1. Introduction

Say that you are considering renting out your house to a couple and they currently live out of town. They might seem like nice people when you talk to them on the phone, but you don’t know them, and so before the introduction of computer information you’d maybe have asked for references, and if those came in looking good you’d hope that they weren’t faked and rent out the house to the couple. Another alternative would have been to hire an investigator in their current home town, but that was so expensive as to be prohibitive.

Now things have changed. A few days ago I needed an address for one of our former faculty members who retired and moved to Arizona. I entered her name in www.whitepages.com and selected Arizona, and it came back with the address and telephone number for her and her husband. So far, no problem. This very fast search has saved me guessing and trying a large number of Arizona telephone books at the library. However the page also has a button telling me that more information is available on her. Being curious I click that and it has a link which gives me the addresses (e- and street) of her neighbors. So now I can phone these people and ask them how well our former faculty member looks after their house, whether they have loud parties all of the time, and so on. Also, the page gives me a link where I can do a background check on our former faculty member and her husband, which includes “Criminal Check, Sex Offender Check, Bankruptcies, Tax Liens, Legal Judgments, Current & Previous Addresses, Alias Names, Roommates, Relatives, Family Members, Neighbors, Property Ownership, Mortgage Data, & more personal profile information.” This would cost me $49.95. If their phone number is unlisted than it appears that

What has happened is that online databases have let me get information about anyone, far faster and dramatically cheaper, than I would have been able to get a few years ago.
Clearly there has been a loss of privacy, but it is unclear whether overall this is good or bad. E.g., should the students in the CS 215 class be able to pay $2.50 each and share the cost to find out all of this information on me, or should they only be able to find out whether I’ve got a criminal record if they have good reason to know? On the other hand, if I’m hiring a baby sitter then knowing whether or not they are a sex offender could be very important to me. Another problem, of course, is how do I find out whether the information about me on different systems is even accurate? If, for example, it somehow confused me with some other Denbigh Starkey and listed me as a sex offender, would I ever even know why I was always being turned down for jobs?

The remainder of these notes will look at privacy issues from different standpoints. The FERPA legislation will discuss your rights as students. I’ll include the EFF recommendations on how to protect yourself from identity theft and look at state security breach and freeze laws. The other major section will be on the legal right to privacy in the US and the case that began the discussion, *Griswold vs. Connecticut*.

2. **Family Education Rights and Privacy Act (FERPA)**

As computers have tended to reduce privacy, a number of attempts have been made to help to protect individuals from loss of privacy and from related issues like identity theft. In education a landmark bill was the Family Education Rights and Privacy Act, also known as FERPA or the Buckley Amendment after the primary author.

Essentially FERPA lets parents and children inspect school education records and to request that any errors be corrected. If the school rejects a change request then formal hearings are required. This applies until the school rejects or attends a school past the high school level, in which case all rights pass to the student and parents lose all these rights.

Other than that the school cannot release any academic records except under very specific circumstances, which the bill lists as:

- a) School officials with legitimate educational interest;
- b) Other schools to which a student is transferring;
- c) Specified officials for audit or evaluation purposes;
- d) Appropriate parties in connection with financial aid to a student;
- e) Organizations conducting certain studies for or on behalf of the school;
- f) Accrediting organizations;
- g) To comply with a judicial order or lawfully issued subpoena;
- h) Appropriate officials in cases of health and safety emergencies; and
- i) State and local authorities, within a juvenile justice system, pursuant to specific State law.
Some of these restrictions become complicated to enforce. E.g., as a school official whose records should I have access to? Before we had computerized records there were copies of transcripts in departmental offices and in the Registrar’s Office. This provided pretty good protection for transcripts. Now transcripts are only online, and so what should I be able to access. I presumably need to access records for my advisees, but advising assignments can be fairly informal and often students come in to see me for advice who are technically assigned to someone else, or a student will come in from another department who is considering switching to CS, and I need to advise them on what requirements they have already satisfied. So MSU has taken the position that faculty, through the secure area of MyInfo, should have access to the transcripts of all students at MSU, and expect us to follow the FERPA requirements. If, however, I were to release a student’s transcript to someone unauthorized then I suspect that not only would I be liable, but MSU would be as well.

Another part of FERPA is:

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

This seems fairly clear, but universities have not always been sufficiently careful. E.g., when I was at WSU a student had requested a block on release of any information about her because she had been stalked in her home town, and was basically hiding in Pullman. Unfortunately she got a straight A average one semester, and so the computer sent a letter to her home newspaper with honor roll information. This forced her to leave Pullman and move to another out of state university, and when I left MSU a lawsuit had been initiated.

Most of the time we go as far as possible to meet not only the requirements of FERPA but also the intent behind the legislation. E.g., when we give examples of student work and transcripts to ABET, our accreditation agency, we black out student names, even though this is a permitted disclosure under the FERPA regulations.
3. Electronic Freedom Foundation

The primary organization dedicated to protecting online privacy and other online freedoms is the Electronic Freedom Foundation. Their Web page is at www.eff.org. This is the first source of information for most online freedom issues because although they tend to strongly oppose most government regulations, including many provisions of the Patriot Act, they provide good links to source materials on most issues.

So using their page will let you get to the information that you need to form your own views on most online freedom issues. I’ll start by discussing their recommendations for protecting your online privacy.

4. Protecting Your Privacy – EFF Recommendations

The Electronic Freedom Foundation has twelve recommended steps to help you to protect your online privacy. I’m directly quoting them below because they are far more comprehensive than anything I could have come up with.

After reading through them I’m somewhat distressed at how poor a job I do at protecting myself much of the time, and intend to improve.

1) Do not reveal personal information inadvertently.

You may be "shedding" personal details, including e-mail addresses and other contact information, without even knowing it unless you properly configure your Web browser. In your browser's "Setup", "Options" or "Preferences" menus, you may wish to use a pseudonym instead of your real name, and not enter an e-mail address, nor provide other personally identifiable information that you don't wish to share. When visiting a site you trust you can choose to give them your info, in forms on their site; there is no need for your browser to potentially make this information available to all comers. Also be on the lookout for system-wide "Internet defaults" programs on your computer (some examples include Window's Internet Control Panel, and MacOS's Configuration Manager, and the third-party Mac utility named Internet Config). While they are useful for various things, like keeping multiple Web browsers and other Internet tools consistent in how they treat downloaded files and such, they should probably also be anonymized just like your browser itself, if they contain any fields for personal information. Households with children may have an additional "security problem" - have you set clear rules for your kids, so that they know not to reveal personal information unless you OK it on a site-by-site basis?
2) Turn on cookie notices in your Web browser and/or use cookie management software or infomediaries.

"Cookies" are tidbits of information that Web sites store on your computer, temporarily or more-or-less permanently. In many cases cookies are useful and innocuous. They may be passwords and user IDs, so that you do not have to keep retyping them every time you load a new page at the site that issued the cookie. Other cookies however, can be used for "data mining" purposes, to track your motions through a Web site, the time you spend there, what links you click on and other details that the company wants to record, usually for marketing purposes. Most cookies can only be read by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie sharing rings. They can track which pages you load, which ads you click on, etc., and share this information with all of their client Web sites (who may number in the hundreds, even thousands.) Some examples of these cookie sharing rings are DoubleClick, AdCast and LinkExchange. For a demonstration of how they work, see: http://privacy.net/track/

Browsers are starting to allow user control over cookies. Netscape, for example, allows you to see a notice when a site tries to write a cookie file to your hard drive, and gives you some information about it, allowing you to decide whether or not to accept it. (Be on the lookout for cookies the function of which is not apparent, which go to other sites than the one you are trying to load, or which are not temporary). It also allows you to automatically block all cookies that are being sent to third parties (or to block all cookies, entirely, but this will make some sites inoperable). Internet Explorer has a cookie management interface in addition to Netscape-like features, allowing you to selectively enable or disable cookies on a site-by-site basis, even to allow cookies for a site generally, but delete a specific cookie you are suspicious about. With Internet Explorer you can also turn on cookies for a site temporarily then disable them when you no longer need them (e.g., at an online bookstore that requires cookies to process an order, but whom you don't want to track what books you are looking at, what links you are following, etc., the rest of the time.) Turning on cookie warnings will cause alert boxes to pop up, but after some practice you may learn to hit "Decline" so fast that you hardly notice them any more. The idea is to only enable cookies on sites that require them AND whom you trust. You may also wish to try out "alternative" browsers like Mozilla (Windows, Mac, Linux), Opera (Windows, Mac, Linux), Konqueror (Linux), and iCab (Mac), which may offer better cookie management.

You can also use cookie management software and services. One example is the Internet Junkbuster Proxy (http://www.junkbusters.com/ht/en/ijb.html). It runs on Win95/98/NT and Unix/Linux (no Mac version), and can selectively block cookies for you (and banner ads, to boot). interMute (http://www.intermute.com/) does likewise (and more - blocks popup windows, etc.; only runs under Windows). Another Windows-only solution is AdSubtract (http://www.adsubtract.com/) A comparable product (Linux, Solaris, Windows) is GuideScope (http://www.guidescope.com/home/) A Java-based solution called Muffin (http://muffin.doit.org/) is also available. While it will run on Mac, Windows and Unix systems, it is definitely for "power users", as it is complicated to set
up and operate effectively. Another recent option (Linux, Mac, Windows) is the (http://www.webwasher.com/), which has advanced cookie filtering capabilities, especially with the Seclude-It and Secretmaker plug-ins available at the same site. One more (Windows) is CookiePal (http://www.kburra.com/cpal.html), and yet another (Windows) is (http://www.thelimitsoft.com/cookie.html). There are also numerous "cookie eater" applications, some which run on a schedule or in the background, that delete cookie files for you. As with turning off cookies entirely, you may have trouble accessing sites that require certain cookies (though in most cases the worst that will happen is that you'll have to re-enter a login ID and password you thought were saved.) "Eating" the cookies periodically still permits sites to track what you're doing for a short time (i.e., the time between successive deletion of your cookie file), but thwarts attempts to discern and record your actions over time.

Yet another option is to use an "infomediary" (some are home-use software products, others may be network-based services), such as SeigeSoft's SiegeSurfer (http://www.siegesoft.com/html/tutorial.asp), Zero Knowledge Systems' Freedom (http://www.freedom.net), among others. These products/services act as a proxy or shield between you and sites you visit, and can completely disguise to Web sites where you are coming from and who you are (and intercept all cookies). Most are Windows-only at this point, though Anonymizer (http://www.anonymizer.com/3.0/affiliate/door.cgi?CMid=13763), Orangatango (http://www.orangatango.com/), and SafeWeb and (http://www.safeweb.com) also offer such services that are Web-based and not platform-dependent. WARNING: Do not confuse honest infomediaries with "identity management services" like Microsoft's Passport service or Novell's DigitalMe. While you may gain some temporary convenience at sites that support them, you'll lose essential privacy, because these services are not there to serve you but to serve marketing purposes by collecting a vast array of information about you and selling it.

The best solution doesn't exist yet: Full cookie management abilities built into the browsers themselves. Only increased user pressure on Microsoft, Netscape and other browser makers can make this happen. Users should ultimately be able to reject cookies on a whole-domain basis, reject all third-party cookies by default, reject all cookies that are not essential for the transaction at hand, receive notice of exactly what a cookie is intended for, and be able to set default behaviors and permissions rather than have to interact with cookies on a page-by-page basis. This just isn't possible yet. You may wish to contact the company that makes your browser software and demand these essential features in the next version.

3) Keep a "clean" e-mail address.

When mailing to unknown parties; posting to newsgroups, mailing lists, chat rooms and other public spaces on the Net; or publishing a Web page that mentions your e-mail address, it is best to do this from a "side" account, some pseudonymous or simply alternate address, and to use your main or preferred address only on small, members-only lists and with known, trusted individuals. Addresses that are posted (even as part of
message headers) in public spaces can be easily discovered by spammers (online junk mailers) and added to their list of targets. If your public "throw away" address gets spammed enough to become annoying, you can simply kill it off, and start a new one. Your friends, boss, etc., will still know your "real" address. You can use a free (advertising-supported) e-mail service provider like Yahoo Mail or Hotmail for such "side" accounts. It is best to use a "real" Internet service provider for your main account, and to examine their privacy policies and terms of service, as some "freemail" services may have poor privacy track records. You may find it works best to use an e-mail package that allows multiple user IDs and addresses (a.k.a. "personalities", "aliases") so that you do not have to switch between multiple programs to manage and use more than one e-mail address (though you may have to use a Web browser rather than an e-mail program to read your mail in your "throw away" accounts - many freemail providers do not allow POP or IMAP connections). If you are "required" to give an e-mail address to use a site (but will not be required to check your mail for some kind of access code they send you), you can use "someuser@example.com" (example.com is a non-existent site, set up by the Internet standards to be used as an example that will never accidentally coincide with anyone's real e-mail address, which is always a danger if you just make up one off the top of your head.)

4) Don't reveal personal details to strangers or just-met "friends".

The speed of Internet communication is often mirrored in rapid online acquaintanceships and friendships. But it is important to realize that you don't really know who these people are or what they are like in real life. A thousand miles away, you don't have friends-of-friends or other references about this person. Be also wary of face-to-face meetings. If you and your new e-friend wish to meet in person, do it in a public place. Bringing a friend along can also be a good idea. One needn't be paranoid, but one should not be an easy mark, either. Some personal information you might wish to withhold until you know someone much better would include your full name, place of employment, phone number, and street address (among more obvious things like credit card numbers, etc.) Needless to say, such information should not be put on personal home pages. (If you have a work home page, it may well have work contact information on it, but you needn't reveal this page to everyone you meet in a chat room.) For this and other reasons, many people maintain two personal home pages, a work-related one, and an "off duty" version. In the commercial sector, too, beware "fast-met friends". A common "social engineering" form of industrial espionage is to befriend someone online just long enough to get them to reveal insider information.

5) Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer.

In most US states and many if not most countries, employees have little if any privacy protection from monitoring by employers. When discussing sensitive matters in e-mail or other online media, be certain with whom you are communicating. If you replied to a mailing list post, check the headers - is your reply going to the person you think it is, or to the whole list? Also be aware that an increasing number of employers are monitoring
and recording employee Web usage, as well as e-mail. This could compromise home banking passwords and other sensitive information. Keep private data and private Net usage *private*, at home. See this *CNN/IDG* article on "snoopware" (which may not be limited to your office...):


6) **Beware sites that offer some sort of reward or prize in exchange for your contact information or other personal details.**

There's a very high probability that they are gathering this information for direct marketing purposes. In many cases your name and address are worth much more to them because they can sell it to other marketers (who can do the same in turn...) than what you are (supposedly) getting from them. Be especially wary of sweepstakes and contests. You probably won't win, but the marketer sure will if you give them your information.

7) **Do not reply to spammers, for any reason.**

"Spam", or unsolicited bulk e-mail, is something you are probably already familiar with (and tired of). If you get a spammed advertisement, certainly don't take the sender up on whatever offer they are making, but also don't bother replying with "REMOVE" in the subject line, or whatever (probably bogus) unsubscribe instructions you've been given). This simply confirms that your address is being read by a real person, and you'll find yourself on dozens more spammers' lists in no time. If you open the message, watch your outgoing mail queue to make sure that a "return receipt" message was not generated to be sent back to the spammer automatically. (It is best to queue your mail and send manually, rather than send immediately, so that you can see what's about to go out before it's actually sent. You should also turn off your mailer's automatic honoring of return receipt requests, if any.) If you have a good Internet service provider, you may be able to forward copies of spam e-mail to the system administrators who can route a complaint to the ISP of the spammer (or if you know a lot about mail headers and DNS tools, you can probably contact these ISPs yourself to complain about the spammer.) If you are getting spammed a lot, there are a variety of filters and anti-spam services available, including: Spam Hater (http://www.cix.co.uk/~net-services/spam/spam_hater.htm) for Windows users; TAG (http://alcor.concordia.ca/topics/email/auto/procmail/spam) for experienced Unix users; SpamBouncer (http://www.spambouncer.org) for experienced Unix users (works well with TAG); BrightMail (http://www.brightmail.com/) for ISPs; SpamCop (http://spamcop.net/) for anyone;

More information on fighting spam is available at:

Elsop's Anti-Spam Page (http://www.elsop.com/wrc/nospam.htm);
MaximumDownforce's Info-n-Links Page( http://www.maximumdownforce.com/hotlinks.html);
Whew's Anti-Spam Campaign (http://www.whew.com/Spammers/).
Many of these are difficult to use for novices, and some require Unix expertise. Others are services that deal with ISPs only, not end users.

8) Be conscious of Web security.

Never submit a credit card number or other highly sensitive personal information without first making sure your connection is secure (encrypted). In Netscape, look for a closed lock (Windows) or unbroken key (Mac) icon at the bottom of the browser window. In Internet Explorer, look for a closed lock icon at the bottom (Windows) or near the top (Mac) of the browser window. In any browser, look at the URL (Web address) line - a secure connection will begin "https:" instead of "http:". If you are at a page that asks for such information but shows "http:" try adding the "s" yourself and hitting enter to reload the page (for Netscape or IE; in another browser, use whatever method is required by your browser to reload the page at the new URL). If you get an error message that the page or site does not exist, this probably means that the company is so clueless - and careless with your information and your money - that they don't even have Web security. Take your business elsewhere.

Your browser itself gives away information about you, if your IP address can be tied to your identity (this is most commonly true of DSL and broadband users, rather than modem users, who are a dwindling minority). For a demo of how much detail is automatically given out about your system by your browser, see:
http://privacy.net/analyze/.

Also be on the lookout for "spyware" - software that may be included with applications you install (games, utilities, whatever), the purpose of which is to silently spy on your online habits and other details and report it back to the company whose product you are using. One MS Windows solution for disabling spyware is the Ad-aware program (shareware, from http://www.lavasoft.de/), which can remove spyware from your computer; it is based on a large collaboratively maintained database of information about spyware. Linux and Mac products of this sort are likely to appear soon.

Java, Javascript and ActiveX can also be used for spyware purposes. Support for these scripting languages can be disabled in your browser's configuration options (a.k.a. preferences, settings, or properties). It is safest to surf with them turned off, and only turn them on when a site you trust and want to use requires them. If you don't know if your browser supports these languages or don't know if they are turned on you can use BrowserSpy to find out (along with a lot of other information about your Web browsing software): http://gemal.dk/browserspy/

Another form of spyware consists of "webbugs", which typically manifest themselves as invisible or nearly invisible image files tied to cookies and JavaScripts that track your Web usage. See http://www.google.com/search?hl=en&q=webbugs+%22web+bugs%22 for more information on webbugs. See also this webbug FAQ, http://www.nthelp.com/OEtest/web_bug_faq.htm for more details. Dealing with webbugs when they are embedded in an otherwise legitimate page is thorny, as there isn't a surefire
way to distinguish between webbugs and run-of-the-mill image files. But see the Privacy Foundation's Bugnosis webbug detector (http://www.bugnosis.org/ - Windows MSIE only). When webbugs are loaded into popup pages, the solution is to close the popups (usually a small page with an ad, though some of them are "micropages" that you can barely see. A few may even use JavaScript tricks to keep you from closing them. If this happens, close all other browser windows, then you should be able to close the bug window). Another tip for defeating webbugs is to reject any cookies from Doubleclick, AdCast, LinkExchange and other "ad exchange networks" (cookie sharing rings), and any other cookies that are not from the site you are currently visiting (most third-party cookies are basically webbugs). Lastly on this topic, be aware that HTML-capable e-mail programs and Usenet newsgreaders make webbugs work in your e-mail and newsgroups. If your mailer or newsreader has an option to turn off cookie support, you should certainly do so. There is hardly any imaginable legitimate use for a cookie in an email or a newsgroup posting.

9) Be conscious of home computer security.

On the other side of the coin, your own computer may be a trouble spot for Internet security. If you have a DSL line, broadband cable modem or other connection to the Internet that is up and running 24 hours (including T1 at the office without a firewall or NAT), unlike a modem-and-phone-line connection, be sure to turn your computer off when you are not using it. Most home PCs have pitifully poor security compared to the Unix workstations that power most commercial Web sites. System crackers search for vulnerable, unattended DSL-connected home computers, and can invade them with surprising ease, rifling through files looking for credit card numbers or other sensitive data, or even "taking over" the computer and quietly using it for their own purposes, such as launching attacks on other computers elsewhere - attacks you could initially be blamed for. Firewall hardware and software is another option that can protect you from these kinds of attacks (available at any computer store; freeware and shareware implementations may be available at sites like http://www.shareware.com or http://www.download.com.

10) Examine privacy policies and seals.

When you are considering whether or not to do business with a Web site, there are other factors than a secure connection you have to consider that are equally important to Web security. Does the site provide offline contact information, including a postal address? Does the site have a prominently-posted privacy policy? If so, what does it say? (Just because they call it a "privacy policy" doesn't mean it will protect you - read it for yourself. Many are little more than disclaimers saying that you have no privacy! So read them carefully.) If the policy sounds OK to you, do you have a reason to believe it? Have you ever heard of this company? What is their reputation? And are they backing up their privacy statement with a seal program such as TRUSTe (http://www.truste.org/) or BBBonline (http://www.bbbonline.org/)? (While imperfect, such programs hold Web sites to at least some minimal baseline standards, and may revoke, with much fanfare, the approval-seal licenses of bad-acting companies that do not keep their word.) If you see a
seal, is it real? Check with the seal-issuing site to make sure the seal isn't a fake. And examine terms carefully, especially if you are subscribing to a service rather than buying a product. Look out for auto-rebilling scams and hidden fees.

11) Remember that YOU decide what information about yourself to reveal, when, why, and to whom.

Don't give out personally-identifiable information too easily. Just as you might think twice about giving some clerk at the mall your home address and phone number, keep in mind that simply because a site asks for or demands personal information from you does not mean you have to give it. You do have to give accurate billing information if you are buying something, of course, but if you are registering with a free site that is a little too nosy for you, there is no law (in most places) against providing them with pseudonymous information. (However, it would probably be polite to use obviously fake addresses, such as "123 No Such Street, Nowhere, DC 01010". If they are generating mailings based on this information - presumably in accordance with the terms of their privacy policy - they can probably weed such addresses out and not waste the postage on them. Definitely do NOT use someone else's real address!) However, if you are required to agree to terms of service before using the free service, be sure those terms do not include a requirement that you provide correct information, unless the penalty is simply not being allowed to use the service any more, and you're willing to pay that price if they figure out you are not providing them with your actual personally-identifiable information.

12) Use encryption!

Last but certainly not least, there are other privacy threats besides abusive marketers, nosy bosses, spammers and scammers. Some of the threats include industrial espionage, government surveillance, identity theft, disgruntled former associates, and system crackers. Relatively easy-to-use e-mail and file encryption software is available for free, such as Pretty Good Privacy (PGP, available at: http://www.pgpi.org/), which runs on almost all computers and even integrates seamlessly with most major e-mail software. Good encryption uses very robust secret codes, that are difficult if not impossible to crack, to protect your data. You can also use specialized services (some free, some pay) that go beyond infomediary services, including running all connections through a securely encrypted "tunnel", anonymous dialup, even anonymous Web publishing. Anonymizer (http://www.anonymizer.com/3.0/affiliate/door.cgi?CMid=13763) offers all of these services. Another type of product is SSH tunnelling (port forwarding) packages, such as FSecure SSH (http://www.fsecure.com/products/ssh/), and SecureCRT (http://www.vandyke.com/products/securecrt/).

Hopefully some day soon, good encryption and computer security will simply be included in all ISP services and operating systems, but for now you have to actively seek out good service providers and add-on products.
For more information on protecting your online privacy:

- EFF Privacy Archive - http://www.eff.org/Privacy/

5. Security Breaches and State Laws

The 2005 Montana legislature passed a new law to require notice if private information on a computer system is disclosed:

**Section 7. Computer security breach.** (1) Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(2) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal information was, or is reasonably believed to have been acquired by an unauthorized person.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, the following definitions apply:

(a) "Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) (i) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) social security number; (B) driver's license number or state identification card number; (C) account number or credit or debit
card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

This law is based on a California electronic privacy law, but is somewhat weaker than that law, which doesn’t, for example, limit notifications to residents of that state.

The California law has most famously been applied to universities, with two notable cases:

- On March 11, 2005, someone was seen stealing a laptop from a “secure area” in the Berkeley Graduate Division Admissions Office\(^1\), which wasn’t occupied at the time. Unfortunately the computer contained information on 98,369 people who had applied to the graduate school. While most of the data was on people who had applied between 2001 and 2004, some data went as far back as the 1970’s. For at least one third of the applicants the data included names, SSNs, dates of birth, and addresses, which is everything that is needed for identity theft. Berkeley announced that they were making every reasonable effort to contact as many as possible of the individuals. They had to do this even though there was no evidence that any of the information had been misused.

- Also in March, 2005, hackers broke into the food services computer at California State University, Chico\(^2\), and were able to access names, SSNs, and addresses on 59,000 students, staff, and faculty who had used their facilities over the last five years. Again there was no evidence that the hackers were looking for this information, but again Chico was required to contact everyone on the list.

- In a case outside California, but also in March, 2005, a hacker broke into a Boston College Computer\(^3\) that contained names, SSNs, addresses, and fund raising information on about 137,000 alumni. Again the purpose of the hack didn’t seem to be to access this information but Boston College was contacting all of the potentially affected individuals through their alumni newsletter. The university said that the information was on a computer managed by an outside entity, and that apparently its security patches were not up to date.

These three cases, particularly the first and the third, really emphasize the fact that it can be very expensive to be sloppy about security. Just trying to contact tens of thousands of people, many of who will have moved, is incredibly time-consuming, and hence expensive (although the approach taken at BC to use a newsletter would be cheap). Even worse, at BC the bad publicity could significantly affect donations and at Berkeley it might affect applications.

39 states and the District of Columbia (in October 2007) have enacted security breach laws, including California and Montana, as discussed above. Massachusetts did not pass their security breach and security freeze law until August 7\(^{th}\), 2007, which let BC get away with just informing people in their newsletter, although under the new MA law if more than

\(^1\) http://www.internetnews.com/security/print.php/3493721
\(^2\) http://www.internetnews.com/security/article.php/3491726
\(^3\) http://www.internetnews.com/security/article.php/3491196
500,000 people were affected or if the cost of notification would exceed $250,000, a less onerous notification called a substitute notice is allowed.\textsuperscript{4}

The first major security breach whose only goal appeared to be to access records for identity theft was at ChoicePoint in February, 2005. ChoicePoint maintains records on nearly every adult in the US, which includes names, SSNs, addresses, and much more. Someone set up 50 fake business accounts and used them to access over 120,000 ChoicePoint records. Because of the California law they were required to send out notices to most of the people affected. Since then, LexisNexis, a similar data aggregator, announced in March 2005 that 32,000 of their records which contained names, addresses, and SSNs, had been accessed by someone using the name and password of one of their customers.

Since then many much bigger computer security breaches have been discovered, but in many cases it has been difficult to discover whether it was just a breach of security or whether these security breaches also led to misuse of data. For example on October 4, 2007, the Massachusetts Division of Professional Licensure sent disks with information on 450,000 licensed professionals to 23 agencies for marketing purposes. They accidentally included SSNs for these people on the disks, instead of just the names and addresses that had been requested, but nobody knows whether this data was misused. The biggest case that I know of was when on July 3, 2007, a Fidelity National Information Services employee stole information, including bank account and credit card information, on 8.5 million people.\textsuperscript{5}

On October 12, 2007, MSU announced a security breach related to applications to the Extended University. Details are sketchy, but apparently a hacker was able to break into a file that contained SSNs and credit card numbers of the applicants. The data was encrypted, so under the law (Section 7-4-b-i) MSU was not required to contact the people whose records were in the files that were compromised, but they took the safe route and did inform them. This notification included information on how to contact the three big credit agencies and monitor or freeze credit information.

\section*{6. State Security Freeze Laws}

Thirty-nine states and the District of Columbia have security freeze laws, most of which have been enacted relatively recently. The Montana security freeze law came into effect on July 1, 2007.\textsuperscript{6} What these laws allow you to do is to freeze access to your credit information. Typically a security freeze law requires that credit companies and other data aggregators must provide a convenient mechanism for people to block all access to their credit information and also to turn access back on when requested. So most of the time

\textsuperscript{4} This substitute notice still requires emails to all consumers, notice on the Web page, and publication in statewide media.

\textsuperscript{5} The initial figures given by Fidelity said that there were 2.3 million stolen records, but 8.5 million was the number that they used later in their SEC filing.

\textsuperscript{6} See \url{http://www.doj.mt.gov/consumer/consumer/securityfreeze.asp} for the MT Department of Justice page describing how to use the law to freeze credit files.
you can turn off access to most personal information, but if you are about to, say, apply for a mortgage then you can turn it back on for a while.

7. Legal Right to Privacy

The right of privacy has had many political and legal implications since it was legitimized in a 1965 Supreme Court ruling, *Griswold vs. Connecticut*. The right of privacy was subsequently used by the Supreme Court in *Roe vs. Wade*, which made abortions legal in the US.

First some brief history. In 1961 the Executive Director of the Planned Parenthood League of Connecticut (Griswold) and a physician and professor at the Yale Medical School (Buxton) were arrested for violating Connecticut state laws against contraception. They operated a center in New Haven from November 1 to November 10, 1961, when they were arrested and ultimately convicted and fined $100 each. At the New Haven clinic they gave information, instruction, and medical advice to married people on how to prevent conception. They examined the wife and prescribed the best contraceptive device or material for her use. In these days this might seem commonplace, but at the time there was a state law which included:

*Any person who uses any drug, medicinal article or instrument for the purpose of preventing conception shall be fined not less than fifty dollars or imprisoned not less than sixty days nor more than one year or be both fined and imprisoned.*

They were charged for conspiracy under another law that included:

*Any person who assists, abets, counsels, causes, hires or commands another to commit any offense may be prosecuted and punished as if he were the principal offender.*

Their goal was to challenge the state law against providing contraceptive advice to married couples. Lower court rulings accepted the convictions, but the Supreme Court overturned them. The majority opinion was written by Justice Douglas who stated that there are many rights which are not explicitly stated in the Constitution like the ability to select a school for one’s children, and so he discussed and supported a new right of privacy in marriage with the statement “there are fundamental personal rights such as this one, which are protected from abridgment by the Government though not specifically mentioned in the Constitution.” The two dissenting justices supported the law, even though they disagreed with it, basically because they didn’t agree with the “right of privacy” argument. Justice Stewart’s dissenting opinion is so short that it can be quoted in full:

*Since 1879 Connecticut has had on its books a law which forbids the use of contraceptives by anyone. I think this is an uncommonly silly law. As a practical*
matter, the law is obviously unenforceable, except in the oblique context of the present case. As a philosophical matter, I believe the use of contraceptives in the relationship of marriage should be left to personal and private choice, based upon each individual’s moral, ethical, and religious beliefs. As a matter of social policy, I think professional counsel about methods of birth control should be available to all, so that each individual’s choice can be meaningfully made. But we are not asked in this case to say whether we think this law is unwise, or even asinine. We are asked to hold that it violates the United States Constitution. And that I cannot do.

Even though Douglas’ opinion actually established a marital right of privacy, his arguments were so broadly stated that they established a right of privacy under US law.

There are still disagreements over this ruling. E.g., on October 17, 2005, Senator Arlen Specter announced that Supreme Court nominee Harriet Miers had told him that she believed that *Griswold vs. Connecticut* was “rightly decided.” After a backlash from some senators the next day he said that she had called him to say that she had been misunderstood. The issue is that *Roe vs. Wade*, the decision that legalized abortion, was based on the right of privacy developed in *Griswold vs. Connecticut*. Most commentators believed that Specter, who is a constitutional law expert, would not misunderstand such a critical discussion, and that Miers had been forced, politically, to back off quickly and say that she hadn’t taken a position on either *Griswold vs. Connecticut* or the right of privacy. Opposition from conservative groups increased and on October 27, 2005, President Bush withdrew the Miers nomination saying that the withdrawal was at her request.

### 8. Mining Private Data

Computers, and the financial changes that they have permitted, have made it possible to find out far more about people than was ever possible before. In particular computers have led to credit cards and online purchasing as normal ways to pay for things. This provides considerable personal information that can be used to learn a lot about issues that would otherwise be private.

Some things are obvious; e.g., if I were to use a credit card to buy subscriptions to certain online sites, then I am releasing information to the databases that I would probably prefer to keep private, but this doesn’t require any mining. Some things might require data mining; e.g., if every time my wife goes to a conference I take a trip to Roundup, then there might be cause for blackmail. Before computer databases this sort of behavior pattern would never have been noticed, but now my wife buys her plane tickets using a credit card, and if I were to go to Roundup then I would buy gas at some point,

---

presumably with a credit card. And if I always bought jewelry and flowers before leaving on those trips using a credit card, then that information would also be available.

The biggest danger to privacy is that more and more information has become available and there is an increased ability to mine all of that data.

9. Clipper Chip

In 1992 AT&T decided to sell a relatively cheap device to the public which could encrypt voice phone calls, which caused a lot of concern to law enforcement agencies because they worried that this device would make wiretaps impossible to operate. The Department of Justice proposed an alternative encryption device called the Clipper Chip, which appeared to provide extremely good encryption under most circumstances. The exception was that federal agencies had a decryption code, held by two escrow agents, which would let them decrypt any traffic that used the clipper chip. In 1993 President Clinton who named Clipper as a national standard for telephone encryption. Later he reduced this to being a voluntary standard.

Things became weird when the US government proposed the clipper technology as an international standard, although the back door encryption would only be available to the US. This attempt failed.

A number of groups opposed Clipper, including the Electronic Freedom Foundation (EFF), the Electronic Privacy Information Center (EPIC), and the Computer Professionals for Social Responsibility (CPSR). By 1996 Clipper was effectively dead, and in 1998 the NSA declassified Skipjack and released the algorithm. By then increased computer power had raised the issue that Clipper could probably be broken using brute force approaches.

---

8 The National Security Agency at first classified the underlying technology, which they named Skipjack, so nobody in the public knew how it worked. However NIST did a review of Skipjack and recommended approval of the underlying algorithm.

9 A related device, called capstone, was developed for data transmissions.