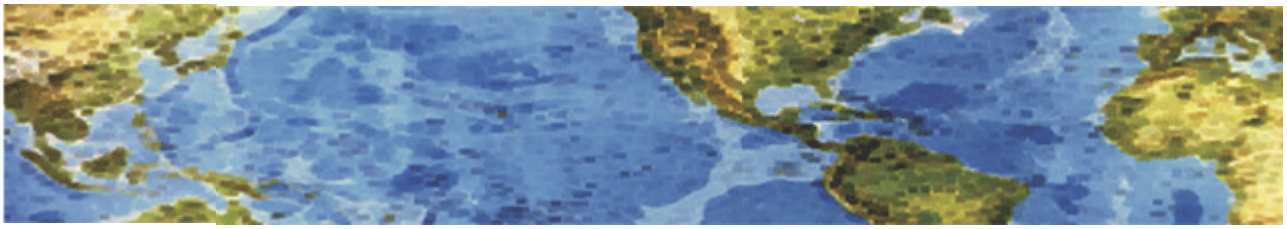
HALL ASSOCIATES



Risk-Based Decision Making Commentary
28 May 2013 Newsletter

What is the Future of Privacy?

Everyone needs to understand how thoroughly cyber stuff permeates every aspect of our lives – both business and personal. I recently ran across several articles on how the Internet of Things affects/interacts with our information and have extracted some of the information in them for this newsletter. The URLS for the full articles are at the end of this newsletter.

The Internet has turned into a massive surveillance tool. We're constantly monitored on the Internet by hundreds of companies -- both familiar and unfamiliar. Everything we do there is recorded, collected, and collated -- sometimes by corporations wanting to sell us stuff and sometimes by governments wanting to keep an eye on us.

Ephemeral conversation is over. Wholesale surveillance is the norm. Maintaining privacy from anyone able to pay for information is basically impossible, and any illusion of privacy we maintain is based either on ignorance or on our unwillingness to accept what's really going on. It's about to get worse, though. Companies such as Google may know more about your personal interests than your spouse, but so far it's been limited by the fact that these companies only see computer data. And even though your computer habits are increasingly being linked to your offline behavior, it's still only behavior that involves computers.

The “Internet of Things” refers to a world where much more than our computers and cell phones is Internet-enabled. Soon there will be many more Internet-connected modules on our cars and home appliances. Internet-enabled medical devices will collect real-time health data about us. There'll be Internet-connected tags on our clothing. In its extreme, everything can be connected to the Internet. It's really just a matter of time, as these self-powered wireless-enabled computers become smaller and cheaper. Lots has been written about the "Internet of Things" and how it will change society for the better. It's true that it will make a lot of wonderful things possible, but the "Internet of Things" will also allow for an even greater amount of surveillance than there is today. The Internet of Things gives the governments and corporations that follow our every move something they don't yet have: eyes and ears.

Soon everything we do, both online and offline, will be recorded and stored forever. The only question remaining is who will have access to all of this information, and under what rules. We're seeing an initial glimmer of this from how location sensors on your mobile phone are being used to track you. Of course your cell provider needs to know where you are; it can't route your phone calls to your phone otherwise. But most of us broadcast our location information to many other companies whose apps we've installed on our phone. Google Maps certainly, but also a surprising number of app vendors who collect that information. It can be used to determine where you live, where you work, and who you spend time with.

HALL ASSOCIATES

Medical devices are starting to be Internet-enabled, collecting and reporting a variety of health data. Wiring appliances to the Internet is one of the pillars of the smart electric grid. Yes, there are huge potential savings associated with the smart grid, but it will also allow power companies - and anyone they decide to sell the data to -- to monitor how people move about their house and how they spend their time. Drones are another "thing" moving onto the Internet. As their price continues to drop and their capabilities increase, they will become a very powerful surveillance tool. Their cameras are powerful enough to see faces clearly, and there are enough tagged photographs on the Internet to identify many of us. We're not yet up to a real-time Google Earth equivalent, but it's not more than a few years away. And drones are just a specific application of CCTV cameras, which have been monitoring us for years, and will increasingly be networked.

Google's Internet-enabled glasses -- Google Glass -- are another major step down this path of surveillance. Their ability to record both audio and video will bring ubiquitous surveillance to the next level. Once they're common, you might never know when you're being recorded in both audio and video. You might as well assume that everything you do and say will be recorded and saved forever. In the longer term, the Internet of Things means ubiquitous surveillance. If an object "knows" you have purchased it, and communicates via either Wi-Fi or the mobile network, then whoever or whatever it is communicating with will know where you are. Your car will know who is in it, who is driving, and what traffic laws that driver is following or ignoring. No need to show ID; your identity will already be known. Store clerks could know your name, address, and income level as soon as you walk through the door. Billboards will tailor ads to you, and record how you respond to them. Fast food restaurants will know what you usually order, and exactly how to entice you to order more. Lots of companies will know whom you spend your days -- and nights -- with. Facebook will know about any new relationship status before you bother to change it on your profile. And all of this information will all be saved, correlated, and studied. Even now, it feels a lot like science fiction.

Lots of these devices have, and will have, privacy settings. But these settings are remarkable not in how much privacy they afford, but in how much they deny. Access will likely be similar to your browsing habits, your files stored on Dropbox, your searches on Google, and your text messages from your phone. All of your data is saved by those companies -- and many others -- correlated, and then bought and sold without your knowledge or consent. **You'd think that your privacy settings would keep random strangers from learning everything about you, but it only keeps random strangers who don't pay for the privilege -- or don't work for the government and have the ability to demand the data.** Power is what matters here: you'll be able to keep the powerless from invading your privacy, but you'll have no ability to prevent the powerful from doing it again and again.

HALL ASSOCIATES

If You Want True Privacy, Use Something Other Than Skype

Ever since Microsoft's acquisition of Skype in 2011, people with a predilection for secret communications have been increasingly suspicious of the massively popular VoIP app's claims surrounding privacy. And over the past week, reports have shown just how much Microsoft can see of people's messages. Simple technical tests proved a Microsoft machine accessed links sent over Skype. According to Ars Technica, that has proven Microsoft can and does look at plain text sent by users. This has blown away the myth that Skype provides end-to-end encryption, it was suggested.
A Skype spokesperson sent the following from its privacy policy: "Skype uses automated scanning within Instant Messages and SMS to (a) identify suspected spam and/or (b) identify URLs that have been previously flagged as spam, fraud, or phishing links. Skype will retain your information for as long as is necessary to: (1) fulfill any of the Purposes (as defined in article 2 of this Privacy Policy) or (2) comply with applicable legislation, regulatory requests and relevant orders from competent courts."

Skype does store information on users' interactions and it can access communications when it chooses, albeit by a scanning tool called SmartScreen. It remains unclear how exactly the technology decides which messages to scan, which has concerned some. Microsoft is doing so largely for security purposes, to check links aren't pointing users to malicious sites, and to respond to law enforcement requests when they come in. As noted in Microsoft's first ever transparency report from earlier this year, the UK police are particularly hungry for Skype data, making more requests for it than any other force in the world. To be fair, Microsoft's scanning of Skype messages isn't too different from techniques Facebook reportedly employs, and what any number of other online services do, too. These companies have a duty to make sure their services aren't abused to circulate malware.

Xbox One surveillance machine privacy

Microsoft announced the next generation of its gaming console today, called the Xbox One. Among the new features are biometrics that promise to know you inside and out, which raise some serious privacy concerns. We'll take you through them one by one.

The Xbox One has a lot of new features, including more powerful hardware that integrates with TV, a game DVR that always records your gaming so you can upload highlights later, and dual-screen capability, letting you do things like have a browser window open alongside a game screen (so you can look at a walkthrough or tweet about a game while you're playing it). It has voice activation and facial recognition. Every Xbox One will come with a Kinect, an accessory that tracks players' movements to tie what you're doing in your living room to what's happening in-game. It's been especially popular with dance and fitness games like Dance Central and Your Shape. The Kinect's built-in HD camera has 60% more field of vision this time around and "can see fine details like fingers and facial features." It can track up to 6 people at once, 4 more than the previous Kinect model.
The Kinect will also be able to detect heart rate, which will be helpful during those fitness games to check if you're working as hard as you should be (or if your heart suddenly stops beating, will the super intelligent Kinect call an ambulance for you?)

HALL ASSOCIATES

Voice recognition will let users navigate Xbox and TV menus without lifting a finger…unless they prefer to use gestures instead. Users will say "Xbox On" to turn on the system, which will not only turn on the Xbox but identify who's talking. We imagine voice and facial recognition will also support security features, such as unlocking user profiles or associated accounts.

The privacy implications: Microsoft, game companies, and advertisers will know exactly who's sitting in front of the TV. They'll know your voice, your face, the games you like to play, the TV shows you watch, the music you have on the Xbox's hard drive, and the ads you see. It could enable a new era of targeted ads that are even more accurate because they'll change with whoever's using the TV. Microsoft has already filed a "living room snooping patent" that detects how many people are watching and makes them buy access to content, like movies, depending on how many eyes there are. Other companies are busily patenting ad targeting based on monitoring the conversations you have around the TV, which listens for who's talking, the tone of the conversation, and the words used.

Although you won't need to be connected to the Internet to do some things on the new Xbox, many games will require connectivity to work. There's also increased emphasis on cloud storage of game data, so say goodbye to traditional memory cards and hello to online storage, most likely integrated with Microsoft's SkyDrive and maybe with other cloud storage services, like Dropbox. Users can store movies, music, game data, and more in the cloud; they can even store gameplay videos and edit them online.

The privacy implications: Once you store something online, it's way easier for law enforcement and **other third parties** to access it. Unfortunately, the law is really far behind on protecting information that's stored in the cloud because of a legal principle called the third-party doctrine. In non-legalese, it means that if you have a document, and you share it with company A (such as Xbox's cloud storage), you lose privacy rights in it and law enforcement can get it without even a warrant.

http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google
http://www.techweekeurope.co.uk/comment/privacy-skype-silent-circle-116889
http://www.abine.com/blog/2013/xbox-one-will-know-your-face-voice-and-heartbeat/
http://arstechnica.com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/