# Self-Reliance Institute Newsletter

September 2014 Volume 2, Issue 9


## This Badger Protects Privacy

This week, I want to let you know about a free web browser add-on that is designed to assist you in protecting your privacy.

Before I discuss the app, called Privacy Badger, here is the August edition of your free Self-Reliance Institute Newsletter. Enjoy!

OK. Back to Privacy Badger.

First, I want to remind you that when I share applications that are designed to protect your privacy, no one application is going to be right for everyone. As with any computer application, you should read the FAQ (frequently asked questions) section at the applications website. For Privacy Badger, the FAQ can be found on the homepage of the website.

With that important reminder, I will tell you that I've been testing Privacy Badger on my desktop and laptop computers for three weeks and I'm pleased to find that the application does what it says it will do and is very, very easy to use.

Also, it was created by the good folks at EFF – the Electronic Frontier Foundation.

So what does Privacy Badger do? Let's turn to those all-important FAQ's for the answer by reviewing a few of the most important questions and answers. Remember,

Badger Continued page 4

**IN THIS ISSUE**



## The Government's Blacklist Rule-book

Do you remember where you were and what you were doing on September 11, 2001, when you learned that the World Trade Center had been struck by an aircraft?

I certainly do and I'm sure you do as well. It was a life-altering day for many of us in many ways.

At the time, I lived just outside Washington, DC. On 9/11, I was scheduled to give a presentation about identity theft to a group that was meeting just to the north of the Pentagon in the USA Today tower in Arlington, Virginia. Of course, the meeting never took place.

That evening, I co-hosted (along with Doug McKelway, who is now a reporter and anchorman for Fox News) the first of numerous overnight radio broadcasts on WMAL – a news/talk station in Washington, DC – about the unfolding crisis.

Within days, every conference presentation I was scheduled to give across the country in the coming months was cancelled because event organizers believed Americans would be too afraid to fly for the foreseeable future.

Yet, by the following week, I was back on a commercial flight to New Hampshire where I was involved in the investigation of an Internet stalker who'd murdered a promising

Blacklisted continued page 3

## The Army Of SWAT

Last week, I discussed whether the United States military can attack or imprison Americans. I received a number of thoughtful emails in response to the information and resources I provided.

Several members of the Self-Reliance Institute raised the issue of law enforcement agencies and police departments that act like they are military units. Or, as it is usually called, the militarization of police.

In recent years, due to the excellent work of a handful of journalists and specific events that have pushed the issue to the forefront, there has been increased attention to the proliferation of police SWAT teams (special weapons and tactics) at the local, state and federal levels of policing. There has also been warranted attention to the increased use of those specialized units for routine police tasks.

In other words, there is growing concern over heavy-handed police tactics being used in non-threatening circumstances.

Additionally, there is growing concern that SWAT units are morphing into armies.

SWAT continued page 5

# The Military and Civil Disturbances

The Military and Civil Disturbances

Don't let the innocuous title of this Self-Reliance Institute Advisory fool you. What I'm about to share with you is extremely important and deadly serious.

And, given the growing potential for civil unrest, it's very relevant to many of the events unfolding across the United States.

During my talk radio career – one of many professional hats I've worn – there was a question that listeners asked with increasing frequency after the Department of Homeland Security was created and rumors of the construction of internment camps began to circulate.

With the election of President Barack Obama, and his penchant for using executive orders to bypass Congress and the Constitution, the question cropped up even more frequently.

The question boils down to this: **"Can the United States military imprison or kill American citizens on American soil?"**

And before anyone scoffs at the notion of the military being turned on citizens, recall that in 2013 U.S. Senator Rand Paul conducted the longest filibuster in recent Senate history as he demanded that Obama affirm that he would not use drones to kill U.S. citizens on American soil.

As the hours wore on, Paul was joined by other conservative, libertarian, and Tea Party affiliated members of the Senate in his filibuster. Even one Democrat came on board.

So it is a rational question.

**Can the United States military imprison or kill American citizens on American soil?**

The answer is, "Yes."

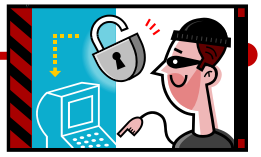
Yes, the U.S. military can imprison or kill American citizens on American soil.

Now I bet some of you, with good reason, are asking: "What about the Posse Comitatus Act? Doesn't that forbid the use of the military against Americans here in the U.S.?"

The answer to that question is, "No, not always."

This week, the good people over at ZeroHedge pulled together the infor-

Disturbances continued page 8



# The Russian Hacker Threat

As you may have heard, Russian hackers stole more than a billion user names and passwords for email and other types of online accounts.

I want to share a bit of information about this reported cybercrime and I want to tell you about the single most important step you can take to make sure you never lose a dime as a result of someone hacking your personal information.

After all, at some point in your life your financial accounts will be hacked. You will have credit card and/or other personal and private financial information stolen and someone will use that valuable information to steal your money or make purchases with your credit.

It's a fact of life. It's going to happen. For many of us it's already happened.

Why? Because you can do everything in your power to protect yourself – you can follow every tip and suggestion I give you – and you'll still be victimized because you don't control all of your personal and private financial information.

Think about it. Unless you keep your money under your mattress or buried in the backyard – and I'm not suggesting you do that – you have to rely on the security of the financial institutions you entrust with your savings and investments.

And, invariably, that trust will be broken.

Cybercriminals are going to continually attack and defeat the electronic fences financial institutions attempt to erect around your financial accounts.

Whether working alone, as part of organized crime, or on behalf of nation-states intent on penetrating the financial infrastructure of the United States, hackers are constantly probing and thwarting the cybersecurity

Hacked continued page 6

# Blacklisted

Continued from page 1

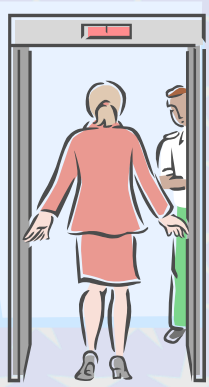
young woman.

That first post-9/11 flight was memorable for many reasons – we flew just to the west of Manhattan and could see the still-smoldering ruins of the World Trade Center – and proved that travel by aircraft had changed forever.

By Thanksgiving, I had taken dozens of flights across the country as I spoke at a series of closed-door seminars for bankers about identity theft – including a small section about how terrorist cells might be funding themselves inside the U.S. through financial fraud and ID theft.

While taking those flights, it quickly became apparent that the government was fumbling its way through the creation of a series of new screening processes for passengers boarding aircraft. As you may recall, it wasn't unusual to be physically searched – and to have your luggage searched – three times by the time you boarded your flight.

At one checkpoint inside Boston's Logan International Airport, where the two flights that struck the World Trade Center originated, a nervous member of the National Guard pointed his rifle at me when a security agent became alarmed at the large amount of electronic equipment in my suitcase showing up on his screen. It was just weeks after 9/11 and I was carrying all of my own projection equipment for a small conference. Easily explained, but it didn't matter as security personnel were extremely jittery and everyone was viewed as a potential threat.



I had to unpack everything at gunpoint, demonstrate that all my electronic equipment was legitimate by turning each piece on and operating it, and then repack before being escorted and observed as I boarded my flight.

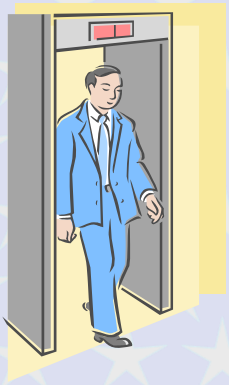
On November 12, barely two months after 9/11, I had just taken my seat on a flight out of Baltimore-Washington International Airport when everyone was ordered off the plane and told to return to the ticket area in the main terminal. We had no idea what was going on and the flight crew wouldn't tell us anything.

As soon as we deplaned and powered up our cell phones, almost every passenger's cell phone began ringing. In fact, almost every cell phone on the concourse was ringing. It was our friends and family calling to see if we were OK because another plane had crashed in a New York City neighborhood.

Bottom line: Air travel has never been the same since 9/11.

And it certainly hasn't been the same for tens of thousands of Americans who've been placed on a secret blacklist – the U.S. government's terrorist watchlist – that has many ramifications, including potentially preventing them from traveling on commercial airlines by placing them on a "No-Fly List."

Now, for better or worse, the most recent edition of the "guidance" – the rules – for placing individuals on the blacklist have been obtained and released. And, since it's been released, I think you should know about it so you can read it yourself and decide whether the government has created a reasonable set of rules for determining who might be a terrorist.



The document, known as the "March 2013 Watchlisting Guidance," can be reviewed by clicking – HERE.

The publication that released the document – the fact that it was released is highly controversial – is called The Intercept.

If you'd like to read The Intercept's explanation of why they released the document and what they believe the document reveals, please see "The Secret Government Rulebook for Labeling You a Terrorist."

The article states at the outset:

"*The Obama administration has quietly approved a substantial expansion of the terrorist watchlist system, authorizing a secret process that requires neither "concrete facts" nor "irrefutable evidence" to designate an American or foreigner as a terrorist, according to a key government*

Blacklisted continued page 7

# Badger

Continued from Page 1

these are the statements of the Electronic Frontier Foundation (EFF), the creators of Privacy Badger.

What is Privacy Badger? "Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it's like you suddenly disappeared."

"Privacy Badger is a browser add-on that stops advertisers and other third-party trackers . . .

How is Privacy Badger different to Disconnect, Adblock Plus, Ghostery, and other blocking extensions? "Privacy Badger was born out of our desire to be able to recommend a single extension that would automatically analyze and block any tracker or ad that violated the principle of user consent; which could function well without any settings, knowledge or configuration by the user; which is produced by an organization that is unambiguously working for its users rather than for advertisers; and which uses algorithmic methods to decide what is and isn't tracking. Although we like Disconnect, Adblock Plus, Ghostery and similar products (in fact Privacy Badger is based on the ABP code!), none of them are exactly what we were looking for. In our testing, all of them required some custom configuration to block non-consensual trackers. Several of these extensions have business models that we weren't entirely comfortable with. And EFF hopes that by developing rigorous algorithmic and policy methods for detecting and preventing non-consensual tracking, we'll produce a codebase that could in fact be adopted by those other extensions, or by mainstream browsers, to give users maximal control over who does and doesn't get to know what they do online."

How does Privacy Badger work? "When you view a webpage, that page will often be made up of content from many different sources. (For example, a news webpage might load the actual article from the news company, ads from an ad company, and the comments section from a different company that's been contracted out to provide that service.) Privacy Badger keeps track of all of this. If as you browse the web, the same source seems to be tracking your browser across different websites, then Privacy Badger springs into action, telling your browser not to load any more content from that source. And when your browser stops loading content from a source, that source can no longer track you. Voila! At a more technical level, Privacy Badger keeps note of the "third party" domains that embed images, scripts and advertising in the pages you visit. If a third party server appears to be tracking you without permission, by using uniquely identifying cookies to collect a record of the pages you visit across multiple sites, Privacy Badger will automatically disallow content from that third party tracker. In some cases a third-party domain provides some important aspect of a page's functionality, such as embedded maps, images, or fonts. In those cases Privacy Badger will allow connections to the third party but will screen out its tracking cookies."

OK. Those are the top three FAQs and they should give you a sense of what Privacy Badger is and how it works. Please take note that currently it does not work with Internet Explorer. It only works with Chrome and Firefox. And, once again, if you're going to give Privacy Badger a try, read all of the FAQ's easily located on the homepage. Also, Privacy Badger is a beta application. So, it's possible that all the kinks haven't been worked out.

But, I'll tell you that it has worked very well for me and has been seamless as an add-on. In other words, it hasn't locked up my system or caused any functionality problems that I've been able to detect. And, the program self-adjusts, so it improves at blocking tracking as you use it.

If you'd like to read more about Privacy Badger, check out "EFF's Snoop-Stopping, Ad-Smashing Privacy Badger Plugin Hits Beta" at PC World.

If you give Privacy Badger a try, let me know what you think by emailing me at Rob@SelfRely.com

Be safe and secure,

Rob Douglas – Former Washington DC Private Detective, Information Security Consultant and Certified Identity Theft Risk Management Specialist

# SWAT

Continued from Page 1

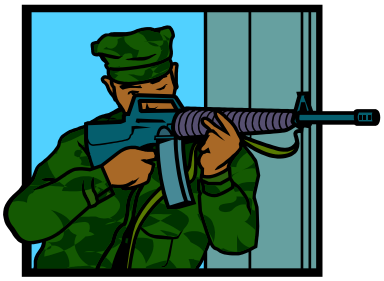
Earlier this year, John Fund raised this issue in National Review Online with an excellent piece, "The United States of SWAT?"

Fund opens by referencing the Cliven Bundy standoff and quickly points out that the force marshalled against Bundy is part of a troubling trend.

"*Regardless of how people feel about Nevada rancher Cliven Bundy's standoff with the federal Bureau of Land Management over his cattle's grazing rights, a lot of Americans were surprised to see TV images of an armed-to-the-teeth paramilitary wing of the BLM deployed around Bundy's ranch*.

"*They shouldn't have been. Dozens of federal agencies now have Special Weapons and Tactics (SWAT) teams to further an expanding definition of their missions. It's not controversial that the Secret Service and the Bureau of Prisons have them. But what about the Department of Agriculture, the Railroad Retirement Board, the Tennessee Valley Authority, the Office of Personnel Management, the Consumer Product Safety Commission, and the U.S. Fish and Wildlife Service? All of these have their own SWAT units and are part of a worrying trend towards the militarization of federal agencies — not to mention local police forces.*

"'*Law-enforcement agencies across the U.S., at every level of government, have been blurring the line between police officer and soldier,' journalist Radley Balko writes in his 2013 book Rise of the Warrior Cop. 'The war on drugs and, more recently, post-9/11 antiterrorism efforts have created a new figure on the U.S. scene: the warrior cop — armed to the teeth, ready to deal harshly with targeted wrongdoers, and a growing threat to familiar American liberties.*'



"*The proliferation of paramilitary federal SWAT teams inevitably brings abuses that have nothing to do with either drugs or terrorism. Many of the raids they conduct are against harmless, often innocent, Americans who typically are accused of non-violent civil or administrative violations*."

Fund goes on in his article to cite a number of specific incidents and statistics that should trouble us all.

He also notes:

"*Since 9/11, the feds have issued a plethora of homeland-security grants that encourage local police departments to buy surplus military hardware and form their own SWAT units. By 2005, at least 80 percent of towns with a population between 25,000 and 50,000 people had their own SWAT team. The number of raids conducted by local police SWAT teams has gone from 3,000 a year in the 1980s to over 50,000 a year today*."

Did you catch that?

From 3,000 SWAT raids a year in the 1980s to over 50,000 a year today!

Amazing, considering that there is far less crime today than there was in the 1980s.

And it's the point that Fund makes about homeland-security grants being used to arm local police with military equipment – including grenade launchers, armored vehicles and aircraft – that brings me to a resource I want members of the Self-Reliance Institute to have so that you can determine what your local police may have obtained in recent years when it comes to military equipment.

The resource is an interactive chart titled "Mapping the Spread of the Military's Surplus Gear" and it can be found by scrolling down to the interactive map of the U.S. on this page, "What Military Gear Your Police Department Bought."

That page begins with this fact:

"*Since President Obama took office, the Pentagon has transferred to police departments tens of thousands of machine guns; nearly 200,000 ammunition magazines; thousands of pieces of camouflage and night-vision equipment; and hundreds of silencers, armored cars and aircraft*."

I suggest you ignore the additional verbiage on the page about the

SWAT continued page 7

# Hacked

Continued from Page 2

of banks and investment companies.

It's a fact of life that there is no truly secure computer system. There is always a way to penetrate cybersecurity.

But, there is a way to be sure that any financial loss is born by the financial institutions you entrust and not by you. And this technique is so obvious – so commonsense – that when I tell you, you're going to get mad at me.

First, some resources to check about the reported Russian hack.

The always excellent Brian Krebs has some good info about the incident in his piece, "O&A on the Reported Theft of 1.2B Email Accounts." As it turns out, Krebs knows the individual, Alex Holden, who broke the story and Krebs discusses whether or not the incident is real (some think not) and as large as reported.

The Federal Trade Commission (FTC), who I assisted with a sting operation against rogue "information brokers" back at the turn of the century (sounds so long ago when I put it like that!), has some good information in "Russian Hackers Might Have Your Info – Now What?"

I know many folks are not very trusting of the federal government – for good reason! But, having been a consultant to the FTC, I can attest to the fact that it does have some very dedicated professionals when it comes to information security. The suggestions in the piece are solid, if somewhat rudimentary.

Over at Wired magazine, "Follow These 4 Easy Steps to Toughen Up Your Passwords" is a straightforward piece with good suggestions about password security.

Additionally, while not specifically about the Russian hack, "Was Your Brokerage Account Hacked? Here's How to Know" has some solid information about password security when it comes to investment accounts.

OK. Let me share with you the most important security advice I give all my audiences when I'm paid to speak at conferences about identity theft, cybercrime and information security.

And please remember I already warned you that you're going to get mad at me when I tell you this because it's so simple.

Ready?

***Read your financial statements every month***.

Simple, right?

Yet, every study shows – and every audience I've asked during the more than 15 years I've been speaking at information security conferences confirms – people don't review their financial accounts on a monthly basis.

That means they're not checking their credit card, checking, savings, and investment accounts on a regular basis to be sure there are no fraudulent transactions.

So, in many cases, once they do discover fraud, the fraud has been going on so long, or is so far in the past, they have a hard time recovering the funds. In short, they may never recover their money.

Yes, as you might know, credit card companies have to refund you for all but $50 lost due to fraudulent transactions on your account. But the more time that has elapsed between the fraud and you reporting the fraud, the harder time you will have convincing the card company that you were a victim and should be reimbursed.

Further, and very important, depending on the amount of time that has lapsed between the fraud and you reporting the fraud, other types of financial accounts – including debit cards – may not have to reimburse you even if you can show that the transactions are fraudulent.

Still, even with financial accounts where the financial institution is not legally required to reimburse your account if you are the victim of fraud, they are more likely to make you whole if you report the fraud within 30 days of it taking place.

In other words, if you come in a year after the date you claim your account was hacked and demand that the bank or investment house make good on the lost funds, you're going to have a tough row to hoe. But if you alert the institution within a month, they will almost always refund your account.

Why?

Because they don't want the reputational harm that comes with the publicity that they've been hacked and didn't refund the accounts of innocent victims who made timely notice of losses.

It really is that simple. They don't want reputational harm.

Hacked continued page 7

# Blacklisted

Continued from page 3

*document obtained by The Intercept.*

"*The "March 2013 Watchlisting Guidance," a 166-page document issued last year by the National Counterterrorism Center, spells out the government's secret rules for putting individuals on its main terrorist database, as well as the no fly list and the selectee list, which triggers enhanced screening at airports and border crossings. The new guidelines allow individuals to be designated as representatives of terror organizations without any evidence they are actually connected to such organizations, and it gives a single White House official the unilateral authority to place entire "categories" of people the government is tracking*

*onto the no fly and selectee lists. It broadens the authority of government officials to "nominate" people to the watchlists based on what is vaguely described as "fragmentary information." It also allows for dead people to be watchlisted.*"

From there, The Intercept goes into great detail about the history of the blacklist and the criteria applied to individuals and groups.

I think you'll find it to be an important read and I highly recommend that you examine the original document. I have mixed feelings about its release. But, sice it's been made public, I think good citizens will want to review it and judge for themselves whether the government is being overzealous in how it determines who is placed on the blacklist.

I'd love to know what you think about this important issue. You can email me at Rob@SelfRely.com

Be safe and secure,

Rob Douglas

# SWAT

continued from page 5

Ferguson, Missouri situation (let's ait until all the facts are in before making conclusions about that specific case) and focus on the raw data the chart provides. You can place your cursor over your county on the map and determine what military equipment the police in your area have obtained in recent years.

Also take note of the other worthwhile links on the page that will help keep the data up to date.

Finally, Fund mentioned Radley Balko – author of "Rise of the Warrior Cop." I interviewed Balko several years ago and he is a true patriot who is concerned about escalating police militarization and the threat that militarization poses to innocent Americans. If you'd like to follow his work, he now posts regular pieces to a blog that can be found HERE.

What do you think about the increased militarization of the police? Write me at Rob@SelfRely.com

Be safe and secure,

Rob Douglas - Former Washington DC Private Detective, Information Security Consultant and Certified Identity Theft Risk Management Specialist

# Hacked

Continued from page 6

Trust me. I've been doing this for quite some time. At the end of the day, no matter what other security steps you take, the best way to be sure that you don't actually lose money when your financial account is hacked is to review your account at least every month so that you can immediately report the loss and get refunded.

Do you have a personal story of dealing with a financial institution after your account was hacked? Email me at Rob@SelfRely.com

Be safe and secure,

Rob Douglas - Former Washington DC Private Detective, Information Security Consultant and Certified Identity Theft Risk Management Specialist

# Disturbances

Continued from page 2

mation about the use of the military against citizens that you need to know and that you need to share with your friends and family.

The article is, *Under What Conditions Can the U.S. Army Engage Citizens: The Army's "Civil Disturbances" Primer*.

I highly recommend you open and read the entire piece. Not only does it provide you with specific information about how the U.S. military can be used to imprison and kill Americans on U.S. soil, it provides you with the links to the government documents that purportedly authorize the military to take such actions under certain circumstances.

Those documents include:

**1)** *ATP 3-39.33 Civil Disturbances (April 2014)* which, among other aspects, lays out various scenarios where the U.S. military can be used against American citizens. As ZeroHedge puts it: **"In other words, if and when the US Armed Forces decide that rioting infringes upon any of these exclusions, then the constitution no longer applies and the use of lethal force becomes a viable option against US citizens."**

**2)** *FM 3-39.40 Internment and Resettlement Operations (February 2010)* which ZeroHedge points out allows for Americans to **"be herded into '*temporary internment camps*' for reindoctrination purposes under the supervision of PSYOP Officer."**

ZeroHedge concludes that, based on these documents, "[I]f and when the time comes to "override" Posse Comitatus, random U.S. citizens may have two options: i) end up in the US version of a Gulag or, worse, ii) be shot."

As always, I prefer that you read the source documents for yourself – that's what we as self-reliant individuals should do.

Once you've assessed the documents for yourself, you can draw your own conclusions about whether the U.S. military could ever be turned against American citizens to conduct lethal or internment maneuvers.

Once you reach your conclusion, I'd love to hear your thoughts. Write me at Rob@SelfRely.com
Be safe and secure,

Rob Douglas - Former Washington DC Private Detective, Information Security Consultant and Certified Identity Theft Risk Management Specialist

PS: As I send this off to you today, residents in and around the northern San Francisco Bay area (Napa) have been struck with the most powerful earthquake in that region since the 1989 Loma Prieta earthquake that killed more than 60 and injured thousands.

As we keep our fellow Americans in our thoughts and prayers, this is a tragic reminder of how important it is to be prepared to take care of yourself and your family for an extended period of time if the need arises.

Are you prepared?