



Attached is a sample of the monthly newsletter The Lemonade Stand is offering as an annual subscription. The subscription includes a monthly newsletter branded with your company logo and colors with the following schedule of topics:

- **April: Privacy** - protecting sensitive information
- **May: Malware** - viruses, worms, Trojans, key loggers, spyware, etc.
- **June: Social networking, social media and Web** - security hazards associated with using Twitter, Facebook *etc.*
- **July: Gadgets** - security issues associated with portable IT devices including laptops/netbooks/tablets, USB memory sticks, smart phones
- **August: Hacking** – information about hackers, industrial spies, insider threats, scammers, criminals, etc.
- **September: Email/messaging security** security issues surrounding email, IM, VoIP, physical security (shoulder surfers!) and more;
- **October: Information Security Awareness Month:** Tips on all topics
- **November: Identity theft** - phishing, Social Engineering and other forms of identity theft;
- **December: Network and Internet security:** information security issues linked with networking and P2P;
- **January: Cryptography** - introduction to encryption and other cryptographic technologies;
- **February: Wireless, mobile and home working** - wireless networking (WiFi, Bluetooth, 3G *etc.*) and laptop security.
- **March: Authentication and identity management** - choosing strong passwords biometrics, identity theft and access control

The newsletter is aimed at customers and employees who are *not* information security specialists, with highlights of what they should know to protect their information. The newsletter will also include “Luddite’s Lament”- a humorous and informative column written by a true technology Luddite addressing the topic of the month.

[Let us know](#) if you’re interested in a copy of the price list for a subscription branded for your company to send to employees and customers.

1



The Lemonade Stand

Fun and effective Risk and Compliance training

2

YOUR INFORMATION SECURITY RESOURCE

APRIL 2011

THIS MONTH'S TOPIC: Privacy

- ◆ Privacy in the News
- ◆ Regulations that Protect Your Private Information: GLBA, FACTA and HIPAA
 - The Gramm-Leach-Bliley Act (GLBA)
 - The Fair & Accurate Credit Transactions Act (FACTA)
 - Health Insurance Portability and Accountability Act (HIPAA)
- ◆ Luddite's Lament - *Technical notes from an anti-technologist*

2

PRIVACY IN THE NEWS



You may have recently read stories from security experts warning people about inadvertently giving away their location when sharing pictures online. Even Adam Savage from the popular science program "[MythBusters](#)" wasn't immune to this recent privacy concern when he posted a picture of his Land Cruiser on his Twitter account. Fans and potential thieves received his home address along with the accompanying text, "Now it's off to work."

How did this happen? Savage used his GPS (Global Positioning System) - enabled cell phone to snap and share the photo taken right in front of his house. The resulting photo contained a geotag, which gives the exact coordinates of where the photo is taken. Mr. Savage said he knew about geotags, but neglected to disable the function on his iPhone before taking the picture and uploading it to Twitter.

The concern here is that most users of GPS technology are not technically savvy or even worse don't understand how important it is to protect their privacy.

It would seem that disabling the GPS functionality should be simple, but oftentimes it involves going through several menus to get to the right place. If you do this incorrectly, you could potentially turn off all GPS capabilities, including mapping, so it's complicated.

Fortunately, there's help. The Web site ICanStalkU.com raises awareness about inadvertent information sharing and has provided [step-by-step instructions](#) for disabling the photo geotagging functionality on many popular GPS-enabled devices.

Before you decide that this is too much trouble, think about some of the pictures you post on the Internet. Are you showing off your shiny new car? Sharing pictures of your children or grandchildren? Do you really want people to know what's up for grabs when you're posting your "I'm at Starbucks" update each morning?

You'll learn more about GPS and how it works in our "Luddite's Lament" column contained in this newsletter. In the meantime, let's take a look at other privacy topics and what you can do to protect your personal information.

2 REGULATIONS THAT PROTECT YOUR PRIVATE INFORMATION: GLBA, FACTA AND HIPAA

DISCLAIMER: These topics contain only a brief summary of the law. Please consult a legal professional for more information on how the specifics of this law may apply to you.

THE GRAMM-LEACH-BLILEY ACT (GLBA)

2



The Financial Services Modernization Act of 1999 is the federal law that covers privacy for personal financial information. It is more commonly known as the Gramm-Leach-Bliley Act (or GLBA), after the sponsors of the legislation.

GLBA requires financial institutions to provide an annual notification to customers about how personal information is collected and describe how they will protect the security and confidentiality of the information in their possession. Companies that share or sell customer data outside of their organization must give customers a way to opt out of having information shared with others.

Doing your part

The notices are usually included as an insert with monthly statements and are easily overlooked. GLBA only covers data shared with outside companies. However, another federal law, Fair and Accurate Credit Transactions Act (FACTA), gives you some rights to stop companies from sharing your personal data with corporate affiliates. Your rights to opt out under the FACTA are usually included in the GLBA privacy notice you receive.

Further information can be found online at the FTC's [Bureau of Consumer Protection](http://www.ftc.gov) site.



Among other protections, the Fair & Accurate Credit Transactions Act (FACTA) requires the destruction of all consumer information before it is discarded and carries potentially severe penalties against violators.

The Act states “any person who maintains or otherwise possesses consumer information for a business purpose” must “properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal”.

Doing your part

Just like businesses that handle your private information, it’s important that you take care to completely destroy your sensitive information before you discard it. Using a shredder is a great way to destroy your confidential paperwork, but you must also take extra precautions to remove confidential data from your computer when it’s time to replace it with a newer model.

You might think that you’re removing the data when you delete a file. Even when you empty your recycle bin, that file is not really removed from your computer. When you delete a file, the operating system only removes the reference of the file from the file system table. Take the extra step in removing those files by [using a secure file deletion](#) program.

You can read more information about FACTA online at the [Federal Trade Commission](#) site.



Established and passed in 1996, the Health Insurance Portability and Accountability Act, or HIPAA, allows patients the opportunity to keep their medical record information safe. HIPAA gives patients full control over who can and cannot see their medical records.

Medical records contain highly sensitive facts which you might not want to share with the world, such as doctor appointments, prescriptions, medical conditions, and other medical information.

Doing your part

If you’re worried about the status of your medical records, you might want to try requesting them yourself. It’s a great way to see whether you can easily get your records or if the staff takes precautions to ensure that you are who you say you are.

Many health facility records are stored digitally. Just like any other business that keeps your confidential information, your digital medical records are required to be kept private. Ask your health care provider about what security measures are in place to keep hackers out of their computer system.

The U.S. [Department of Health and Human Services](#) has more information about HIPAA.

③ Optional- We'll add your content here.

Content must be received by The Lemonade Stand the third Friday of the month to be included in the next month's newsletter.

➤ LUDDITE'S LAMENT - *Technical notes from an anti-technologist*

As part of an insidious plan to drag me kicking and screaming out of retirement and into the twenty-first century, I have been asked (prodded and coerced) to contribute to this monthly endeavor. The purpose, as I understand it, is to help educate the masses about certain attributes of commonly used technological devices i.e. cell phones, computers, cameras, etc. and their inherent dangers to your personal privacy and security. So without further ado I welcome you to the wonderful of information security for the less than technically gifted.



This month's subject is the Global Positioning System (GPS) and what you need to know about its capabilities and use. Briefly, the GPS uses the intersection of satellite signals to fix a position in three-dimensional space (a more detailed explanation is available at [How Stuff Works](#)). It is an excellent tool with many practical applications. The problem with excellent tools is that they can also be used for nefarious purposes. If you search "GPS Tracking" on your computer, you will find any number of software uploads which allow you to keep tabs on cell phones or automobiles equipped with GPS. The software allows tracking in real time and determines routes travelled, time spent at each stop, and even distance and speed between stops. Some of the newer cameras can even tag a picture with the location it was taken.

Now you know what information can be gleaned from your GPS equipped devices, but how can you control that information? The only sure way is to not use devices so equipped, but if you must, then familiarize yourself with the following:

- ◆ If power is applied (the battery is installed) the device can be tracked.
- ◆ Never allow anyone to load anything on your phone or other device.
- ◆ Use the GPS off function accessed through the menu on your device.
- ◆ Disconnect the GPS antenna inside the device (serious geeks only).
- ◆ Remove the battery.
- ◆ If all else fails, sit in a dark room wearing a hat made of aluminum foil to keep them from reading your thoughts.

"Any sufficiently advanced technology is indistinguishable from magic." (Arthur C. Clarke)

④

Included in the price:

- ① Your logo
- ② Accents, titles and borders in your company colors
- ③ Additional content provided by your company (Optional)
- ④ Your contact information