"All the News I Feel Like Printing."

Science Comm. Times

Golden CO

VOL.I. . . No.2 *OCTOBER 18, 2017* ZERO DOLLARS

Privacy: A Thing of the Past?

By BRENNAN FIECK

In 2010, as an April Fools joke, a company name "GameStation" updated its terms and conditions to include a clause legally entitling them to the "immortal soul"s of any who accepted the terms. The company did not enforce this policy, and emailed all the users that accepted it to reassure them, but it's this same trickery that allows companies like Facebook to legally spy on their users.

It seems to be more and more the case as time wears on that the Western Democracies are sacrificing personal liberties in the name of safety. What is more sinister than the massive breaches of privacy that have become commonplace is the degree to which they are being perpetrated without the knowledge of the general public. For example, a close reading of Google's privacy policy shows that they are able to read all incoming and outgoing emails for any given Gmail account, and sell that information to advertisers. Facebook routinely tracks its users' Internet browsing, even after they have left the Facebook website itself, then sells that information to advertisers.

These both seem pretty unreasonable, but are both totally legal and are completely overlooked by users scrolling through sometimes dozens of pages of an End User License Agreement (EULA). Unfortunately, "unreasonable" is a fairly subjective term, and is currently the only metric against which an EULA may be judged.

But it isn't just sites themselves that participate in this spying. As of March 23rd 2017, the US Senate struck down rules that would require Internet Service Providers (ISPs) to ask for permission before collecting and selling information gathered from their users. What this means is that anyone with enough money to afford it can buy your personal Internet search history. It may be the case that you "have nothing to hide", but that does not mean you "have nothing to fear". If you use an unencrypted email client, such as Gmail (which as of August 2017 is the 2nd largest email client with approx. 23% of the market share - reported by Litmus Email Analytics) then this could easily include the contents of emails on that service, and possibly Facebook messages and things of that nature. In a world where communication is increasingly taking place over the Internet. Anything you've ever said online, possibly even those with the expectation of privacy, are fair game to be quoted, misquoted, taken out of context, and in general paraded around for anyone to see.

Even more troubling, if you've used Google Maps or similar services, your locations and itenerary could become public knowledge. In 2006 the website "Gawker" launched a new app, troublingly titled "Gawker Stalker", which allowed users to report seeing celebrities with additional comments. Shockingly, this tool was not struck down due to legal action, but due to public outrage. Widely regarded as a dangerous tool enabling deranged killers to easily find their targets, the app received massive blowback and was taken down within a year. What this means, however, is that giving away or selling a person's physical location at all hours of the day may still be totally legal.

Today, ISPs are being allowed to do essentially the same thing, and are faced with nothing more than quiet acceptance. A person's personal history, identity and full contact information are slowly becoming totally exposed to anyone who wants them. Even if this information is being stored with the "innocent" intention of improving customer experience - itself a ludicrous statement from companies like Verizon and Samsung who have already been caught spying on users back when it was still illegal - that is no more comforting in a world where a company like Equifax can be breached, lose the information of 145.5 million US citizens (and between 408,000 and 44 million foreign citizens), not report it for 6 weeks while selling stocks and buying services that victims would need and changing leadership to ensure the right patsy takes the fall, then proceed to not only profit off of their incompetence, but fall for and participate in phishing scams causing even more damage.

Our personal information isn't safe in the hands we've placed it in, and these organizations have failed us before. A lack of transparency, accountability, and a refusal to even reconcile damages ensures that if nothing changes, we will all eventually pay for the mistakes of a few. I encourage you to write to your representatives and tell them to care more about protecting your identity, and pass laws that keep up with today's technology.