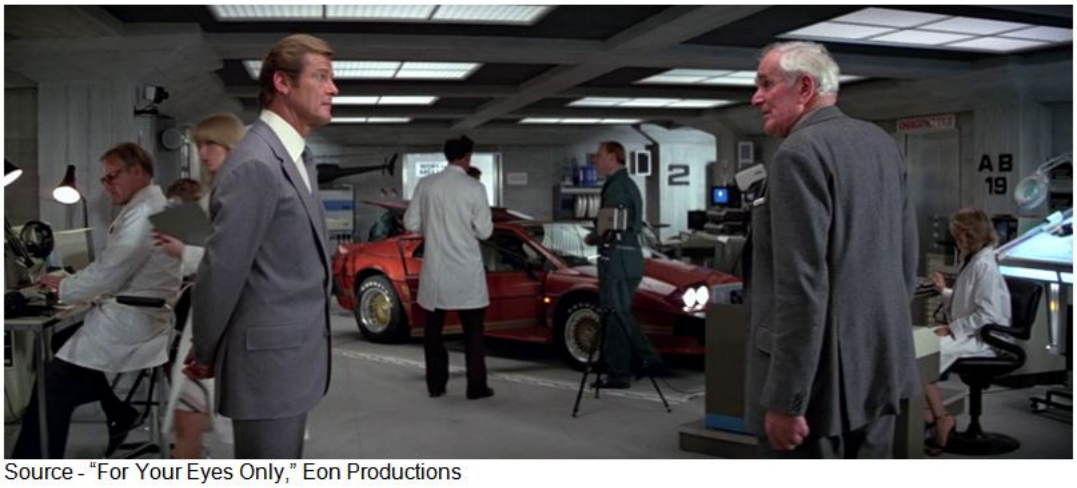
Content Insider #416 - For Your Eyes Only

Privacy and Security are Personal, Very Personal



Source - "For Your Eyes Only," Eon Productions

"*I'm afraid we have to inform the Prime Minister that Operation Undertow is dead in the water. Why... she'll have our guts for garters!"* – **Frderick Gray, "For Your Eyes Only," Eon Productions, 1981**

If you're uncomfortable with the idea that the social media sites you regularly visit or your apps could be sold and your "private" information could be a key part of the deal, you're never going to get any sleep when IoT (Internet of Things) and IoE (Internet of Everything) take hold.

By then, there will be an estimated 50B things talking to thousands of other things; and some of that information is going to be yours … and yours … and yours … and

You can bitch-n-moan about it.

Governmental agencies can enact new laws to protect you. Of course, that's right after they get backdoors into all of your devices.

The Electronic Freedom Foundation (EFF) and idealists can sue for free, open, secure, private communications. But there's not a damn thing you can do about it!

It wasn't designed that way; it will never be that way.

When a few engineers and scientists developed the network of networks back in the '70s and '80s, they had no idea that their "little clique" communication tool was going to be so indispensible to over three billion people every day.

When Motorola's Martin Cooper made his first mobile phone call, he had no idea you'd never let the little sucker be very far from you because you might miss out on something really important.

The Internet and wireless services by their very nature are fast, open, frictionless connections that carry stuff from one person to another, one source to any who want it.

Source – ZDNet

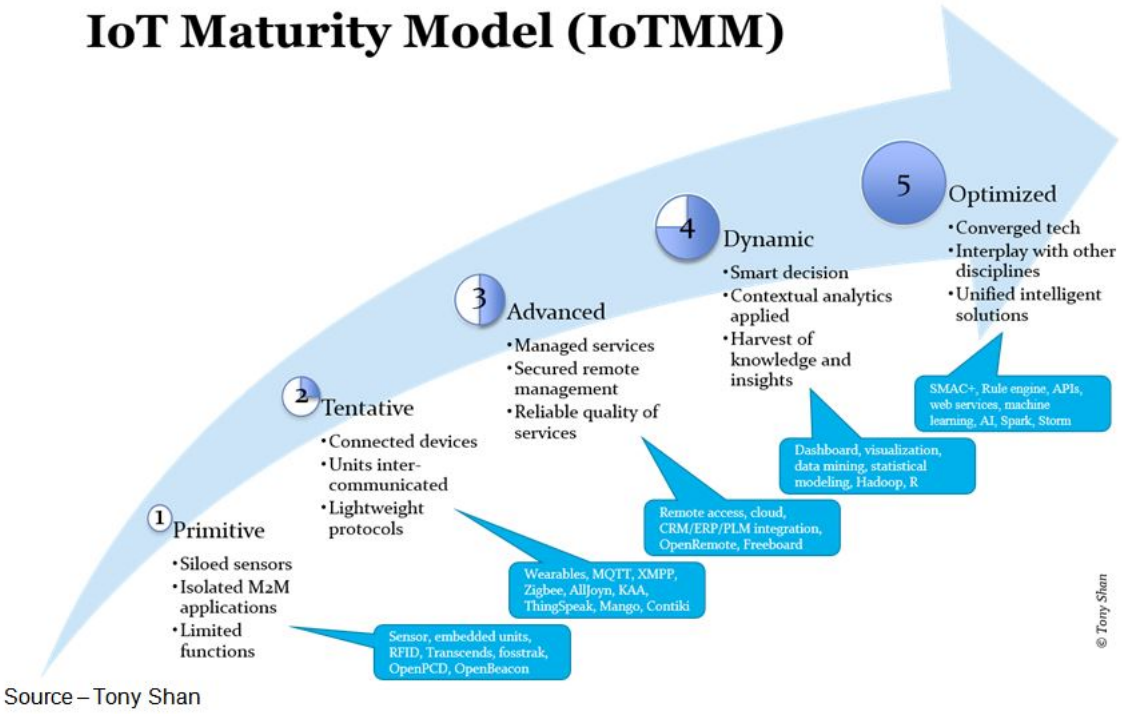
> ***Communicating Environment –*** *Almost everywhere you go, everything you do today involves data communications – something talking to something. Personal/professional devices, wearables and digital eyes/pads track you and your activities. The volume of really great data and information continues to grow and be amassed by someone.*

The developers weren't naïve. They knew there were bad people out there and they knew that ultimately, people/organizations had to make money (hopefully, a profit) from their efforts; but they didn't know how ingenious these folks would be.

They couldn't imagine that every government agency in every country on the planet would be so interested in who's doing what to whom, when, where, why, how.

So it came to you as a big surprise when the ***New York Times*** suddenly uncovered that, despite the fact that most sites/services say they respect your privacy, there's a mouse-type statement in their user agreement that says all of your information – name, birthday, email address, sites visited, stuff watched/read, devices (including cars, appliances, other), locations used, etc – could be an integral part of any sale to someone?

You give and they (sites, apps, data brokers, analytics firms) gather more and more details from your activities and devices so they "can better serve you."



Source – Tony Shan

IoT Sophistication – *The implementation of the Internet of things/everything has only just begun but already industry leaders have big plans for the things they can do with the information from individuals and devices. All we know is that there's a lot to learn from the people/things around us.*

The more you tell them, the better job they do in delivering product messages at just the right time and you're happier with your online experience.

BAM!! everyone is happy.

True, that information can also be used to determine your religion, political leaning, fitness, medical condition, financial status and other preferences; but you just have to hope they mean well.

At the Ford Trends Conference earlier this year Jaap Suermondt, HP Labs analytics lab vice-president and director, noted that Ford, HP, SAP and many other firms are addressing the privacy and security concerns at the beginning of their projects rather than as an afterthought.

Source – Khor Sow Yee

> ***Data Clouds –*** *HP's Suermondt highlighted the fact that even the simplest of information gathering device sends personal information to someone's cloud where there is the potential for use … and abuse. Multiple proprietary clouds and channels will make it difficult if not impossible to protect individuals' information/data.*

Using the lowly fitness tracker as an example, he noted that anyone who wears one sorta', kinda' knows all of that personal data goes into someone's cloud.

"You keep your fingers crossed and you hope that they're being good to your data." he commented. *"You hope that the company that sold you the fitness tracker doesn't get acquired by another company that then gets acquired by another company that then sells your data to your health insurance provider, which is the monetization mechanism."*

He acknowledged that given the speed firms are introducing new IoT products/services and the divergent paths, there should be more concern about data privacy.

Of course his company, Ford, SAP and the firms HP is partnering with, plan to "flip the Cloud" so the data can really be protected by engineering.

In their approach, personal data never goes into the cloud but rather a unique distributed mesh computing solution that will get the auto firms into the connected service business instead of car business.

I guess that might work as long as you're in your car.

Of course, the idea that engineering can control it for you is a lot like the early Internet developers who thought they could exclude all the untrustworthy, nasty folks.

They focused on the overwhelming challenge of just getting files and emails moving quickly and reliably while protecting the network of networks from intruders and enemies.

That was a huge task in itself.

Back in the good old days hackers only took on computers; but once the fun wore off there, they took on bigger, better (more lucrative) challenges like banks, retailers, government agaencies, Hollywood studios, utilities … and ordinary people.

Who could have imagined users would turn on each other?

> ***Close Personal Friends –*** *Once we entered the brave new digital connection world, the rules changed dramatically as to who wants to know what about whom and what you can find out with just a few clicks and there's no turning back.*

Most people think privacy is important in their daily lives, even though they realize that they are under surveillance when they're out and about and that data about them is being collected.

Since breaches now occur with boring regularity, people who take their privacy/security seriously want limits placed on what personal data is collected, how it's used, where it's stored and who has access.

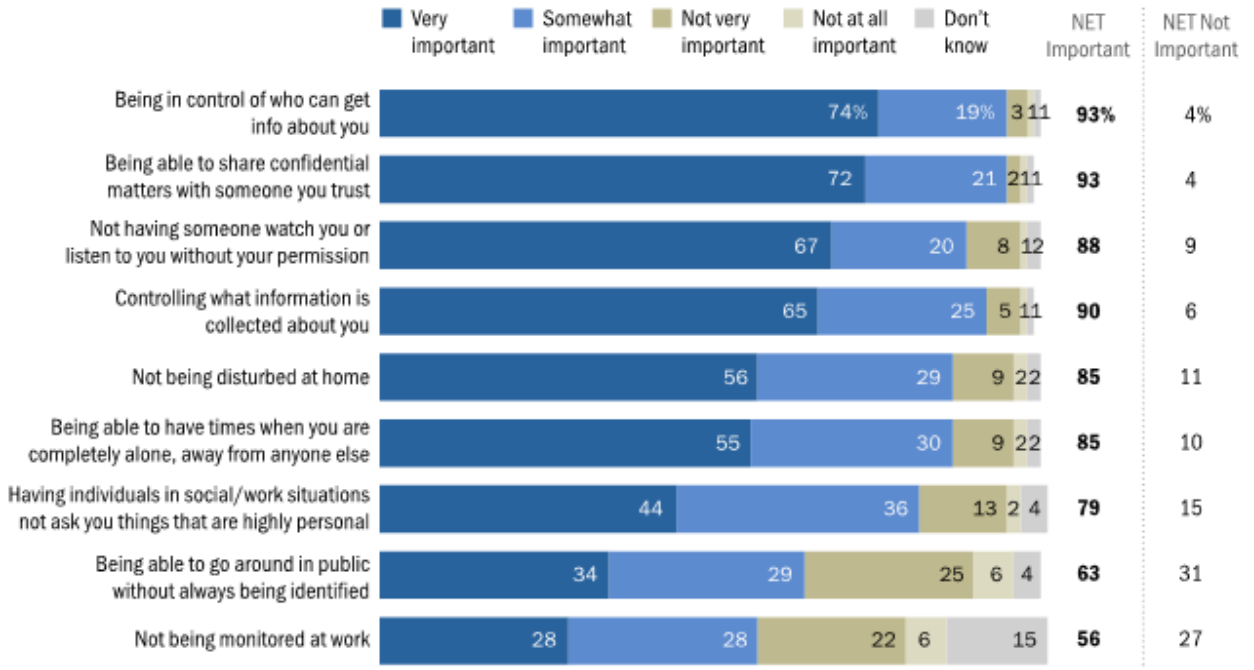
In addition, they find being proactive with the use of encryption and hiding their information, correspondence, discussions, purchases, activities, etc. is in their best interest.

People today have very low levels of confidence in the privacy and security of records maintained by most organizations; so in their own small way, they've taken their own steps to cut the collectors off.

Americans Hold Strong Views About Privacy in Everyday Life

In response to the following question: "Privacy means different things to different people today. In thinking about all of your daily interactions – both online and offline – please tell me how important each of the following are to you . . ."

% of adults who say ...



Source: Pew Research Center's Privacy Panel Survey #4, Jan. 27, 2015-Feb. 16, 2015 (N=461). Refused responses not shown.

PEW RESEARCH CENTER

> ***Managing, Controlling –*** *While people understand their information--and information about them--is needed to deliver the best products, services possible. They also want to be able to manage and control how that information is used.*

Few folks have taken aggressive privacy enhancing measures; but they do feel there should be limits as to how long organizations keep the records. And they think there should be limits on the government surveillance programs.

The world's most prestigious security technologist have all come out against government demands that they have special access to encrypted communications, saying it would put the world's most confidential data and critical infrastructure in danger.

It's a long and well-thought-out position statement, but what it really says is ***"Bull Pucky!"***

Most people feel it's important – often very important – to maintain privacy and confidentiality in their daily lives. That includes who is collecting what about them--especially when they're at home, work, during social gatherings and when they just plain want to be alone.

Pew Research's survey early this year showed:

- 93% of adults say that being in control of *who* can get information about them is important; 74% feel this is "very important," while 19% say it is "somewhat important."

- 90% say that controlling *what* information is collected about them is important—65% think it is "very important" and 25% say it is "somewhat important."
- They feel they should be able to share confidential matters with another trusted person

Most people manage their own settings/activities because sadly few are confident that organizations – government agencies, credit card companies, social media sites – will protect their privacy/security.

People increasingly feel they can control how much information is collected about them and how it is being used, which is why many were taken off guard that a company sale would include their data.

With all of the monitoring going on around the globe, Pew and Nielsen have found there is an upswing in how people protect their information including:

- Clearing cookies or browser history (59% have)
- Refusing to provide information about themselves that wasn't relevant to a transaction (57% have)
- Using a temporary username or email address (25% have)
- Giving inaccurate or misleading information about themselves (24% have)
- Deciding not to use a website because they asked for a real name (23% have)
- 10% of adults say they have encrypted their phone calls, text messages or email
- 9% say they have used a service that allows them to browse the Web anonymously - proxy server, Tor software or VPN (virtual personal network)

Depending on the organization, some people are okay with them retaining the individual's records, but others not-so-much--even when it may be needed to provide certain functionality (search engines, social media sites).

Source - "For Your Eyes Only," Eon Productions

People aren't opposed to giving some folks their information but they agree with James Bond, "*Now, if we could identify that 'someone'...*"

# # #