Introduction

In the last lesson we examined the goofy Windows 10 interface and how to make it more appealing to you.

In this lesson, I'm going to show you how to get Microsoft's prying eyes out of your business.

Okay, there's some things that Microsoft has absolutely no business knowing about you and in this lesson I'm going to show you how to get your privacy back.

Now, when I worked at IBM, I was a technical support engineer and I took calls; people would call in: they were System Administrators, they were Network Engineers – that sort of thing. And you know, I would answer their questions, or try to answer their questions without Googling too much.

And I remember that I always kind of felt that somebody was watching me – right? And maybe it wasn't my boss but just somebody on the inside. Like, one of the Network Administrators or – inside the company – they're just – you know tracking my activity on the corporate local area network.

They're monitoring my network usage.

They're looking at what applications I'm using making I'm following procedure.

And then the funny thing is a couple of years later I actually moved into a position where I was that guy. I was the director of a small media company and I was the guy that, although I wasn't monitoring anyone, I realized the people that I supported, our staff, like the Marketing people, the Sales people, they had this sneaking suspicious – that I was just tracking all their habits. And the truth is I WASN'T!

But the point is that that feeling, that feeling that you're being tracked – that someone is in your business is really disconcerting. And so in this lesson I'm going to show you how to get your privacy back.

There's a couple of tricks that you need to be aware of and it will really help you to be more at peace when you're using Windows 10.

In this lesson

We are going to look at the privacy statement.

I know it's a boring, lengthy, legalese document, but I've read through the entire statement and I've pulled out a few of, what I think, are the most important points – ones that you really need to care about.

So we're going to look at those and then I'm going to help you understand your privacy settings.

This is really the meat and potatoes of this particular lesson. Alright, so let's take a look at this stuff.

Read the Privacy Statement

First, read the privacy statement. And, it's not as lengthy as you think. There are actually several headings and then you can read sort of a synopsis of what that heading is and then if you want more information you can click "Learn More" and it'll give you more details.

And it's really important because I've actually found ways to disable certain privacy features by reading through the privacy statement. There are links that will, if you're already logged into your Microsoft account, will actually take you directly to where you need to go to disable certain unwanted features.

So there's a couple of statements in the privacy statement that I found kind of interesting. So one it says that: "When you use Bing services, we collect

your search queries, location and other information about your interaction with our services"

That's a little disconcerting and also there's a section below that that says:

"We collect data about you, your device and the way you use Windows". What does that even mean? Granted, I did take these excerpts out of context and that's why I'm going to show you the entire Privacy Statement now.

So here is the gloriously long Microsoft Privacy statement. You can get here by going to https://privacy.microsoft.com and I'll include the link in the notes.

It's a long document. There's a lot of material here and admittedly I'm about 99.99% certain that almost no one has actually read this document; has gone through it.

And even like this: Cortana, if you click "Learn More" there's even more information in there like what she does and how she uses your search history and that sort of thing.

So I took the liberty to read through the guide and I pulled out some of the most interesting bits of language here. Now, I encourage you to read through the entire doc for yourself. Yeah, it's not great afternoon reading and it's probably not going to keep you entertained but I think it's really important that you know what you're agreeing to do and what information you're agreeing to give over to Microsoft and also how to turn off some of those things.

So, definitely do that: read through this document.

So here are the ones that really stuck out to me. The first thing that stuck out to me is: it says Microsoft says in "How We Use Personal Data", they say:

Well, let me just start from the middle of the paragraph:

> We also may use the data to communicate with you, for example, informing you about your account, security updates and product information. And we use data to help make the ads we show you more relevant to you. However, we do not use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files to target ads to you.

So they're saying they're not going to target ads based on your personal information like you know, if you have a photo that you took and you named it something like "Photos to Switzerland" – you're not going to get ads for trips and discounts to Switzerland.

Now you can actually click on "Learn More" and find out exactly what that entails but that's the gist of it – that's really the main part of this section right here.

The other privacy part that I think is worth mentioning is the part under "How we use Personal Data".

If you scroll down, there's a section under advertising where Microsoft tells us how we can actually opt-out of receiving interest-based advertising – that's what this is all about – by visiting our opt-out page.

So if you click this opt-out page you can actually opt-out. So you can select okay: I don't want to personalize ads on this browser.

You can say "Personalize ads whenever I use my Microsoft account" I want that t be off.

"Personalized ads in Windows 10" it actually tells you how to turn those ads off by going to Settings > Privacy > and Let apps use my advertising ID for experiences across apps.

So you can actually go here: Click the Start Button > go to Settings and then you would just type in “privacy”.

And in privacy you can turn off the “Let apps use my advertising ID” right here – so that’s where you would turn that off.

So this is actually very useful and I got here from looking at the original privacy statement.

Another interesting point here is the one about web beacons. So if you scroll all the way down – not all the way down but sort of toward the middle where it says cookies and similar technologies…

Microsoft has this paragraph that says:

> We also use web beacons to help deliver cookies and gather usage and performance data about our services. Our services may include web beacons and cookies from third-party service providers.

So a web beacon is really just a little packet of information that contains data. And here Microsoft is overtly telling you that these web beacons will basically gather usage information so they can tell how much you’ve been using a particular service and they can use that for analytic purposes or research or whatever they use it for.

But, this is pretty important. You can actually click “Learn More” as always and then find out more information about this. So definitely don’t neglect to go through this section and check this out because there’s a lot of information here that will help you gain control of your privacy.

I think the that one of the most eye opening sections is the one on Bing. Now, there’s actually too much here to highlight – you should really just read the whole section. But one of the things that you might want to do is immediately opt-out of the Bing rewards program.

So where it says:

> When you are signed in with your Microsoft account, we use data about your interactions with Bing services to provide rewards credits. To opt out of this feature, go here.

So you can actually sign out of that by clicking here and I strongly suggest you do that. Now, you're going to have to sign in to do that but there's no reason that you should be sending data to Microsoft that is targeting you with these rewards credits.

You know, there's this section here that talks about:

> When you conduct a search, or use a feature of a Bing-powered experience that involves conducting a search or entering a command on your behalf, Microsoft will collect the search or command terms you provide, along with your IP address, location, the unique identifiers contained in our cookies,

Now by the way, a cookie is just a text file just to clarify that. It's not, it's just a file, a text document that contains a attribute and a value pair that's sent from the client, that is – your machine, to the server which is Microsoft in this case.

Usually people use it to stay signed into different websites. For example, if you log into Google it sets a cookie in your browser so that if you close the browser and reopen it, you're still logged in because it pulls that data from the file. So cookies aren't necessarily bad but they can contain personal information.

And here Microsoft is saying that we're providing your IP address, your location, your time and date of your search and your browser configuration. And if you're using Cortana you're providing even more information.

So – you know – just keep that in mind. Now some of this isn't as bad as bad as it sounds. Some of this stuff is absolutely necessary in order for anything to work. It doesn't mean Microsoft is using this data illicitly but you should still be aware of the settings and what's going on here. So I encourage you to peruse and read this document thoroughly and devote a few hours on a weekend to really ingest it.

The last part I just wanted to show you is in the Windows section. There is a part here that's kind of interesting where it starts and it says… let's just read this paragraph:

> Windows 10 ("Windows") is a personalized computing environment that enables you to seamlessly roam and access services, preferences and content across your computing devices from phones to tablets to the Surface Hub.

The Surface is their tablet…

> Rather than residing as a static software program on your device, key components of Windows are cloud-based

Meaning, there's just some server that's accessible from the internet: that's all we mean by "cloud-based"

> and both cloud and local elements of Windows are updated regularly, providing you with the latest improvements and features.

Now here's the thing:

> In order to provide this computing experience, we collect data about you, your device, and the way you use Windows.

So there's constantly data that's being collected. Now you can learn more if you click "Learn More". And this is where you learn more about some of the settings that are being collected so, again you know, read through this when you can but we're actually going to go into some of the setting and I'm going

to show you what you really need to care about so this is not so overwhelming to you because I know right now you're probably feeling like:

This sucks. Why would I ever use Windows 10? There's no way that I'm ever going to be able to read through this document and figure out what I need to enable to disable.

So let me show you what really matters and what you can change.

A walk through your privacy settings.

There are a bunch but we're going to look at a couple of them. We're going to look at all the general privacy settings and the ones you need to pay attention to. The privacy settings that are related to your location, your camera, microphone, speech, inking and typing and your general account info.

We're also going to look at the privacy settings that relate to your contacts, calendar, call history, email, messaging and radios. So as you can see there's a lot of sections. I counted about twelve so far and there's a lot of new things that you didn't have in Windows 7, or in Windows 8 or in Windows XP. So let's go ahead and walk through these carefully so you can have a better understanding of what Microsoft is actually tracking from you and how you can stop some of these things.

So let's open up the settings and we're going to go to the privacy section. This is where we're going to spend our time.

So the first thing is this advertising ID.

If you leave this on, it lets Microsoft give you personalized content in the ads. And then it basically displays that in any apps that you download. Remember, the apps are just the programs that live in the Microsoft store and Programs (or applications) are what you're already conversant with in Windows 7, in Windows XP, Windows 8, well not Windows 8, but they're just

the traditional Windows programs – so that's the difference between apps and programs as a review. Apps live in the Store, Programs don't.

So by turning this off we're just saying we don't want any ads targeted in our apps. So there's no reason to keep that on.

The second thing is: there's this SmartScreen Filter. Now, this is actually a good thing. It's good because it protects you from accidentally visiting malicious links that are present in any apps that you might download from the store or that you might have access to in other ways. So to make sure that it's enabled, you should leave this on. And also I would make sure this is enabled in Microsoft Edge to.

Let me show you how to do that real quick – let me show you – I'll show you that here. I was debating whether to show that next lesson but let me show you it here.

So if we go to Settings > View Advanced Settings and there's a section that says… where is it… "Help protect me from malicious sites and downloads with SmartScreen Filter".

You want to make sure this stays on because this really does do a good job of protecting you from viruses. In fact, when I do malware work, malware analysis and reverse engineering, this thing often gets in the way when I'm trying to purposely download viruses to infect my lab machines - so it actually does a good job of blocking some malicious content – so keep that on.

And keep it on here as well.

Now the third option is "Send Microsoft info about how I write to help us improve typing and writing in the future".

I don't really see a reason why this should be enabled so I disable it.

"Let websites provide locally relevant content by accessing my language list". This is good because you want to make sure your content is relevant. Of course they're going to have some of your regional information but I don't find that as intrusive as some of the other settings here.

"Let apps on your other devices launch apps and continue experiences on this device" – that's to give you that seamless experience where if you have a Windows phone and you have a Windows tablet and you have a Windows laptop, you can let the experience transfer across all these devices.

Now if you don't have all of these things, if you only have a Windows laptop, there's no reason to leave this on so I'm going to go ahead and disable it and leave everything else the way it is.

Now, if you click this "Manage my Microsoft advertising and other personalization info" it will bring up a browser… looks like my browser crashed. Nice. Let's try that again.

So it'll bring up a browser and it'll bring you to that window we saw earlier where you can actually go into your ads and save some of the settings here about what's being disabled.

So keep that in mind.

Alright, so let's go ahead and look at the location services and what we can do with location settings. The first thing here is that you can change the location for the device, in other words – you can disable location services for the complete device, or you can specify individual apps that are running on that device and you can disable location services on an app-by-app basis.

So right now it's set for the device but if I click "Change" I can disable it for the complete devices. This means all users, all accounts on the device, it's disabled for everyone.

I actually like to leave it on for the device but then I'll go back through here and I'll manually select which apps I want to disable location services on.

One other thing I want to show you here is that whenever an app is using your location you'll see this little icon here actually in the taskbar by the system time.

And this icon will give you an indication that your location is actively being used. So there is a visual notification when apps are using your location. So I like to keep that on so you can see that there.

Also, you can… if we scroll down to location history, one thing I like to do, is periodically go in here and clear out your location history – if you're using location services.

This is a good way to clear the cache and restart so that that data isn't sitting on your computer.

The last thing I wanted to share with you is this new thing called Geofencing. And this is actually really interesting. This technology has been around for a while but it's now making its way into Windows 10.

And what this does is it basically uses your GPS, or your Wi-Fi or Bluetooth settings, to create a virtual fence, a virtual boundary around a specific location.

And the reason this is good is, I actually don't recommend disabling this unless you have a specific reason to do so, but the reason why it's good is because you can actually have certain apps that will remind you to do certain things based on where you are and what you're doing.

So let's say, for example, you're at work. You can set a location-based reminder so that when you leave work, an alert pops up on your smartphone, your windows phone or your laptop if you had it open, telling

you to remember to buy your wife roses or remember to stop by the laundry mat or whatever it is. So that's kind of nice.

And in some cases you can actually set up a Geofence around your laptop so that, let's say that you've got your smartphone in your pocket, you can have it so that when you leave your laptop, it'll automatically lock your laptop because the Bluetooth signal will degrade. And when the signal reaches a certain threshold, Windows will lock itself.

Now this is actually in the Windows 10 anniversary update. There's going to be new functionality where proximity controls on companion devices, so if you have an Android or Windows phone, it can lock based on your proximity ot the device. I don't know if it's going to be available for iPhone or when that's going to happen but I just wanted to let you know about that.

So let's look at some of these other settings here. There's the camera and microphone – now these two go together hand in hand.

Let's look at Camera first: there's a lot I have to share here. So it's kind of funny – before we dive into this I just want to share a story with you.

I used to have a friend, or a college as well, who… hehehe he had a Macbook Pro so it wasn't a Windows laptop but he would keep a piece of tape covering his webcam. And one day I asked him and I said what's that for and he told me and he said it's for privacy. And you know – this is really important – this is a really important section here.

What we're looking at are all the apps that have access to your camera. We can scroll down and we can see this. Now – just because an app has access to your camera doesn't mean that your camera is always in use. The way that it works is that when the camera is on, if your laptop has a light indicator, that light should be on. Otherwise, if you don't have this light indicator built into your laptop, most laptops do, you'll see a notification pop-up in Windows.

So here we can search which apps have access to that – our camera – or we can just turn the camera off completely.

Now, if you're really paranoid, and let's say that this isn't sufficient; let's say you turn it off but you're still paranoid because this is a software control right? So it's possible that there could be some loophole that some hacker could find a workaround to enable it without turning on the light.

If you're really paranoid, you can actually disable this in the BIOS. So you would reboot your box or press F2 or Del or something like that, and you would look for like a webcam setting or an integrated setting and do it that way. Or you can just put electrical tape over the camera but there's also some more solutions that you could actually look at on Amazon for.

Let me show you this for a second.

So there's the web address. This is actually an affiliate link so if you buy this product through that link – let me show it to you again – if you buy the product through this link:

http://amzn.to/2a28S1o

I will get a commission so I just wanted to be up-front with you on that. But this is a webcam privacy shield by STEAGLE. It's got pretty good reviews and you can actually just slide this over your laptop and it will block the screen – block the camera and the microphone. So this is a really nice technique – really nice tool for doing that.

And you could of course read the reviews and see what people have to say about it but sometimes people use things like this and it works.

The other option is to use a webcam cover that's a little less sophisticated than the STEAGLE I just showed you but it actually has a reusable adhesive so – backing – so you can stick it on to your camera and then you can wash it off

and you can reuse it again – multiple times – hundreds of thousands of times. Let me show you that one.

http://amzn.to/2a8MglJ

And there's my link up there. You can see that this is called the WebCam Cover Solid Black. And this thing is just a little sticker thing that you put over the camera. And the nice thing is that it's reusable – you can keep on using it over and over again. And it's really simple – it just works. And it's really cheap too it's only five bucks. And you can see what people say about that.

So if you're really really paranoid and you want to make sure your camera and microphone is protected, you can use something like this to help you with that.

And of course, the Microphone settings go hand and hand with the camera. You can disable it for specific apps or you can disable the whole thing. And one thing I really want to say about this before I move on is that privacy is a really big deal.

And in fact, the chair of the National Data Protection Commission in France, issued a formal notice to Microsoft, demanding that it stop collecting excessive data about users without their consent – it actually gave Microsoft three months to comply.

You can read about the article here… let me see if I have the link – I think I do. On the commissions website, the CNIL website, and you can find the URL here I'll also include it in the links:

https://www.cnil.fr/en/windows-10-cnil-publicly-serves-formal-notice-microsoft-corporation-comply-french-data-protection

This is a big deal. You're not the only one that sees that Windows 10 has a privacy issue. There's lots of people that have recognized this problem and

we're hoping that Microsoft is actually going ot heed these notices and change but there's no guarantee about that.

Anyway, so if we go back to this section. Let's look at the "Speech, inking, & typing"

Oh, did I skip over Notifications? I did.

So in Notifications you can go in here and say which apps have access to your notifications. I actually don't have any apps that have access to it but if I did you would see them here.

And go to "Speech, inking, & typing" and this in opinion, is probably the most excessive privacy setting. Especially the part that says this:

> Windows and Cortana can get to know your voice and writing to make better suggestions for you. We'll collect info like speech and handwriting patterns, and typing history.

Think about that. The things that you type – a history of that. It's almost… I mean – I don't want to call it a keylogger but your keystrokes are in a sense being logged and uploaded to Microsoft's webservers for analysis or analytics or whatever they're using it for.

Now you have to use this if you want to use Cortana but if you're not using Cortana, you should definitely disable this section because it's a little concerning to say the least.

And you can go to "Account info" and you can also specify which apps have access to your account data. I don't actually have any that have access to this but if I did they would show up in this section.

And then the last couple of sections:

Contacts, Calendar, Call History, Email, Messaging and Radios… these are all sort of grouped into the same category.

So Contacts: these are apps that have access to your contacts; contact information. Your Calendar: you know apps that have access to your Calendar data.

Call History: this is more relevant for a smartphone, but if you're using Skype or a messaging app of that sort, you might also have a log of phone calls that you've made so and you want to make sure you're controlling access to that.

And of course, your Email. Some apps can actually send email on your behalf – so you want to be aware of what those apps are here. Along with messaging apps – you can see Skype is here.

And then your Radio apps that have access to your Bluetooth signals and that sort of thing.

One thing I do for these settings, all these settings, I just… if I'm not using it I turn it off but I actually like to keep it on and then manually go through each of these and specify which apps have control over all these settings.

So take the time to look at these settings and go through them to make sure that you're not unwittingly revealing excessive information.

Now one last thing I want to show you before I wrap up this lesson, I know this lesson is kind of long so I don't want to overwhelm you with all this data, all this information, but I just want you to be aware of free spyware protection programs.

So there's some software out there that says it will protect you from Windows 10's privacy issues. But, sometimes those programs themselves actually contain spyware – ironically. And so one of them that you might have heard of is called "DoNotSpy10".

So if we open up our browser and you can go to DoNotSpy10's website

http://pxc-coding.com/de/portfolio/donotspy10/

And I think he's a German coder who created this application – and it works – it's one tool that sort of consolidates all of the Windows 10 spying, all the privacy attributes into one application, but there is an OpenCandy – I guess you wouldn't call it spyware – but it's a potentially unwanted program – a PUP as we call it in the Malware Analyst lingo.

So you want to make sure that you know… I guess what I'm trying to say is that there's some software that's meant to help you and sometimes it includes software that's undesirable. So just pay attention to that – just be wary of these tools and know what you're installing before you install it.

The Bottom Line

Microsoft is nosy but fortunately you now have the tools and the skills, the knowledge I guess you could say, to sort of get Microsoft out of your business – or at least to the best of our ability, to gain some control over our privacy.

Coming Up

In the next lesson, coming up, what do we have in store? We're going to look at how to secure privacy in Microsoft Edge, specifically Edge the new browser.

And then we're going to show you how to protect your privacy using Microsoft accounts. Alright so let's go ahead and jump right into that because in my opinion those are two of the most important things we need to look at.

