a Yahoo server in Southern California. One important caveat is that you should be careful about downloading any attachments sent to you via e-mail from a suspect. Attachments can carry viruses or Trojan horse programs that could send information about your computer back to the suspect. Accordingly, they should be isolated and scanned prior to opening them.

3. Using a government computer or government Internet server to interface directly with a suspect in real time = Moderate to High Risk.

During an undercover Internet investigation there will be many opportunities to engage with one or more suspects in real time while using the Internet. Examples include on-line chatting, instant messaging, and voice over Internet protocol (VOIP) programs such as Skype. Anytime you are directly interfacing with a suspect on the web, there's a risk that he or she has the computer know-how or software to do some snooping. This risk is much lower if you're using a large and reputable third party service provider. For example, instant messaging hosted by AOL or VOIP hosted by Skype is lower risk since you are using third party servers and software to engage in the real time communication. However, always be on guard for instant messages that contain attachments or anytime a suspect sends you a file via the real time conversation. The file he's sending could include a virus or Trojan horse that brings with it the ability for the suspect to take a peek at your computer. If you are engaged in real time communication and your suspect sends you a digitized photo of the wildlife item he's trying to sell, it might damage the relationship if you don't immediately download and open the file. If you decide to engage in real time communication with a suspect while using a government computer or Internet connection, be ready to deal with this scenario if it comes up – "Oh, can you e-mail that to me? The computer I'm using right now belongs to my boss and I could get fired for downloading attachments that aren't related to work. In fact, he'd fire me if he knew we were chatting right now. I'll download it later and get back to you."

All undercover contacts with suspects, whether in person, over the phone, or over the Internet, have some risk associated with them. During an in person meeting, there's the risk of discovery and potential personal safety issues.

Network Your Own Support:

There are many city, state, and federal law enforcement agencies involved in investigations that include covert Internet work. Networking with these officers will help you gain a better understanding of what is and is not possible on the web. A network of investigators specifically involved or interested in wildlife cybercrime investigations is available through the Wildlife Cybercrime Enforcement Group (WCEG), a secure special interest group hosted by Law Enforcement Online at www.leo.gov. The WCEG membership includes state, federal, and foreign wildlife law enforcement officers.

The Bottom Line:

The bottom line to all of this myth versus reality is straight forward. All undercover contacts with suspects, whether in person, over the phone, or over the Internet, have some risk associated with them. During an in person meeting, there's the risk of discovery and potential personal safety issues. On-line or on the phone, there's the risk of suspicion or discovery, which can ultimately jeopardize the case or create safety issues in future meetings. A smart suspect will always be suspicious of you and will test you to satisfy themselves that you are not a law enforcement officer. The fact that they test you proves nothing more than that are naturally suspicious. As with all undercover activities, our risks are calculated and we work to minimize them but, in the end, risks must be taken to solve wildlife crimes and we are the men and women willing to take those risks. When conducting undercover contacts through the Internet, use your best judgment but don't limit yourself or your options based on myths and rumor. If you hear something about what you can or can't do while undercover and it's not obvious or you don't understand the technical aspects of it, ask questions and test the truth of the statement before abandoning your most logical and preferred avenue of attack. As a supervisor of officers conducting Internet investigations, avoid reaching premature conclusions. Test your assumptions, realistically balance the risks, trust your officers' judgment, and then turn your investigators loose on those that would destroy our wildlife with the click of a mouse.

Be safe out there!

Ed Newcomer is a Special Agent with the United States Fish and Wildlife Service and currently serves as the Deputy Resident Agent in Charge of the Torrance, California field office. Ed has conducted a number of covert Internet investigations resulting in felony arrests and convictions for wildlife offenses. In 2009, Ed initiated the Wildlife Cybercrime Enforcement Group (WCEG) and currently serves as its moderator. The opinions expressed by Ed in this article do not necessarily represent the views of the US Fish and Wildlife Service, the US Department of the Interior, or the United States Government.