We Regret To Inform You That "Due to Insecurities Beyond Our Control, Your Privacy Has Been Cancelled For Your Convenience"

Pacific Institute for Ethics and Social Policy Conference on
Technology, Intelligence, and the Preservation of Civil Liberties
Saturday, November 18th, 2006
Cannery Pier Hotel and Maritime Museum, Astoria, Oregon

Joe St Sauver, Ph.D. (joe@uoregon.edu)

http://www.uoregon.edu/~joe/pacificinstitute/

Section 0. Introduction

Disclaimer and A Note On The Format of This Talk

- I've prepared this talk in some detail so that:
  -- it can be followed by those not currently present,
  -- to insure that the contents of the talk are fully accessible to any hearing impaired members of the audience, and
  -- to minimize the need for the audience to do note taking.
- We'll also likely have more material than time, so we'll cover what we can until we run out of time; you can finish the rest of the material on your own
- **Disclaimer: all opinions expressed in this document are strictly my own. Independently assess and reconfirm all information presented, and note that even if you follow all the recommendations given here, you may still experience a privacy or security breach.**

The Premise of Today's Talk

- I suspect that some may be wondering about the somewhat odd title for my talk -- 'We Regret To Inform You That "Due to Insecurities Beyond Our Control, Your Privacy Has Been Cancelled For Your Convenience." It may be easiest to begin by decomposing that title into its component parts:

  -- computer/network security issues have become ubiquitous,

  -- collectively, we can't mitigate many of those issues for you,

  -- while you might be able to take personal steps to do so, doing so may be inconvenient, which means you probably won't take those steps, and thus

  -- your privacy will often end up being effectively nullified.
- The remainder of this talk will explore this premise, and what steps you might take to avoid this situation.

The Online Privacy and Security of the *Law Abiding Individual*

- Today's discussion is meant for the law abiding individual who wants and needs to protect his or her privacy and security against potential attackers such as spammers, identity thieves, phishers, stalkers, etc. You have the right to be secure against online attacks by these miscreants, and to be able to operate online without being constantly tracked by privacy-invading marketeers.
- It is not my desire nor intent to help criminals or terrorists, nor to interfere with the efforts of those working to defeat them.
- Consequently, everything we'll cover today has been carefully limited to topics which have already been publicly disclosed and which presumably the bad guys already know.
- I've also kept this talk to a technical level that's accessible, while including a few topics of interest to geeks who're here.

Section 1. Privacy and Email Security

Email

- Let us begin with the most fundamental Internet application of them all, electronic mail.
- While some of your messages may be public or semi-public (such as postings to mailing lists), most of your email is, or is probably meant to be, personal/private...
- Isn't it ironic, then, that:
  -- the simple mail transfer protocol (SMTP) usually transfers mail between mail servers as plain text (e.g., unencrypted)?
  -- email is normally stored on mail servers unencrypted?
  -- when you download your email to your desktop/laptop with POP or IMAP, your account credentials and your email traffic will typically flow over the network unencrypted?
  -- system administrators with suitable privileges have the (technical) ability to access all your unencrypted email?
  -- when you delete a message, it often really isn't "gone"?

Encryption of Email In Flight

- Email doesn't have to be such an "open book."
- For example, encryption via TLS (transport layer security) can be used to prevent eavesdropping on traffic between mail servers, and TLS can also be used to secure your messages and your password when you retrieve email via POP and IMAP with a mail user agent (MUA) such as Mozilla Thunderbird or Outlook.
- UO, like many colleges and universities today, strongly promotes the use of encryption in conjunction with email, requiring the use of encryption for POP and IMAP and for all web mail access to uoregon.edu email accounts. See http://micro.uoregon.edu/security/email/index.html
- Once an email server is configured to support this sort of secure access, configuring a user's system to use TLS is generally just a matter of checking a box on the user's MUA.

Encryption of Email At Rest

- Advisable though it is to encrypt all email traffic while it is in flight, we know many email systems still don't support this, and doing so won't protect your email from a potential curious system administrator, or from the possibility of infinite archival retention and review without your consent.
- Use of a public key encryption product such as Gnu Privacy Guard (GPG) or Pretty Good Privacy (PGP) can be used to help mitigate those risks. A GPG/PGP-encrypted message will be able to be decrypted ONLY by the intended recipient, so even if a GPG/PGP-encrypted message is retained forever without your consent, it won't matter because GPG/PGP encrypted messages can't be read without knowledge of your secret pass phrase.
- **Regrettably most people don't bother to use GPG/PGP.**

Why Is GPG/PGP Still Uncommon?

- Given that your email is at risk of being compromised, and simple procedures could substantially reduce that risk, why is it so rare for email traffic to be secured using GPG/PGP?
- If you talk with users and/or system administrators, you'll hear a variety of different "reasons:"

  -- never heard about encrypting email/never thought about it

  -- there's never been a problem with my mail being snooped before, so what's there by default is probably okay for me

  -- none of the mail I get or send is all that secret--why bother?

  -- I want to do PGP but those I write to just can't figure it out

  -- PGP is too complicated for me to figure out

  -- use of strong encryption is forbidden at my site

  -- the system I use isn't configured to offer it as an option

  -- encryption interferes with antivirus scanning

  -- crypto CPU overhead is prohibitive, etc., etc., etc.

Those Aren't Reasons, They're Excuses

- **The real reason most email users don't use strong encryption is because it's *INCONVENIENT***
- Given a choice between
  -- *email that's easy to use*, or
  -- *email that's both private and secure*,
  users will go for ease of use/convenience every time.
- This is the first of a number of examples I'll mention where users are known not to mitigate known privacy vulnerabilities using readily available technologies because doing so might be **inconvenient**.
- That convenience comes at a price, and that price can be **your privacy and your security**.
- I urge you to think long term and to be proactive, rather than just accepting the easy and convenient status quo.

Keeping Your Email Private: It's More Than Just Strong Crypto...

- Protecting the privacy/security of your email goes far beyond just strong cryptography. Some password-related examples:

  -- As a matter of convenience, do you use the same password for more than one account? If so, you're multiplying the risk that the contents of all your accounts may be violated if the password security of any of your accounts ends up being compromised.

  -- As a matter of convenience, do you store the password for your email account in your MUA (mail reading program), thereby making it easy to automatically check for new email every few minutes? Doing so is unquestionably convenient, but it increases the chance that a visitor to your home or office with access to your computer may also be able to gain access to your email via that stored password.

Password Reset Mechanisms

- Another premier example of an email-related privacy risk lies in password reset mechanisms created to deal with forgotten passwords.
- Your mother's maiden name, or your dog's name, or the name of your high school, or your favorite color – none of those security questions really amount to top secret / high grade cryptographically robust protection for your email account, yet that's all too often what's used to "authenticate" a request to reset your account's password.
- When you get right down to it, passwords as an authentication mechanism really aren't where you want to be anymore, yet two factor authentication methods (such as hardware crypto tokens, or biometric methods) have had slow roll out due to cost of fielding those technologies for large audiences, and because they're not convenient. :-)

Your Email Convenience, Your Correspondents' Email Privacy

- What you do with your email as a matter of convenience can affect your correspondents' privacy as well.
- For example, we all know that some malware is designed to harvest the contents of address books – when you put your correspondent's addresses in your address book for your messaging convenience, you increase the risk that their addresses may end up in the hands of spammers.
- Do you retain email longer than you should? It certainly can be convenient to retain an archive of all your old email, and some messages may be required by law to be retained for a specified period of time by some recipients, but in other cases your correspondents might be horrified to learn that you've still got copies of all the personal email they sent you many years ago. Keep saved email prudently pruned.

HTML Formatted Email

- HTML (hyper text markup language) is a set of tags and conventions originally invented for use in making web pages. Somewhere along the line it also became a common and convenient way to add formatting to email messages.
- Do <u>you</u> accept or send <u>HTML</u> <u>formatted</u> email? If so, you should know that any time you or one of your correspondents opens an HTML formatted mail message, you may be triggering a "web bug" (a 1x1 pixel transparent image file with a specially coded unique URL). Web bugs potentially tell the message sender yes, you did open that message, from IP address www.xxx.yyy.zzz, and you read the message using a system running operating system A and application B.
- Spammers and other bad guys just <u>love</u> that sort of information.
- **Use plain text formatted email to avoid HTML web bugs!**

HTML Formatted Email and XSS

- You should also be aware that by electing to accept or send HTML formatted email, you may also be enabling a whole class of system attacks via something known as "cross site scripting," or "XSS." Cross site scripting attacks take advantage of the ability of HTML formatted documents to run scripts or programs. If a bad guy/gal is able to run scripts or programs on your computer, (s)he'll can compromise it.
- Programs that display HTML formatted messages received from potentially untrustworthy sources normally attempt to "defang" or "sanitize" risky content which may be included, however the identification and sanitization of risky HTML is an imprecise art, and many vulnerabilities slip through even the latest versions of popular browsers (see the nice XSS exploit summary cheat sheet at http://ha.ckers.org/xss.html for some examples broken down by browser).

What About Attachments?

- Attachments are another fine example of a very popular convenience feature which may come with a huge potential security risk, e.g., the infection of your system.
- While being able to send those sort of files by email is undeniably convenient, it also represents a tremendous potential vector for systems to be compromised.
- ***"But Joe! We site license an antivirus product and our users rigorously update their antivirus definitions! Surely that must make non-text attachments safe!"***

The Problem With AV Products

- Most AV products are "signature based," and identify viruses based on peculiarities ("signatures") unique to each virus.
- New virus signatures only get released by the vendor and downloaded by the end user perhaps once a day, while miscreants can release new not-yet-detectable versions of their malware as often as they want (e.g., multiple times a day). The virus writer can thus guarantee that they will have a period of time during which user systems will be vulnerable.
- Virus writers also enjoy another key advantage: they can empirically test and repeatedly tweak their code and its packaging until their exploit doesn't get detected by current popular antivirus products. Thus, it is a virtual certainty that at least some malware will get past your current AV solution… But most users don't understand that... AV software is way too nice of a convenient security blanket

Another Risk: Traffic Analysis

- Sometimes there's an assumption that you need access to the contents of a message in order to violate someone's privacy. That may not be true. Sometimes all you need to know is who's talking to whom, or when they're talking, or how often they're talking. This is known as "traffic analysis."
- For example, knowing that a person is exchanging email with an investigative reporter may be sufficient to violate the privacy of that individual (perhaps with profound real life consequences), and yet email server administrators routinely log email traffic as it is received/sent.
- Use of an anonymous remailers may potentially decouple the sender and the recipient, but is not a satisfactory solution for a variety of other reasons (including the fact that anything sent through an anonymous remailer may in and of itself send up a "red flag" to a traffic analyst).

What About A "Semi-Anonymous" Free Web Email Account?

- Sometimes in talking with users they may mention that their privacy wouldn't be susceptible to traffic analysis attacks because they use a free, convenient web email account.
- Free web email account users may not be very happy when they learn that many free web email accounts include the account user's IP address as part of the message headers included in any email sent from that account.
- An IP address (with a time stamp) is often enough to tie a message to a specific location / a specific individual, and ISPs are under increasing pressure to retain the logs that are required to do that mapping of IP addresses to customers.
- Why don't users notice their IP addresses in the email they send? Well, most people suppress the display of full headers as a matter of convenience when looking at messages.

Section 2. Privacy and The World Wide Web

The World Wide Web

- Enough about email! :-) Second only to email, the world wide web IS the Internet for a lot of users, and their software gateway to that online world is, of course, their web browser.
- How do they select that web browser? Given that they may be paying bills online, or shopping online, or researching sensitive health-related topics online, surely they've carefully selected the web browser with the fewest vulnerabilities and the best privacy enhancing features, right? No.
- In a large number of cases, users simply use whatever web browser that comes with their operating system by default, usually Internet Explorer in the case of Windows.
- They don't pick the most secure web browser or the web browser that best defends their privacy, they use the one that comes with their system because it's most convenient.

Web Browsers Vulnerabilities (11/11/06)

- **Internet Explorer 6.x (http://secunia.com/product/11/):**
  106 advisories
  19 unpatched <== *NOTE*
  most severe unpatched: extremely critical <== *NOTE*
- Internet Explorer 7.x (http://secunia.com/product/12366/):
  3 advisories,
  3 unpatched
  most severe unpatched: moderately critical
- Mozilla Firefox 1.7.x (http://secunia.com/product/3691/):
  36 advisories
  6 unpatched (Firefox 2.x currently has 0 advisories)
  most severe unpatched: less critical
- Opera 9.x (http://secunia.com/product/10615/):
  2 advisories
  0 unpatched

Applications Driving Browser Choices

- To be fair, some users WANT to use a safe(r) web browser, but applications such as an institutional ERP system (e.g., a core administrative database-driven application) or an institution's teaching and learning system or a critical vendor partner's web site may simply not function with anything except a particular less secure web browser.
- When that happens, you may be able to minimize the impact of those constraints by only using the vulnerable web browser when you have to but we know that that may not be very convenient (so users will often just use the "lowest common denominator" browser "everywhere")
- Be sure to also pay attention to any helper applications and plugins you install. Foregoing some multimedia content may dramatically help to harden your web browser against specific exploits.

Cookies

- Another well-known web convenience feature is the ever fabulous "cookie," or small chunk of information saved by web sites on your system for later retrieval.
- Cookies can be used to automate logins to sites which require a password. Cookies be used to save preferences across visits to a web site. Cookies can be used to remember your identity so that a shopping site or its advertising partners will know to always tell you about shopping offers "of interest"
- Cookies also lay the foundation for persistent user tracking and profiling and the wholesale loss of online privacy.
- While cookies can be convenient, or at times necessary in order to do business online, you should never, ever, persistently accept cookies. Periodically double check to make sure you haven't accidentally accepted and saved any cookies without meaning to do so.

Cookies Aren't The Only Thing Your Web Browser May Remember About You

- Besides cookies, your web browser also likely caches the list of sites you've recently visited, copies of web pages you've viewed, bookmarks, and a host of other items. These are, of course, all web browser "convenience" features which many users enjoy, however, if abused, they can also violate a user's privacy. Users should get in the habit of routinely running a system cleanup tool (such as CCleaner) to securely clean up a lot of the files that might otherwise accumulate.
- Cybercafes and other shared computer facilities represent a particular risk to user privacy since the next user may be able to sit down and dredge through much of what you've just finished doing (assuming you don't tidy up after yourself), to say nothing of the danger of keylogging spyware, etc.

Web Pages and Web Proxy Servers

- Some or all of your web traffic may go through a web proxy server, either one that you've explicitly configured, one that has been auto discovered and auto configured, or one that's working passively/transparently. Web proxies allow ISPs to economize on bandwidth by locally saving a copy of each page the first time it gets retrieved, letting the ISP satisfy subsequent requests for copies of that page from the locally saved copy. Web proxies also generally deliver an improved "user experience." If it feels like some popular web pages get delivered *incredibly* quickly, those pages are probably getting proxied and re-served to you from a local web cache.
- All good things, right? Well, yes. But if web privacy is important to you, you should know that a proxy server may ALSO provide a location for your provider to log, save, or selectively block web pages you visit or attempt to visit.

And Even If You're Not Being Proxied

- ... a passive intrusion detection system (such as Snort or Bro) may still be monitoring all network traffic (including the web pages you visit).
- You may be able to overcome that sort of loss of privacy through use of an encryption-based anonymizing service, such as those offered through the Tor network (see http://www.torrify.com/index.php), however even then it can be risky to assume that your web based activities will be fully anonymous.
- You should also know that some sites or networks may completely block all inbound connections from known anonymizing services, since anonymizing services may sometimes be used to launch attacks.
- Isn't protecting your privacy on the web just a "ton of fun?"

Another Exposure: Web Search Engines

- Unless you've been living under a rock the last few months, you probably know that most search engine companies save all your search queries.
- Hoping to get some confidential recommendations for the private treatment of an embarrassing hemorrhoid problem? Well, that (and every other search engine query you've ever made, regardless of how private the topic) has been saved.
- ***"But surely those searches can't be tied back to me!"***
  Maybe, maybe not... search engine companies:
  -- know the IP address associated with each query
  -- often know a persistent cross-search cookie-based
     identifier, too, unless you've been rejecting cookies
  -- in some cases you may even have logged in with a
     username, as occurs when you have a personalized search
     page or a free email account offered by a search company.

Suggestions for Using Search Engines

- Search through an anonymizer with a safe(r) browser
- Reject all cookies, and religiously clean up other files which may be left behind on your system
- Do **not** sign up for email or other personalized services provided via a search engine, convenient though it may be.
- Use a number of different search engines, don't just use one (of course, each additional search engine you use may result in an incremental possibility of being tracked, but you're striving to avoid a single integrated picture of everything you do online)
- Avoid so-called "vanity queries" (e.g., searching for your own name, your own email address, your own phone #, etc.)
- If you know a URL, enter it directly into the browser address bar, don't enter it into a search engine's search box

Privacy and Phishing

- Many of you receive emails every day urging you to "confirm" your eBay account or asking you to login to complete a survey and receive a reward from your bank. Those phishing messages can be a tremendous threat to your online privacy and financial safety.
- One convenient tool that's been released to deal with that is the "anti-phishing toolbar," and many users now use them. Anti-phishing toolbars can block you from accidentally accessing at least some phishing web sites, although just like anti-virus software, they don't (and can't) catch everything.
- What you may not be thinking about is that at least some anti-phishing toolbars send EVERY URL you visit to the provider of the anti-phishing toolbar for checking. This may, or may not be a privacy issue for you, but it is at least a privacy-related consideration you should weigh.

Section 3. Operating Systems

Choice of OS

- Just as in the choice of browser, for many users little if any thought goes into their selection of an operating system. Windows comes pre-installed on most systems they might buy, so that's what they end up using. Besides being pre-installed, most of the software that's out there was developed first for Windows, most of their friends have Windows, some applications are ONLY available for Windows, etc., so that in the end, their default choice of operating system ends up being quite convenient.
- Windows, however, is also the OS that's traditionally been hit the hardest by security vulnerabilities, and the OS that seems to have the biggest issue with persistent vulnerabilities that just don't get patched.
- Those vulnerabilities can directly affect your privacy online.
- Checking Secunia again...

Some Operating Systems (11/11/06)...

- **Windows XP Pro (http://secunia.com/product/22/):**
  157 advisories
  30 unpatched <== *NOTE*
  most severe unpatched: extremely critical <== *NOTE*
- Apple Mac OS X (http://secunia.com/product/96/):
  77 advisories
  2 unpatched
  most severe unpatched: moderately critical
- Red Hat Fedora Core 5 (http://secunia.com/product/8808/):
  11 advisories
  1 unpatched
  most severe unpatched: not critical
- So which OS should a user consider running if privacy and security are priorities?

Secure File Deletion

- Secure file deletion is another common operating system-level problem. Most users assume that when files are deleted, "poof," they're gone forever. In reality, of course, all or most of a deleted file can often be routinely recovered unless that file has been overwritten multiple times. Is it inconvenient to delete files securely? Well, yes, potentially, because it can take a lot longer than just unlinking a pointer to that file, but how much time is your privacy worth?
- Another occasion when secure file deletion can be an issue is when you're selling or otherwise disposing of a used system. If you haven't carefully sanitized the system you're retiring, you may be leaking private data all over the place. See "Information on Hard Drives in Surplus Hardware: 'Deleted' Does Not Mean 'Gone'," at http://cc.uoregon.edu/cnews/summer2005/purge.htm

Whole Disk Encryption

- Widespread reporting about privacy breaches involving the disclosure of personally identifiable information (PII) has sensitized many to the need to protect data stored on laptop computer disks. While you could GPG or PGP to encrypt and decrypt each sensitive file on a laptop on a file-by-file basis, that may be awkward and inconvenient when dealing with a large numbers of files. Automatic encryption of the laptop's *whole disk* may be a much more scalable alternative.
- Some operating systems, like Mac OS X, include easy-to-use whole disk encryption as an integral part of the OS (on the Mac, it is called FileVault). If you use a different operating system, you may need to add whole disk encryption via an external product such as TrueCrypt (a free open source laptop encryption product for Windows and Linux, see http://www.truecrypt.org/)

The Domain Name System

- One final privacy/security risk I'll flag for your attention today... the domain name system.
- DNS, the domain name service, is the way your computer translates a fully qualified domain name (like www.uoregon.edu) to an IP address (like 128.223.142.89)
- DNS service is delivered by DNS servers, normally run by your ISP or whomever provides your network connectivity.
- Just like email servers or web proxy servers, DNS server administrators (and network administrators, for that matter, since DNS traffic is not encrypted) can tell an awful lot about what you're doing or where you're going, or may THINK they know a lot about what's going on based on the DNS queries they may see your system make -- but couple this DNS privacy exposure with malicious distribution of messages includes web bugs for bad sites... see how evil this can get?

DNS Cache Poisoning

- DNS services also represents a real vulnerability when it comes to your online security: if someone can poison the results returned by the DNS server you're using you can easily be made to go to any arbitrary location of the attacker's choice instead of the destination you'd meant to go to (see for example http://www.lurhq.com/cachepoisoning.html)
- Examples of why this might be a problem:
  -- you might try to go to your favorite search engine, but instead of going there, you end up at a virally "hot" site
  -- you might attempt to go to an online merchant or your bank to do some financial transaction, only to be routed to a fake site run by phishers. Yes, that site might use a "snake oil" self signed cert, but who looks at SSL certs, anyhow?)
- Options available to end users to practically control this risk are very, very limited.

Section 4. Cellphones and Your Privacy

A Non-Internet Example: Cellphones

- Does ANYONE here today *NOT* have a cell phone? If so, I'd be very surprised... they're just far too convenient to use.

- The bad guys, just like the good folks here today, also like to use cell phones. Thus, it is probably not surprising that of all wiretaps reported in the *2005 Federal Wiretap Report*, 91% were for portable devices carried about the person, such as cell phones or digital pagers. See http://www.uscourts.gov/wiretap05/WTText.pdf at pp. 6

- Since cell phones are such a popular interception target, it's worth considering several of their privacy-related characteristics.

The Trackability of Cellphones

- For instance, I assume you know that if you carrying a powered up cell phone, it is trivial (at least as a technical matter) to track your location via the triangulation from multiple cell sites, right?[1]
- Sometimes this can be a good thing, as when a cellular user having a coronary calls 911 for help... other times, well...
- You *could* carry a pager and a powered-*down* cell phone instead, which wouldn't expose you to the risk of potential tracking (although the pager traffic could obviously be easily intercepted), or you could just use an old fashioned pay phone, but people don't/won't: it's just too inconvenient.

----

[1] See the discussion of legal requirements associated with cell phone location requests by the former head of the DOJ computer crime unit in "Tracked by Cellphone," http://www.securityfocus.com/columnists/376/1

Location Based Services (LBS)

- Beyond simple cellular triangulation, some providers now offer quite precise GPS-based tracking of cellular customers. One leader in this space is Wave Market, see http://www.wavemarket.com/ , the technology provider behind things such as Sprint/Nextel's "Family Finder" technology, and Cingular's "StreetHive Mobile" friend locator service (now in beta).
- Run a fleet of vehicles? Want to track (in real time) where they are, when and for how long they've been stoped, or how fast they're driving? Commercially available automatic vehicle locator services can collect and deliver that data for suitably instrumented vehicles. The biggest market for LBS, however, is likely commercial (e.g., steering cellular users to the most geographically convenient espresso stand, assuming the stand owner is willing to pay to attract these customers).

Prepaid vs. Regular Cell Phones

- Let's consider another cellular-related example, this time the distinction between prepaid and regular cellular phones.
- Unlike regular cell phones, which often involve multiyear contracts, credit checks, etc., and thus the generation of quite a paper trail which persistently ties a particular phone to a particular person, basic prepaid cellular phones can be anonymously purchased off the shelf by anyone, anytime, for as little as $20 at convenience stores or major retailers.
- Because those prepaid cellular phones are not tied to an individual's identity, and because their low cost makes it easy for individuals to employ them on a use-them-briefly-then-throw-them-away basis, prepaid cell phones potentially offer significantly greater potential privacy than regular cell phones. But don't just take my word for it!

The Expert Consensus...

- Consider the US DOJ Office of the Inspector General's March 2006 report on "The Implementation of the Communication Assistance for Law Enforcement Act," Audit Report 06-13, http://www.usdoj.gov/oig/reports/FBI/a0613/final.pdf at pdf page 13: "*officials surveyed by the OIG identified pre-paid calling cards and <u>pre-paid cell phones</u> as the top two threats affecting their ability to conduct electronic surveillance." [emphasis added]*
- At least some countries have already taken steps to require the registration of pre-paid cellular phones in an effort to preven a variety of abuses, including spam and use of cell phones in conjunction with command-detonated improvised explosive devices ("IED"s). See "China Cracks Down on Cell-Phone Spam," http://www.informationweek.com/news/showArticle.jhtml?articleID=175700760

One More Note Re Prepaid Cellular

- "Bulk" purchases of prepaid cell phones in and of themselves may also trigger official investigations, as it did in Michigan (http://detroit.fbi.gov/dojpressrel/pressrel06/de081606.htm).
- Some retailers have begun to limit purchase quantities of prepaid cell phones, nominally to control the "arbitrage"-like resale of the loss-leader phone handsets abroad (see "WalMart limits prepaid cell phones to 2," http://www.msnbc.msn.com/id/15335329/), or to prevent the culling of lithium from the cell phone's lithium batteries for potential use as a reagent in the illicit production of methamphetamine.
- What a bizarre world in which we live, eh?

What About Content Sent To Your Cell?

- You may be surprised to learn that your phone company may control what content gets made available to you via your cell phone, either as a matter of complying with federal law, or as a matter of its own initiative.
- Sometimes this may be a good thing, as in the case of wireless spam, blockable by default when sent to registered domains used by cellular or other commercial mobile radio services, see www.fcc.gov/cgb/policy/DomainNameInput.html
- Other times, however, private access to content of your choice may be subject to your cellular provider's discretion, and some of those decisions may feel just a bit paternal/invasive...

www.vzwdevelopers.com/aims/public/wapContGuide.jsp

Inappropriate Content:

Alcoholic beverage-related

Tobacco-related (cigarettes, cigars, pipes, chewing tobacco, etc).

Guns/weapons-related (firearms, bullets, etc).

Illegal Drugs-related (marijuana, etc).

Pornographic-related (sex sites) or otherwise obscene.

Crime-related (dealing with the notorious).

Graphic violence (including certain types of game sites).

Noncompliance with any applicable law or regulation.

Encouraging or promoting violence or criminal conduct.

Gambling-related (casinos, lotteries, etc).

Involves unauthorized or unapproved use of Verizon Wireless' intellectual property.

Involves a copy or parody of current or past Verizon Wireless products or services.

Involves an implied affiliation, association or endorsement by, or favored status with Verizon Wireless.

Potentially Inappropriate Content:

Politics-related (lobbyists, PAC sites, political campaigns).

Death-related (funeral homes, mortuaries).

Other "controversial topics" (politics, social issues, etc.) as determined by Verizon Wireless in its discretion.

Conclusion

- On your way home today I hope you'll take a minute or two to reflect on the choices you've made in your own life – how you read your email, how you surf the web, the operating system you use and yes, even whether / how you use a cell phone or other mobile device.
- Only you can determine how much privacy and security you're willing to relinquish in favor of convenience, or even if any of the risks we've talked about today are of material importance for you. I urge you to choose carefully because once your privacy and security have been compromised, in many cases the damage will be irrecoverable.
- Well, that's probably more than enough for today, and sorry if I've run over – I really appreciate having had the chance to talk today! Are there any questions?