Has Privacy Been Lost Forever?
Security and Personal Privacy In The Cyber Age

What is privacy? The right to privacy refers to the concept that one's personal information is protected from public scrutiny. U.S. Justice Louis Brandeis called it "the right to be left alone." While not explicitly stated in the U.S. Constitution, some amendments provide protections.

Statutory law most often protects the right to privacy. An example is the Health Information Portability and Accountability Act (HIPAA), which protects a person's health information. In addition, the Federal Trade Commission (FTC) historically has enforced the right to privacy in various privacy policies and statements.

A couple of decades ago privacy issues centered on what people did in the privacy of their homes. The passage of time and multiple court decisions have generally settled the law governing this type of privacy. Now the controversy has shifted to the digital realm.

The Internet is more than 45 years old. Its original Internet protocols were designed to support the sending of electronic mail from one computer to another. However, some 15 years later, its underlying technologies enabled creation of the World Wide Web and our global communications network. Today the user base has swollen to over 3.4 billion global users and is used extensively for business and personal interests.

Leaving aside the issue of government surveillance and stolen identities, a significant motivation for the collection of personal data is the directed ad business model used by platforms such as Facebook and Google, which is a major source of revenue for those companies. In addition, they sell that information about us to third parties.

Internet Service Providers (ISP)s have been lobbying Congress for years to allow them to collect the same information as social media platforms mentioned above. This month, Congress passed and the President signed a bill that would allow companies that provide access to the Internet to collect and sell the information produced from our on-line activities to third parties. This law repealed an Internet privacy rule proposed by the FCC. Under the rule, Internet Service Providers (ISPs) would have needed to get a user's permission to share that information with a third party. As a result of the law, that step is not required.
http://www.npr.org/sections/alltechconsidered/2017/03/28/521813464/as-congress-repeals-internet-privacy-rules-putting-your-options-in-perspective

As mentioned above, Internet entities such as Google, Yahoo, Facebook and others already collect personal information to support their directed ad model, but users can avoid Google, Yahoo and Facebook and avoid giving up such information. It's a lot harder (probably impossible) to avoid providing this information to one's ISP. Often people have only one choice of an ISP. This restricted choice was a major reason for the FCC rule.

Many messaging services have adopted end-to-end encryption that prevents anyone besides the sender and recipient from viewing the contents of a message. However, not everyone agrees this is a good idea—especially law enforcement. Over the past couple of years there have been several incidents when law enforcement demanded access to encrypted

messages or devices. WhatsApp, a popular messaging service utilizes end-to-end encryption and it is impossible for the company (Facebook) to see message content or provide it to a third party. This has caused the company some problems. The use of WhatsApp was blocked for a short time in Brazil because of the company's inability to provide information to authorities about a criminal case. More recently a UK minister has argued against the use of messaging encryption. http://www.reuters.com/article/us-britain-security-rudd-idUSKBN16X0BE?feedType=RSS&feedName=technologyNews

Just this month Twitter was hit with a demand from the Federal Government for information about the identity of a user who has been posting tweets critical of the President. The demand came without any specific claim of illegality. Should Federal, State or Local governments have the right to know the identities of people who criticize them and who might then be exposed to retaliation? http://www.reuters.com/article/us-twitter-lawsuit-idUSKBN1782PH?feedType=RSS&feedName=technologyNews

There are several steps you can take to help minimize your data exposure. First, you may have noticed that when you go to a banking or financial web site, the address (URL) is slightly different, i.e. https://www.website.com vs. http://www.website.com. The subtle difference is the "https" vs. "http". The "s" on the end of "https" means that communication to that site is encrypted and your ISP will not be able to see what you are doing. More and more non-financial web sites are using a "https" version. Your ISP won't be able to capture your data when you use a "https" connection, but it will capture the fact that you visited that site.

Another option is using a Virtual Private Network (VPN) to avoid data capture by your ISP. A VPN creates a secure, encrypted connection between your device and a private server somewhere else, preventing anyone from seeing what you send. When you browse the internet, data goes to the server, which passes it securely back to you. When you send data, it appears to come from the server, not your computer. While you aren't anonymous—the VPN can see your traffic, and law enforcement can request information from VPN companies—it obscures what you're doing online. The downside to using VPNs is that your connection will be slower. Also, you need to be careful to find a VPN with a strong privacy policy.

Even if you were to decide not to use a VPN on your home network in order to avoid data collection from an ISP, they can be a good idea when you are using public WIFI networks. Almost anyone can capture your data if you are on a public WIFI network (like Starbucks) and not using either encrypted messaging or "https" websites.

http://www.pcworld.com/article/2031908/the-5-biggest-online-privacy-threats-of-2013.html

http://www.livescience.com/37398-right-to-privacy.html

http://gilc.org/privacy/survey/intro.html

http://www.theverge.com/2017/3/31/15138526/isp-privacy-bill-vote-trump-marsha-blackburn-internet-browsing-history

http://www.pcadvisor.co.uk/feature/internet/how-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780/