Are we the new Digital Soylent Green?

Preprint · May 2020

DOI: 10.13140/RG.2.2.23312.02562

1 author:

David Dickson
DKS DATA Alberta, Canada
9 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Are we the new Digital Soylent Green?

Social Media & IoT - Turning People Into "Green" - What is our privacy worth?

Note: This is an update to a number of articles I have written over the past few years. - THIS IS CURRENTLY BEING UPDATED FOR THE POST COVID 19 WORLD.

Contents

For more on COVID 19 - See A SARS-COV-2 Story.

Look at this set of articles from the point of view of widespread tracking, DNA testing and more. Now you might understand the impact to Privacy from the reaction to COVID19. And what can they do with even more data. If you think they controlled the Vertical and the Horizontal before...welcome to the Twilight Zone of COVID 19.

1. ***The Best Laid Plans. COVID-19***
2. ***COVID 19 – Is the lock down working?***
3. ***COVID 19 - The Spread of A Virus***
4. ***How the humble Gin & Tonic may save the world from COVID 19.***
5. ***COVID 19 Risks - a Personal Message***
6. ***COVID 19 - A Personal Message Postscript***

High level paper here:
https://www.researchgate.net/publication/341271402_The_Best_Laid_Plans_COVID-19_A_SARS-COV-2_Story_A_SARS-CoV-2_Story_P_a_g_e_2_88

Remember to eat your greens. Privacy and our Digital World.

Now back to your regularly scheduled 'programming' update. Get your daily 'bug' 'fix' and back to sleep. Welcome to Stepford, 1984 style. How a to program a population to accept the 'new normal'. Remember to eat your Soylent Greens.

We all worry about protecting our privacy but surprisingly we give it up daily without a second thought. We are providing access to every aspect of our personal and business lives to private companies at a level of intrusion that the Security Services would be hard pressed to achieve. We allow this data collection from smart speakers, smart thermostats, doorbells, cameras, our phones and so much more. You don't even have to sign up or directly interact anymore. Just being in the vicinity or having your image or voice uploaded can contribute to your digital presence forming in the 'cloud'.

Now with the age of COVID 19, in less than three weeks, we went from Privacy champions with The GDPR, DPA 2018, ePR, PIPEDA, PIPA, FOIP and more, to handing over our digital souls without a squeak. Why would that be? FEAR... the greatest motivator ever imagined.

Where does it start?

Surfing the web, shopping online or even opening an email? Marketing tools that track just by looking at a website from Google Analytics to Google Fonts. Facebook Pixels to Transparent Gif's in your email. Even that innocuous branded SAFE and secure company logo at the at the bottom of an email could be tracking you without your knowledge. Imagine Fed Ex breaking into your house to leave a letter instead of asking for a signature!

So, what if these simple tasks felt more like having your house broken into?

Digital Burglary?

Enters any building (device) or part of a building (browser/email/app) as a trespasser (nonconsensual tracker) and with intent to commit (to track) any such offence (against Privacy Directive etc.)… You wouldn't accept 'Legitimate Interest' for Burglary? So, why accept it in stealth tracking email, websites or apps?

We have all heard of Cookies. They might taste nice but they shouldn't be hiding on your computer or mobile device without your permission. And yet, these stealth tracking

mechanisms are everywhere, even in the very systems that claim to protect your privacy or hail to be 'GDPR Compliant'.

These hidden tracking devices are just the start of your digital profile. From here we enter the consensual process of giving away our very digital souls.

Why do we do this?

You stand at the checkout wondering if anyone can see that 4-digit PIN you tap in, protecting it like it is your first born. Yet, we discuss our most private details within earshot of our phones and smart speakers and post so much online without a second thought. If the checkout clerk ‘liked’ your PIN number, would you let that clerk or anyone else see it? Ironically, that PIN number has very little risk associated with it in comparison with Tap to Pay, the 'new normal' for the cashless society.

Add to this the dependency on social media for our minute by minute dopamine hit, the internet is grabbing and analyzing data about us on a scale that could not have been imagined even a few years ago. And now it has teamed up with governments worldwide in the largest personal data grab the world is ever likely to see. All our movements, interactions and health information collected to 'save lives' under the fear induced government sanctioned mandates.

You sit down to watch the latest series on Netflix. You open your browser. You log onto Facebook. You check your email. You spit into that 23 & Me or Ancestry DNA test tube. Have you noticed how all of these companies know what you like, what you have been looking for and how targeted emails, suggestions and advertisements keep popping up? This isn’t magic or coincidence. It is big data analytics, Machine Learning and AI all building a profile of your every digital breath, literally.

In the age of COVID 19, no longer are these practices to obtain DNA and the expanding digital footprint consensual, they are demanded and enacted by laws driven by fear. That fear allows the laws to be used with the appearance of consent.

But is consent obtained through fear, really consent?

23 & Me has become a COVID 19 test to qualify you for a COVID 19 passport, all to 'allow' you to go outside. Tracking cookies and pixels have become tracking/tracing apps with proximity alerts. We want these things so we can go outside, but what if you refused... would you be allowed? And who is helping to collect and analyze this information? Why the GAFA is of course (Google, Apple, Facebook, Amazon...etc.)

Tap and pay will soon become cryptocurrency so we can remove the untraceable 'dirty infected' money. Our every move, our every COVID 19 infected breath, tracked, quantified and fed into the ever growing digital footprint. Feeding the beast that is AI with the ever growing digital gluttony inducing big data.

We all have a digital footprint that is shared online. This can be used to cross reference all the information available to build bigger and better profiles. All in the name of marketing, 'saving lives' (and more). In some cases, it is even the absence of information that can help build a better profile. In my years analyzing redaction (the art of removing identifying information from documents etc.) or ‘black lining’ as it is sometimes called, I have seen how missing information is easily extrapolated. Remember a Dave sized hole, might a well have a "Dave was here" sign on it.

Without data, AI and Machine Learning would starve. So, they need more data to feed the beast. Luckily for them, we are happy to oblige and provide a veritable feast of personal information with abandon. In most cases we don’t even know we are doing it. Social media and all the electronic devices we invite into our

lives, are purposely designed to provide the feedback we all crave. We are what we do and say (or not) and we share that information without a thought.

This is why, in part, that the GDPR and other privacy legislation had expanded the view of protected data to include "Personal Information", not just a select set of data points in the old PII. But in the days of COVID 19, health trumps privacy … every time… but should it?

Now in the COVID 19 are we ready for the digital 'new normal' where data privacy has evaporated into the air like a cloud of COVID 19 microdroplets. Constant snapshots of our lives gobbled up faster than we can upload images to Facebook, Instagram or the next best platform.

Speaking of photographs. How many people really understand the mammoth amount of information even just a digital photograph contains? From the location, time taken, who you are with, type of camera/phone used and more. Upload that photo and it gets tagged to your own digital profile after which it is liked (or disliked etc.) connecting it to many more profiles.

With our current confinement and 'social distancing', we rely more than ever on the digital tools we were once so concerned about. Suddenly Facebook, Zoom and Google are our saviors. No longer are they untrusted platforms the security professionals warned about oh so long ago (well a few weeks back anyway). Now they are here to help... collecting all our ever-growing information as we are unable to communicate any other way. No private social gatherings, no standing and talking in line, everything is now digital and managed by the tech giants we felt so much distrust of only a few short weeks ago.

They don't just control our output though; they now also control our input. From Facebook to YouTube, any attempt to discuss anything outside of the single (but ever changing) COVID 19 narrative has now been declared *'Harmful Content'* and as such will (and has) been automatically removed from the platform... WHAT! Even world leaders discussing what is now becoming mainstream opinion through the medical and research community, is removed...[1] (Bloomberg, 2020)

So, all we are left with is our filtered view profiled individually and with targeted message like a laser guided missile, no longer just to sell the latest brand of toilet roll, but now with ever more

[1] https://www.bloomberg.com/news/articles/2020-03-31/facebook-twitter-pull-misleading-posts-from-brazil-s-bolsonaro

insidious messaging. While all the time we continue those innocuous posts to Facebook, Twitter, Instagram and more. We provide detailed insight into every aspect of our lives with abandon. Political views, personal preferences, people and places we are connected to, all in a single photograph. Until recently, the text we typed was the primary target for profiling and this provided a wealth of data to add to our digital profile. Now we can analyze images and other 'structured data' (documents, pictures, video, audio etc.), read the metadata and more. This can be cross referenced to not only our own but every other digital profile in near real time. Imagine the wealth of data hidden in the random Snapchat image that really has no value to you, other than to allow you to text a message!

Consider the following example. Someone emails (or posts) a picture of you in front in a doorway holding a birthday cake saying "Happy 30th, Dave!" Maybe it is a photo taken on a smart phone weeks earlier. How much personal information does this innocuous image disclose?

- Name, age, date of birth (from the timestamp of the picture and the image of the cake), sex, eye colour (just zoom in), hair colour, approximate weight and height (just compare to the standard dimensions of that door frame), location (GPS data embedded in the picture)... the list goes on.

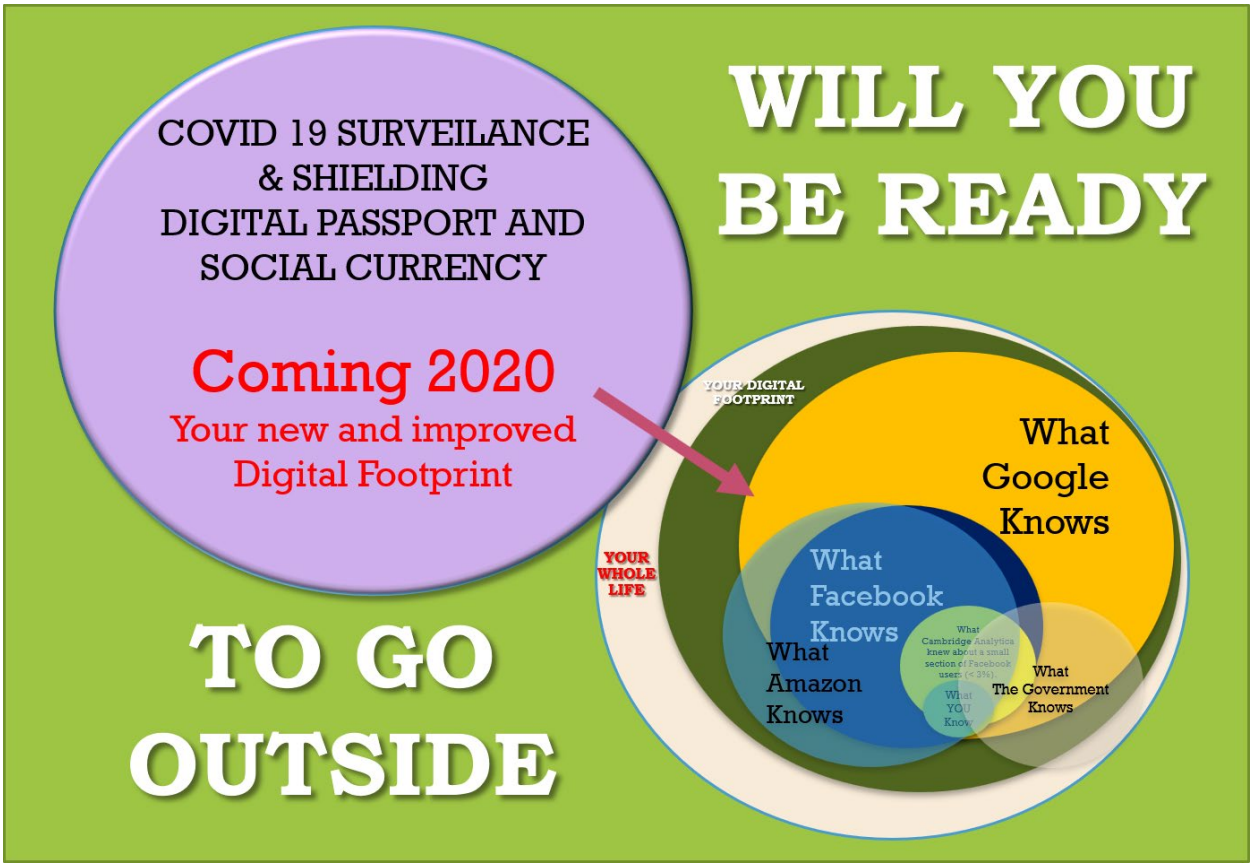
With enough data (easily obtained in our 'selfie-obsessed' age) and technologies such as point clouds i.e. Photosynth, we can even work out the exact spot the photographer was standing in and who else was in the room. If the room contains more people with their own data capture devices or IoT (camera's Alexa, Google Home and more), then the connections grow exponentially.

If anyone has watched 'The Circle', you may be shocked to know that even without those little cameras, your digital profile is working against you. Now add in the Internet of Things (IoT), voice and video enabled devices, tracking/tracing apps and we open ourselves to even more data collection. Ask Google for the local pizza store and suddenly you are bombarded with pizza coupons. Sometimes you don't even have to interact to be targeted. Walk to close to a suspected 'infected' or otherwise 'unfavorable' person and you could suddenly be locked up for another two weeks (or more). In some

countries, the cell towers are weaponized for marketing. Just being in a location can trigger geolocation texts or COVID 19 alert in the near future. All of this information goes back to be stored and analyzed at a later date. As AI gets smarter, the information that can be gleaned grows exponentially. Sadly, even when the AI gets 'smarter' with its ever-expanding data set, it also has a tendency to develop increasing and unexpected bias. In personal interactions such as Google Maps, you can Trust but Verify[2] (Dickson, 2017). However, how can you verify an outcome if you can't even understand how it came to the decision? This is why GDPR banned automated processing that has a legal impact. But where is that protection now? What about the COVID 19 data? Everything from that COVID 19 government loan or other payment from the government, now processed automatically without a single human interaction. Just press 1 to receive a payment into your bank from your local tax agency and not a person around to say hi, how are you. All automated, all seeing, all knowing all data collecting. Do you even know it is happening though? This automated large scale data collection can lead to many unintended (or intended) consequences from a wrong turn, to professional discrimination to things we can only imagine in our worst nightmares.

Welcome to the post COVID 19 world of privacy...

[2] https://www.linkedin.com/pulse/ai-trust-verify-dave-dickson/



Can't we anonymize the data or maybe even use tokens? GDPR thought of that too (and so have Google, Facebook et al.).

“…Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person…”

"...However, a second team within the organisation ... For this, the identification of the individual is unnecessary. Therefore, the firm ensures that the second team can only access the data in a form that makes it not possible to identify the individual couriers. It pseudonymises this data by replacing identifiers ... with a non-identifying equivalent such as a reference number... The members of this second team can only access this pseudonymised information. Whilst the second team cannot identify any individual, the organisation itself can, as the controller, link that material back to the identified individuals...".

Pseudonymisation, anonymization or tokenization. Call it what you want. If information can be traced back to an individual, then it is personal data. Wondering how much can be gained from apparently disconnected or innocuous information? Maybe try The Einstein Puzzle Rebooted [link].

At present, it isn't perfect because multiple people can use multiple devices. I, for one, would rather not have Netflix assume I am an avid Paw Patrol watcher. However, when my grand-daughter comes to stay, Paw Patrol rules! These nuances on whose data belongs to whom will soon be extrapolated as more data is analyzed and AI learns. In the meantime, we are exposed to potentially unfair bias, misleading (and annoying) advertisements and suggested posts/shows. What if that misinformation gets tagged to your credit score though (spoiler alert… it already has to some extent)? Now what happens when there is yet another security breach?

We trust that all that data is secure. We assume it is unusable beyond its original purpose for disclosure. However, large companies and governments are looking at ever more creative ways to use that data to build a better profile. These profiles are more valuable than the best Cryptocurrency in circulation. The more detail they contain, the more valuable they are. It is frightening enough just thinking what a marketing team might use these profiles for (toilet paper anyone)… what about your insurance company?

Now what about all those data breaches that keep happening?

What if your whole life is stolen and becomes available? You can change your credit card number, you might even be able to get new ID or even a new gender but can you really change the fundamental way you are and how you behave?

Imagine you are using Facebook and Google for the first time. You provide both with an email address and password. At this point they know nothing about you…or do they? They will know where you logged in from, what type of devices you use and have access to the history of the devices including websites, apps and more. This is before you even send an email or make your first post. Fill in the complete profiles they ask for and they already have enough information to fill out more than just a basic credit card application.

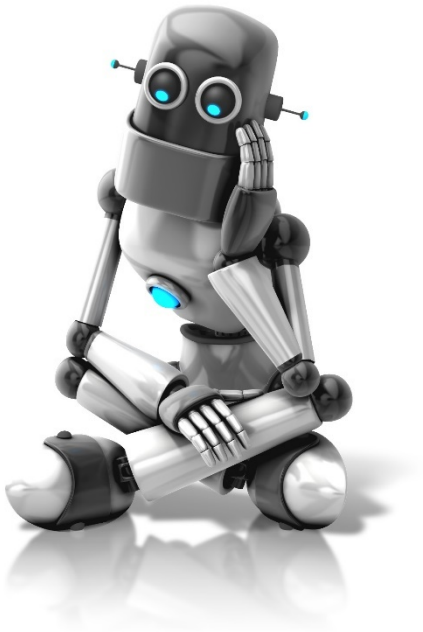
What if you use a different email and password for each? Do you also use different devices? The answer is probably no. So, the digital profiles get connected and now even more information about you is connected. At this point you still haven't done anything.

However, once that first email comes back, you get a warm fuzzy feeling… "somebody cares about me". Post your first photo or status and wait for the likes. The feedback starts to become addictive, as it was designed. How do I get more likes? Make more posts, provide more information, make controversial statements. Each of these adds to the detailed picture of you. Then you like someone else's post and suddenly you are seeing posts that are similar in your daily feed. You see one that says, "So and So likes Diply". Did you like that post because they liked it? Did you notice that it didn't say "So and So likes this specific post"? Probably not. However, the system now knows a little bit more. Sometimes you ignore the feed it gives you. That provides a wealth of information about you also. As these systems talk to each other and exchange information they get to know you piece by piece. But they provide anonymous data, I hear the professionals say.

I will again point to the exercise in redaction. If enough information is shared, you don't need an obvious Personally Identifiable Information (PII) connection to have exposed your "Personal Information".

So, how did we get here?

From the First Industrial Revolution to the The First Digital Evolution [Link].

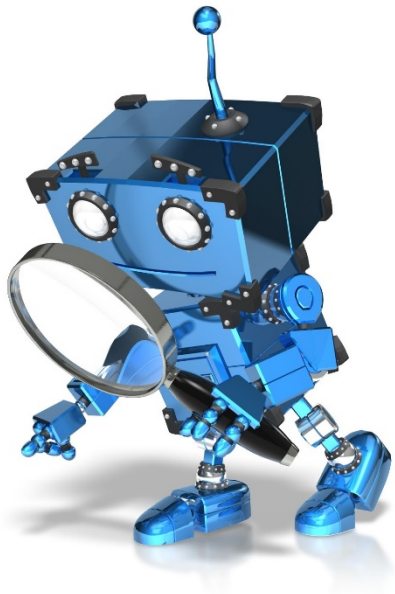


In the 18th and early 19th century, we automated and collaborated with machines to change the way society worked. This was assisted by the introduction of the steam engine. The 19th and early 20th century, saw the expansion of automation and the harnessing of electricity, steel and other technologies expanding the power of industry to meet the needs of the people i.e. customers and workers. These focused on industry. The new machines and tools were not available for home use or home-based businesses. Starting mid-late 20th century until the early 21st century, computers and digital technology expanded at a rapid rate. Although some of these tools were put in the hands of the public, the primary focus for new technology was industry. Access to some of the resulting technology helped spark the next revolution as the public started to gain access to tools and knowledge that had, to this point, been restricted. This was indeed an Digital Revolution, not restricted anymore to just industrial forces. Technology, biotechnology, computing power, software and manufacturing is now being targeted at industry and people simultaneously. This is no longer an Industrial Revolution as its focus is not just on industry. It is no longer just a revolution as we move into AI, Biotechnology and more. We are hurtling towards the First Digital Evolution [Link].

During the Third Industrial Revolution, the most powerful men in the world met to prevent an escalation of power and divide that brought us closer than ever to annihilation.In a world that was facing a rapid evolution of digital technology, people made the ultimate decisions. That meeting of East and West gave us the famous words 'Trust but Verify' [Link].

This is something we should remember as we put our everyday lives in the hands of the unknown box we call AI. Be it Alexa or Google, from Search to Maps, thermostats to door bells, these devices are connected and collecting our digital profiles to turn us into their ever growing pile of cryptocurrency 'green'.

Digital profiling is like the world's biggest game of Clue (or Cluedo for the Brits out there). No-one knows who is in the envelope but if you ask enough questions you can narrow it down really quickly. Now imagine the wealth of information attached to some of the most sophisticated analytical systems imaginable and it is easy to see how vulnerable we can be.



AI and Machine Learning is now taking that one step further in order to 'guess' what you will do next, even before you do it. A company recently created a profiling system to 'guess' if a realtor's contact is likely to sell their house soon. All the realtor has to do is upload his contact list. Did his contacts (maybe not all clients) give him permission for that? Now suddenly they are receiving posts on house renovations, moving companies and more. They have no idea where these came from though.

So, before you make that next post, upload that next picture, speak around Google, Alexa or Siri, or even send that next email, consider what you are giving up. Read those privacy policies a little more carefully. Even if the company that collects the data does no harm, when a security breach occurs, ***the new possessor of your information probably didn't read the privacy policy either.*** They may also have breached multiple systems so are able to build digital profiles more sophisticated than even Google or Facebook could dream of.

We are in a time where this is no longer just about the collection of data. This information can now be used to manipulate our everyday lives. Using techniques such as the micro push, it is possible to nudge our purchasing decisions and even manipulate our political choices.

Wondering how easy it is to manipulate our decisions and even our memory? Just take a look at Derran Brown and Simon Pegg [Link]. Now think about that gift you just gave or received this holiday season. Is it what you wanted, or what was 'pushed' through the power of Social Media and IoT driven data?

What does ***'Stay Safe, Stay Home'*** really mean... in the age of the Behavioral Priming [Link].

Is Google, Alexa the MSM or government giving you what YOU want, or what 'THEY' want you to want?

Take this a step further and watch Derran Brown's further works including "The Push" (not for the faint of heart).

1. Derren Brown Advertising Agency Task - Perception Without Awareness Stage 1
2. How to control a Nation - Perception Without Awareness Stage 2 [Link]
3. Heist - What would you do - how far would you go? [Link]
4. Sacrifice - Would you sacrifice yourself for your worst unimaginable enemy? [Link]
5. The Push - Could You Kill Someone? [Link].
6. Apocalypse - COVID 19 - Is it all real or is this the next Derran Brown special we are living through? Part 1[Link] , Part 2 [Link].

Even if these companies and government cry out "We are Compliant", "this is for your safety" you have to ask, would you have consented in the true sense of the word to what they are doing? We have to hope that these companies and government will work with the three wise monkeys of Cybersecurity, Compliance and Consent. But don't hold your breath or you may end up breathing your last on a ventilator, becoming the latest statistic for the glowing red maps.

Sadly, everything would suggest they might not be working in our best interest after all. Even professionals we trust might not get it right all the time (or even at all). Is that secure email solution doing what you think or is it creating more issues? Is Blockchain or Cryptocurrency really providing the solution you expected or is there a simpler solution? Does that 'new' COVID 19 model make any sense? Just because it is new, shiny or red and scary, doesn't make it the best solution. In some cases, our reliance on technology is making us less smart.

In all of this, not only do we have a lack of privacy but our security is not always top of mind either. In a lot of cases, this is due to a focus on one or the other (or neither). We have to remember that with Cyber security and Privacy - it's a partnership, not a competition.

The genie is out of the bottle and is not likely to be put back anytime soon. It is critical that we have enforceable privacy, compliance and security in place to protect the ever-growing knowledge pool about every digital breath you take...

Now that the world of Digital Soylent Green has come to pass as a result of COVID 19. Take all of the above and the steps the government, with the help of Silicon Valley, is doing and ask yourself... How did we get here, before a Digital Soylent Green isn't just digital anymore.

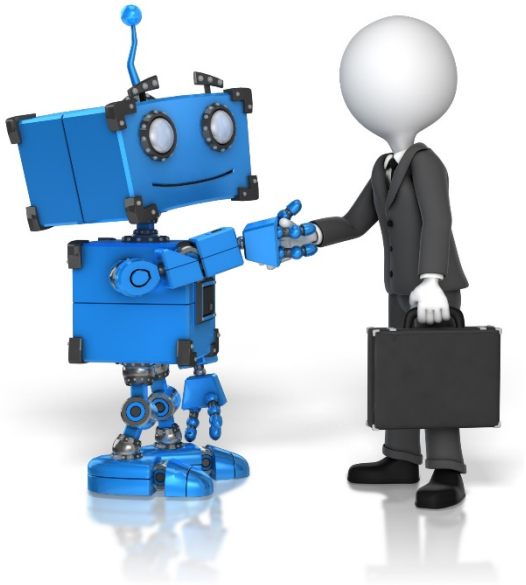
As the media fiddles, we are watching Rome burn. Only China appears ready to rise from the ashes. So, don't be a Nero. Join the conversation beyond the four corners of your TV and help us climb out of this hole before it is too late. **#COVID19**, **#RomeIsBurning**, **#ABetterPlan**, **#jointheconversation**

1. ***The Best Laid Plans. COVID-19***
2. ***COVID 19 – Is the lock down working?***
3. ***COVID 19 - The Spread of A Virus***
4. ***How the humble Gin & Tonic may save the world from COVID 19.***
5. ***COVID 19 Risks - a Personal Message***
6. ***COVID 19 - A Personal Message Postscript***

David Dickson is a Consulting C.E.O./C.I.O and owner at DKS DATA

Appendix A – Trust But Verify

Published on January 11, 2017

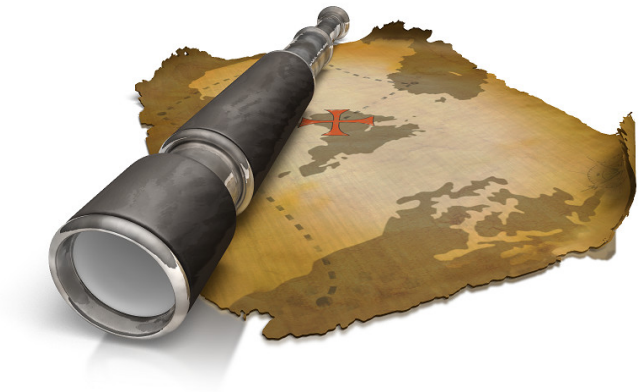


Three years ago, before the age of COVID 19, little did I understand the relevance of these three words. For more on the COVID 19 story see;

(1) ***The Best Laid Plans. COVID-19*** , (2) ***COVID 19 – Is the lock down working?***, (3) ***COVID 19 - The Spread of A Virus*** (4) ***How the humble Gin & Tonic may save the world from COVID 19.***, (5) ***COVID 19 Risks - a Personal Message***, (6) ***COVID 19 - A Personal Message Postscript***

Back to the world of numbers and our propensity to trust but unwillingness to verify in the information age.

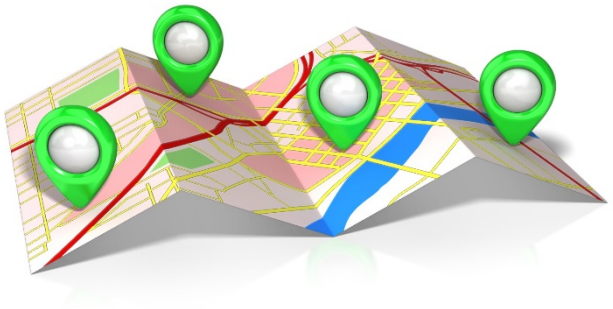
A new year and a whole new world upon us. With all the talk about Russia and Artificial Intelligence (not necessarily in the same sentence) I thought the title would be appropriate. As Ronald Reagan said, "Doveryai no proveryai". I don't think he was thinking about the world today, but it is becoming very relevant as we hand over our lives to that funny little back box called technology.



AI is not 'coming soon', it has been with us for quite some time in one form or another. I grew up in an age of paper maps, grid and lined paper, protractors, pens and those little Rolodex™ popup pads for phone numbers and addresses.

I remembered phone numbers without the aid of a phone and a picture, I could remember how to get from A to B without the aide of Google, I could add up without a calculator and spell (badly) without a word processor. How many phone numbers do you remember? No, these were not the dark ages, they just feel like that when we look back.

Now I say 'call Mum' and the phone dials, I say 'Fast Food Restaurant' and I am directed to food, I open an app to do the most basic of math calculations. At every point I still ask, 'Does that look right?' Most of the time, the technology gets it right, but not always, so *'trust but verify'*. How many of you ask that same question when google says, 'turn left here'? Don't let your answer be 'why are my feet wet?' or worse!



'Measure twice and cut once' goes the age old saying. The worrying part is the trust we put in the technology today without any verification. If a stranger passed on an unlikely story, you would probably go to the internet to check it. By doing so, you just completed the 'trust but verify' process. However, did you 'verify' what the internet said? Probably not!

From the age of 9, I have been coding (self-taught) and pushing the envelope in technology wherever I can. Other than the general interest (or obsession as my wife would say), my main focus on coding or creating algorithms was always to make life simpler. You could say I code because I am lazy; I just don't like doing repetitive tasks if I can make a machine do it for me. During this process, I learned that code can be flawed and 'garbage in' leads to 'garbage out'. The difference today with the event of AI and Machine Learning is the level of trust increases and the ability to verify is reduced.

In people we think of 'nature vs. nurture'. We have discovered that most of the time it is a combination of the two that results in the sum of what we are. In the world of AI, the code or algorithms are the 'nature'. These were initially created by people who are not by their very nature, infallible. The 'nurture' is the data we feed this learning machine. The more data we feed it the 'smarter' it gets. However, what if the data is flawed or has an inbuilt bias?

Imagine teaching an AI that 2+2=4. Sounds simple doesn't it? However, if the data we feed is smaller numbers of 2 to one decimal point then it is just as likely that we could find that 2+2=5 for the AI. *"HAL, what's 2+2?"* The answer you expect is 4 but what if you told HAL to learn from a group of data such as 2.1+2.4, 2.2+2.3, 2.4+2.3.

Each of the numbers in these sets of data rounds down to 2. However, the sum of these pairs rounds up to five. So naturally 2+2 equals 5 or *"I'm sorry Dave, I'm afraid I can't do that"*.

Now this is a deliberately simplistic and silly example. Now imagine that you are teaching your new hiring algorithm to filter out resumes. If you only input college graduates, it could develop a bias against a skilled candidate who progressed through another route i.e. Armed forces, Police, Trades etc. As the *'trust'* is in the pile of resumes that pass the AI or algorithm filter, you may never know you have a problem. What you now have is a process that may even breach human rights legislation or local discrimination laws and regulations by filtering out more qualified candidates for the actual role intended. How many of today's leaders might fall foul of a hiring algorithm and not qualify for even an entry level position? Do you really want to filter out the next Bill Gates or Steve Jobs?

The more data you input, the faster the AI *'learns'* but it can also just enhance the bias if we are not careful. Microsoft learned that lesson when its Twitter bot went from innocent child to raging monster in less than 24 hours. (*http://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist*). In that case the data 'fed' was manipulated and the result was obvious. However, what if the data was so large or disconnected that the bias was unknown?

There are many other examples where we are maybe trusting a little too much today and relying on the 'algorithm' to protect us. These include aspects relating to eDisclosure, Redaction, loan qualifications, aggregated news feeds and more.

Don't take my word for it though... *'trust but verify'*.

Appendix B - Real World Turing Test. Would You Pass?

First Published on February 26, 2017

As I sit here thinking about the possibilities and rapid growth of Artificial Intelligence, I start to wonder how much this has already impacted our lives? I suppose the first question should be 'What is artificial intelligence?' Before we go there though, I thought I would check, what is 'intelligence'. Off to Google I go and ask;

"intelligence oxford definition".

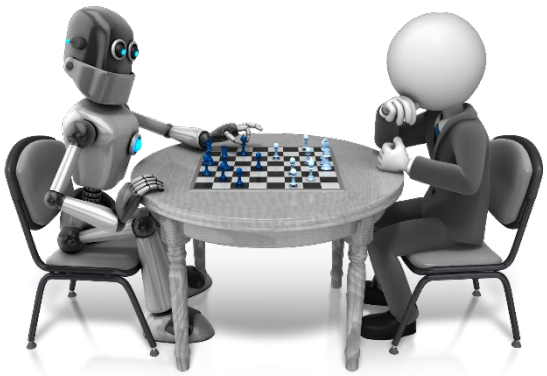
The first result...

"The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."

So, I guess that answers that question. AI 1, Human 0. Intelligence according to AI appears to be something that *'**normally** requires human intelligence'*. So, what happens when AI becomes the *'norm'*? To answer that we should probably go to the first *'norm'* for AI. This could probably be best identified as the Turing Test in the real world i.e. the chatbot. If you have ever interacted with online help, you have already participated in one of the millions of hybrid (person/AI) or pure AI Turing Tests that occur daily.

The next time you respond to the *'Hi, my name is [insert name here]. How may I help you?'* followed by a delay or *'Let me check on that for you'*, ask yourself, is this a person or or this a *'Test'*? Typically, it is an interaction involving both where keyword searches, NLP and other techniques help the actual person respond to many callers at once by focusing the discussion and inserting artificial delays. These artificial delays are similar to how the older automated call centers asked you to *'press one for…'* then *'enter your account number'*. This is was usually followed later in the call by a person asking for the account number you had typed in at the beginning of the call. The key presses in most cases were just to distract while you held on the line for the next person to answer. Once you realized that tactic, or lost patience when this was your 'nth call, it was not too long before you just hit the '0' key and got straight to a person. In the case of pushing keys on your phone, the automated part is easy to identify. However, would you recognize which parts are automated and which are *'human'* in that chatbot conversation?

We may be a long way from HAL's *"I'm sorry, Dave. I'm afraid I can't do that."* AI that can truly pass for 'human' and meet the next generation Turing Test might appear to be a long way off. However, we are now in a world of twitter, text and other forms of instant messaging which have become the *'norm'* for human interaction. As such, we could be inadvertently making it easier for the machine to meet our new conversation standards. When conversations are limited to 140 characters or less, the bar for communication isn't so high. Reduce that further to emoji's and acronyms and we are moving our standard closer to that of the early chatbot's. Just as AI learns recursively through repetition, so do we. The current trend continues to erode the formal communications the older generations were used to in favour of short bursts of



chatter. As a result our day today, electronic interactions are starting to look more like that of the AI.

With the evolution of communication, maybe the question now becomes, would a modern-day human interaction pass the Turing Test of old? Is it more likely that you might be mistaken for a computer trying to behave like a human? Press 1 to answer yes, press 0 to answer no.

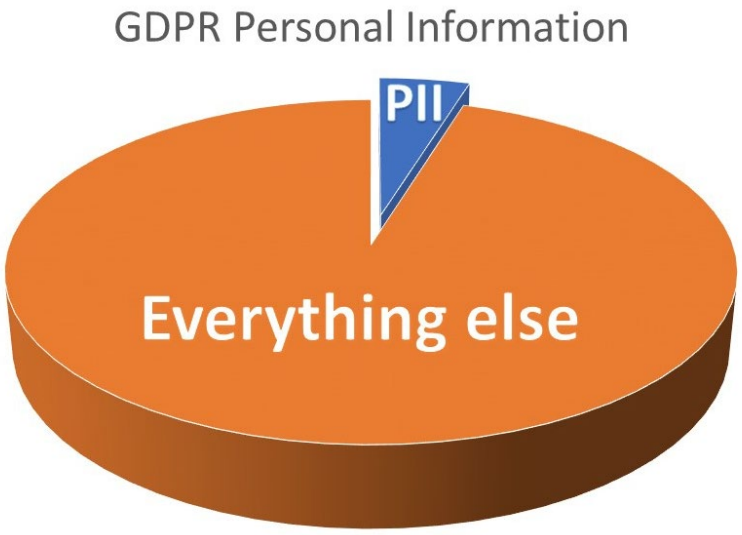
Appendix C - Data, Data, wherefore art thou, Data!?

Published on June 4, 2017

Cybersecurity, Compliance and Consent. All words to live by in the data rich world we live in. Data is the new Oil just as Oil was the new black gold. Most data breaches are looking for **Personally identifiable information** *(PII)*** even before Financial Data. In some of the largest recent data breaches financial data was ignored because it had no 'shelf life'. Credit card numbers can be changed but your date of birth might be a bit harder.

****Note:** Since this article was written, GDPR came into full effect bringing with it the expanded definition of 'personal information' that went beyond PII.

"means **any information** relating to **an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier **or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;** "



Have you ever asked yourself;

- Do we know where our data is?

- Are we compliant?
- Did we get the appropriate consent to use that data?
- Who has access to the data?

The IT department will usually answer, 'Yes, it's in the cloud, yes, we assume we are compliant or the legal and compliance people would have said something and we use the data the way the business wants us to'. The Legal and Compliance departments mirror that comment with assumptions that IT would have made sure it was safe, secure and compliant. Does this sound familiar?

'We used a well known system/service provider with lots of security'

- 'We made sure our data was in our own domain'.
- 'We did a full Privacy Impact Assessment'.
- 'We have full control of all our data.'
- 'XYZ Company/City is already using the same system.'
- We have an open policy so data location and access is not that important.
- Our customer gave us the data so we can use it however we want.

But do you know where your data, records and email are? Do you know if you are compliant? Do you know what you can do with this data? How secure is that data?

The following outlines a Canadian viewpoint but can equally be applied to the EU (GDPR, NISD) or US (Patriot Act, Privacy Shield, EO 13768, Cloud Act and more).

Government bodies advise against using data centers outside of Canada for private/sensitive data but often the reasons cannot be articulated. *'They didn't say I can't use Amazon, Google or Microsoft's Cloud'* is often stated with less confidence than you would expect. It seems companies have a gut feeling that there is an issue but can't really put their finger on it. With no-one holding up a sign outlining the specific section in FOIP, PIPA, PIPEDA, CGSB, ATIP, CASL etc. that prohibits it, companies just move ahead blindly into a compliance quagmire. Did you

know that having a compliant approach to handling data is an important step to showing due diligence in the event of a breach?

Finally, we may have reached an area of thinking where the human mind and experience can compete or even think beyond the linear focus of AI and into the big picture world of Global Business Architecture. You could look all day through those individual pieces of legislation and not find anything to prohibit or even discourage international hosting of data, records or email. To find the reason, you have to look beyond the local legislation. The answer lies in the legislation, practices and policies local to where and who with the data resides and the constraints it imposes.

The nebulous nature of electronic data and records makes it hard for people to comprehend the challenges. To most *'in the cloud'* just means stored 'elsewhere' and accessible locally from anywhere (laptop, phone, tablet, web browser). The reality is all you really have is a digital photocopy to view.

Imagine if your Canadian master paper records were stored in a warehouse somewhere in the US, or Europe. Each file folder could be stored with millions of other customer records. These file folders could be distributed throughout dozens of warehouses. This would enable your company records to be more easily indexed and accessed. Maybe all the records 'a-c' are in one warehouse and 'd-f' are in another. These could be stored along with similar records from many other individuals and companies. This would be to make the recovery of those records easier for the *'service provider'*.

Now when you request a record you get a photocopy mailed to you. At each stop en-route, there could be other *'temporary'* photocopies made and held for a period of time. If you need to make a change, you send a modified photocopy to the *'service provider'*, using the same process, with the assumption that it replaces the old

original record and no unauthorized copies or versions exist. This is only a hope as the custody care and control is now shared. The local authorities can access that information at anytime under the local legal powers but you won't always know it has happened. As a result, you can't let your customer know who has accessed that file. You have been assured that *'your'* files are secure though but the service provider can't identify exactly which warehouse each file is in as the whole system is a *'black box'*. I think I just heard a privacy and compliance officer weep! This would be bad enough even if you assume that none of these warehouses have been compromised and records removed, destroyed or changed. What company would even consider such a scenario for their mail-room or records department?

So, back to the cloud and the world of electronic data, records and communications. At each point in managing personal data (including things as simple as an email address) you should know some of the following;

- Where is my customer (in a global market you may have global customers)?
- How and where was the data collected and under what authority?
- What can I use it for?
- What do I use it for?
- How must I manage it (security, privacy, audit, retention, accuracy and more)?
- Where is it stored (and where are the copies, if any)?
- When I access the data, does it go anywhere else or are there 'temporary' copies made (store and forward)?

Now look at each of these questions specifically from the geographical legislation it falls under. Imagine that the data is stored in an EU data-center (you think, although it could be distributed over US and EU data centers). Your customer is a US citizen and you are a Canadian company. You discover a privacy breach, or worse, your customer informs you of a privacy breach they have been made aware of. Do you know the impacts to your business?

It is also important to remember that not all data breaches are brute force hacking from the internet. Sometimes your data can leave with an employee or consultant (either willfully or otherwise i.e. Edward Snowden a fired employee or a lost phone). Some of the largest data breaches in recent history have relied on the human factor to bypass Cybersecurity solutions from the inside. These could be willful removal of files to email attacks such was Wannacry or the John Podesta phishing email. Do you know;

- Who has access to the data (employees, consultants, third parties)?
- Can you manage or remove access to data at a moments notice? This has been standard with tools such as Good, Citrix or Microsoft security policies.
- Can you control the data when it leaves your environment? Did you know Microsoft has a solution that can control document access outside of your environment?
- Do you have a responsible data security policy and system for BYOD? Can you control which devices have access to data and what they can do with it?

Allowing employees to access and download email on a personal phone, tablet or home PC that doesn't have even a rudimentary password policy can leave your organisation exposed. It was bad practice before the cloud became so popular, what would make people think it was OK now?

What can you use that data for? In a world of AI, Big Data and Machine learning it is so easy to reuse that large store of data you have been collecting for new and exciting purposes. However, if that data was collected for a specific purpose you may have to get new explicit consent from the owner of the information. Just because you have the ability to crunch data technically, does not mean you can legally. You might have a list of email addresses but CASL has something to say about spamming even your existing customers.

Don't wait to discover you are not compliant, safe and secure. This is an area where the law in all geographical areas is quite unforgiving and *'ignorance is no excuse'*. It could cost you more than you think.

It's never to late to address the problem but it may be too late after you discover a breach or fail an audit. In the world of the cloud, like real estate, you should always remember, location, location, location.

For an example of how this impacts the view of information you may have and how the unconnected can become connected. Einstein Puzzle REBOOTED.

Appendix D - Sometimes the Destination is more important than the Journey.

Published on July 19, 2017

Following on from my article on Data Sovereignty and compliance (*Data, Data, wherefore art thou, Data!?*), the focus recently has moved from Data at Rest (where data is stored) to Data in Transit (data moving along the ether(net)). It has reached a point where it has become a distraction from data sovereignty to the point that organizations are split between two conclusions.

- We can't stop our data crossing the border when in transit so it doesn't matter where it is stored. Conclusion, store it anywhere with a reputable company.
- We can't stop our data crossing the border when in transit so we shouldn't move to the cloud. Conclusion, digital transformation stagnation.

Both of these conclusions suffer from the same issues relating to assumptions on Risk and Compliance. The assumptions are that Risk and Compliance equally relate to Data in Transit and Data at Rest. This is an incorrect assumption. You can't be compliant with data not under your control. However, you can be responsible for the data that should be under your control.

Imagine if that same assumption was made for Phone Calls or Regular Mail. Would you only call people inside the office on a closed loop telephone system? Would you only send mail internally and by person? The answer is obviously, no.

But they are not the same, I hear the cry. Actually, the dissemination/ transmission of information through each of these processes is essentially the same.

Look at the following scenarios;

A customer calls your office to discuss a file. At the outset of the call, you inform the customer that *"call's will be recorded for….reasons"*. That recording would most likely be digital and will contain Personally Identifiable Information (PII)** subject to privacy legislation. As such, it

requires a level of security and management to ensure it is not compromised. However, the method of collecting that information i.e. the phone call, is outside of your control. Is the customer recording the conversation, is a third party monitoring it, is there a legal or illegal wiretap on the line? All of these scenarios are possible, but out of the control of your organization. Does that mean that the recording you have doesn't need to be treated according to best practice and privacy laws? No, of course it doesn't. Does it mean that a breach of access to that recording is meaningless because the information may be stored (or monitored) elsewhere? Of course not. The recording you have is unique and most likely contains additional information, not part of the call i.e. unique identifiers and links to a client file, notes from your company staff, metadata from the call itself. This makes a potential breach identifiable back to your unique source, under your unique control. So, although the risk and compliance relating to the external parts of the call i.e. external VOIP lines, external servers, caller's phone, people in the room with the caller etc. are outside of your control, the data at rest in your organization is not. Unless you were negligent in knowingly allowing another party to illegally record or listen to the call, without the customers knowledge or permission, there is minimal risk. Trying to secure those transmission lines, outside of your control would be impossible outside of a closed loop system.

Take that same discussion but this time it is between two separate offices of your organization, one in Vancouver and one in Toronto. Again, you can control the environment at the two endpoints but not the lines in between. You can increase the security for inter office communications but more on that later.

Now take the same scenario but this time with letters between your company and a client. This letter will contain, names, addresses, client number maybe even credit card details or health record details. Do you ask the customer to pick that up from the office for fear of it being read while in transit? No. Again, if you sent this letter completely open (not in a sealed envelope) then you have an issue with negligence and privacy breaches. However, this isn't how the world works. Even Revenue Canada uses regular Canada Post. Would you refuse to send the letter to certain areas of the world because it might cross an international and legislative line in transit? No. Even secure mail between offices might cross international borders during transit, that does not automatically create a non-compliance or privacy risk.

In both of these scenarios, we have communication with a client and inter office communications where PII** and more is exchanged. In both scenarios, there is a significant risk that data has been transmitted through a third party, not under your control, and as a result it could have been transmitted across international borders.

Does this mean that you have breached privacy legislation? Maybe if you did this in such a fashion that guarantees a data breach then you have bigger issues. However, if you have followed good business practices and maintain compliance, would this stop you from communicating externally? No.

In both of these scenarios, there are ways to increase security for phone calls and regular mail, where required. For phone calls *(inter office, B2B and even to your customers)*, use encrypted VOIP lines. This can also have a cost benefit and increase functionality over a regular phone line using systems such as Skype for Business *(not the consumer Skype system)*. For regular mail, you can use secure and even serialized tamper proof envelopes with checks and balances at both ends. Making these extra security steps mandatory or even a general standard for best practice would seem overkill, yet this is the standard for electronic

communications through the cloud. Essentially, your data (and your client's data) is probably more secure in transmission to Compliant, Data Sovereign cloud providers than that phone call and letter you think nothing of providing.

Would you be more concerned with someone getting direct, unfettered access to your phone or mailroom or intercepting that call or letter en route? So, why is data in transit such a concern?

Even if you think you have a closed loop secure system for transmitting information, chances are you don't. Is your network connected to the internet? Is there anyone else in the building sharing infrastructure *(phone or internet switches provided by external vendors etc.)* or are you in multiple buildings without a dedicated hard line between them? Then you have a data in transit risk. That risk is not controllable and is minimal as long as basic precautions are taken.

Remember, most security breaches for electronic data occur at rest due to poor security, human error or deliberate human action. Moving to the cloud can decrease those risks, if implemented properly and with a compliant organization i.e. with an infrastructure that ensures your data at rest is compliant i.e. in your legislative jurisdiction for PIPA, PIPEDA, FOIP GDPR etc.

So, instead of dismissing the cloud because of the risk outside of your control, look at the benefits it can provide in security, compliance, scalability, functionality and cost savings.

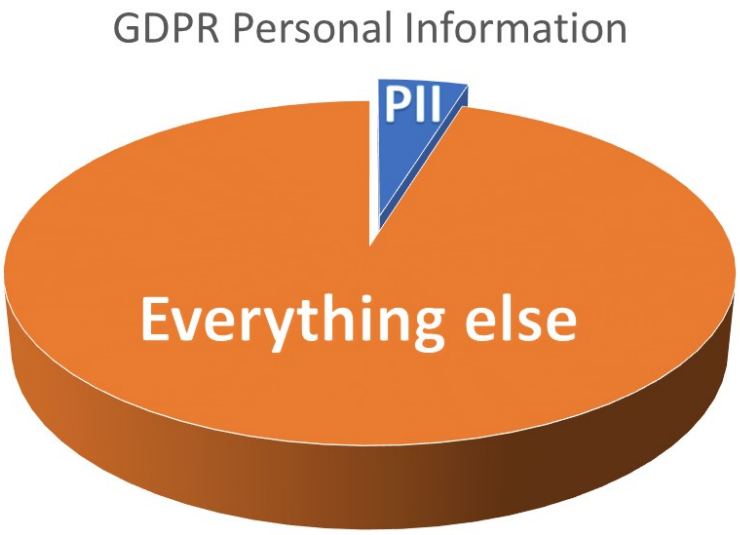
Are you more at risk for having your credit card stolen on the daily drive to work, or having your house, office or car broken into? It doesn't take a retired Police Officer like myself to answer that question.

Considering all the billions of electronic communications moving through the billions of lines in the world, what is the chance that your communication will be intercepted and used against you or your customer? The answer is very slim. It is all about return on investment and risk. Target your internal infrastructure where there is a large amount of data that can be captured and many lines of attack.

"it's not the destination but the journey" is the common adage. In this case, the journey (Data in Transit) is important and should be secure and compliant. However, we really should focus on the destination (Data at Rest), especially when looking at the cloud for the future. Pick a compliant data center, follow best practices and embrace the future.

****Note:** Since this article was written, GDPR came into full effect bringing with it the expanded definition of 'personal information' that went beyond PII.

"means **any information** relating to **an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier **or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;** "



For an example of how this impacts the view of information you may have and how the unconnected can become connected. Einstein Puzzle REBOOTED.

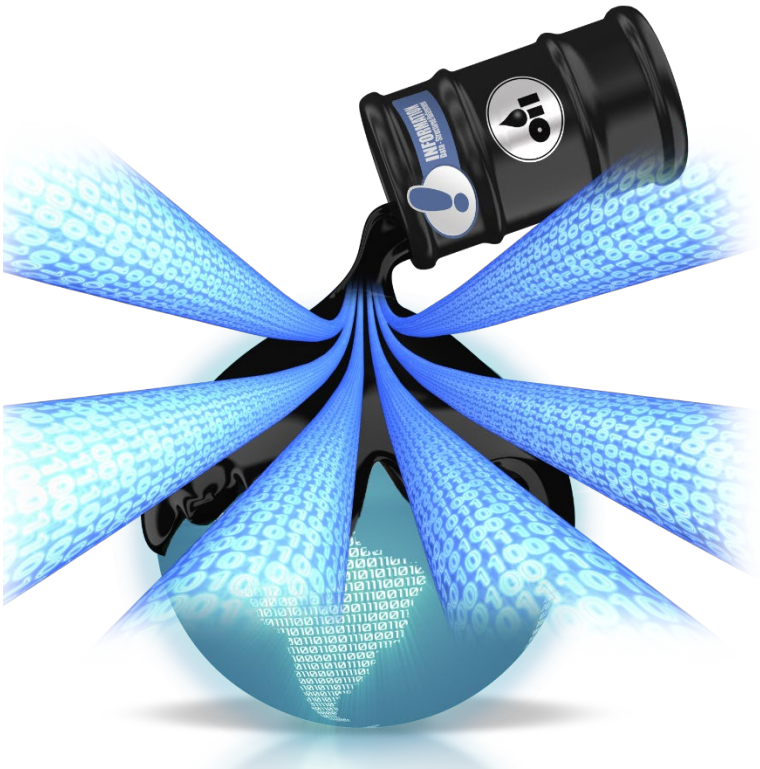
Appendix E - Cyber-security, Compliance and Consent.

Published on December 4, 2017

When “No Means No” is not enough.

Note: This article is availble in Video format with soothing background music [Link].

Data is the new Oil is the new rally cry for investors. They do share a common challenge. An oil spill can be devastating to an organization as well as the environment.



A data spill (or data breach) can be just as devastating to an organization and its customers.

So, why do we handle data so poorly?

Cyber security is top news today. Too many organizations think they are either too small to matter or their data isn't significant because they are not the only ones that have it.

The bad news is neither is true.

In recent months, I have written about AI, Chatbots, Data Sovereignty, Data In Transit and more. What do these areas have in common?

Information.

In today's world, we gather information, both structured (databases etc.) and unstructured (documents etc.) at an alarming rate. Due to the global digital transformation, the line between structured and unstructured is already becoming blurred. As a result, the challenges of managing all of this information responsibly can become incrementally more challenging. However, this can be more easily navigated with a responsible approach to digital transformation.

So, how does this impact you and your organization? The answer boils down to one focal point.

Consent – more than just a definition in the legislation.

Consent under GDRP and other privacy legislation has a narrow definition. However, it is important to view "Consent" in its larger dictionary definition when looking at information under your care, custody and/or control.

Understanding cyber-security, physical security, legal and compliance rules is a complex task. However, by taking each area and applying one simple question will help clarify what you can, cannot, should or should not do.

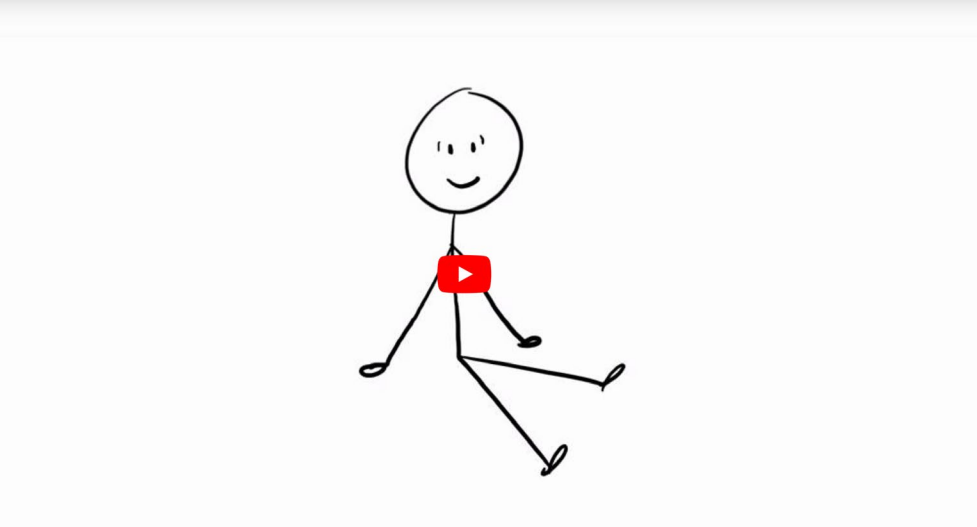
Ask yourself;

Would the customer/owner of the information truly "consent" to what you, or someone else is about to do (or has done) with the information?

This could be anything from an unauthorized breach by an internal/external party (cyber-security) to a new use of the information such as using AI/Machine Learning/Deep analysis or even third-party disclosure (compliance/legal) for something other than the reason it was originally gathered.

We have all heard the cry ***"No Means No".*** However, in real life, you don't actually have to say ***"No"*** to mean ***"NO"***. This short (2:50) video by Blue Seat Studios illustrates Consent in the non digital world.

Link: Consent a cup of tea solves everything.



I'm going to need an explicit YES.

In the digital world, ***"NO"*** is usually inferred **AND** you need explicit consent to show otherwise at every step of the information management, analysis and transformation. Be prepared to show a time and date stamped explicit acknowledgement of everything from buying the tea bags, to washing the cups (and everything in between or after) in the above example, especially if you suddenly want to make coffee!

Article 4 of GDPR (11),

“(11) 'consent' of the data subject means any **freely given** , **specific** , **informed** and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;”

Although the wording may be slightly different in each privacy legislation, the intent is the same in most cases.

To further complicate matters, most privacy legislation has focused on identifying 'personal data'. For GDPR, this has been expanded to;

“means **any information** relating to **an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier **or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;** ”

“Once more unto the breach, dear friends”

There are many forms of breach beyond having your data stolen by a foreign hacker. Effectively an unauthorized access or use of the data you have custody and/or control is deemed a breach. You should assume that no matter what your privacy policy might state, customers do not consent to a breach.

Just because they don't drink the tea, doesn't mean you can give it to someone else or leave it out for someone else to drink.

Ask yourself;

- Has your customer truly consented to storing their data in the current location *(#datasovereignty)*?
- Would your customer be happy if a foreign government or third party accessed their information without their knowledge?
- Would a customer be happy with you using the data in new and exciting ways?
- Does your customer (or you) truly know what data you are collecting, or is being collected by systems you have in place?
- Has your customer consented to storing their data in the current location?
- Would your customer be happy if a foreign government or third party accessed their information without their CONSENT?

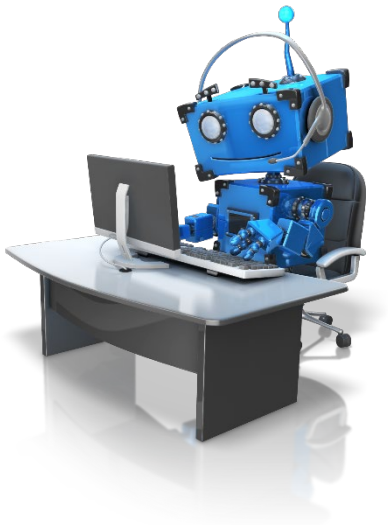
Think about hosted systems that may be gathering and extrapolating from your customers' use of your systems hosted or supported by others i.e. the digital supply chain for information;

- e-Commerce
- Web Sites
- Apps (voice, data, video)
- Chatbots
- Third Party WiFi hosts

Can they hear me now? *(Who's listening?)*

The IoT devices we now see proliferating our every-day life are always listening and collecting data to 'make your life better'. However, did the client who just walked in to your office, consent to their voice or other data being captured, stored and used by a third party?

- Think home/office automation and the IoT *(Google Home, Siri, Amazon Echo and more.)*



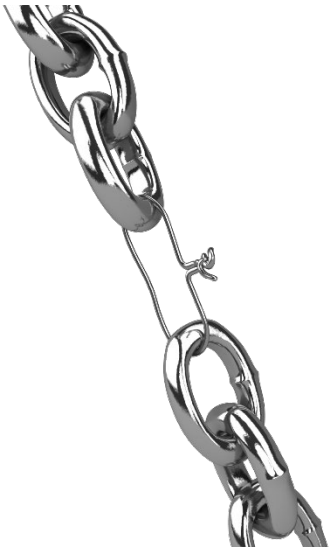
Do you really know what information you have in your

If not, then you probably should rethink your process for obtaining informed consent, change what data you collect, the way you collect it and how it is stored/accessed.

Do you know what to do if you discover a breach?

- **Clue:** *Paying hackers and trying to cover it up is an **'uber'** bad decision!*

The digital information supply chain, end to end.



Third parties may be collecting data at various levels as a bi product of the services they provide. Do you know what they gather and what they do with that data? Do your clients or other individuals who use your systems or premises know that they may have their digital identities or other personal information captured? An unintentional (or intentional) disclosure of this information to a third party could be a breach.

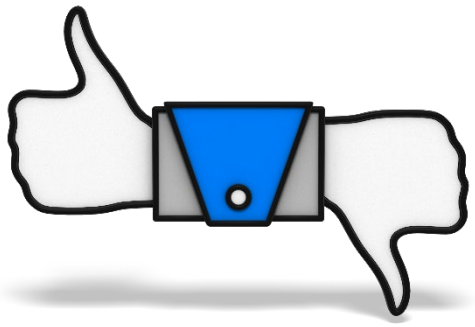
Don't be a weak link in the supply chain and don't be a victim of another weak link.

Is an expectation of privacy reasonable anymore?

If you are in a private location or you have provided data willingly, you may have a reasonable expectation of privacy. Is that realistic anymore in a consistently monitored and digitally connected world? If not, what are the implications to the new privacy laws and society as a whole?

Are we even trying to maintain our privacy anymore?

When we discover that our personal data has been compromised, we cry from the rooftops about the injustice. Yet we have probably provided that same information (and more) on social media, at restaurants and over the phone many times before without even a passing thought. This information is collated, analyzed and extrapolated from us in milliseconds.

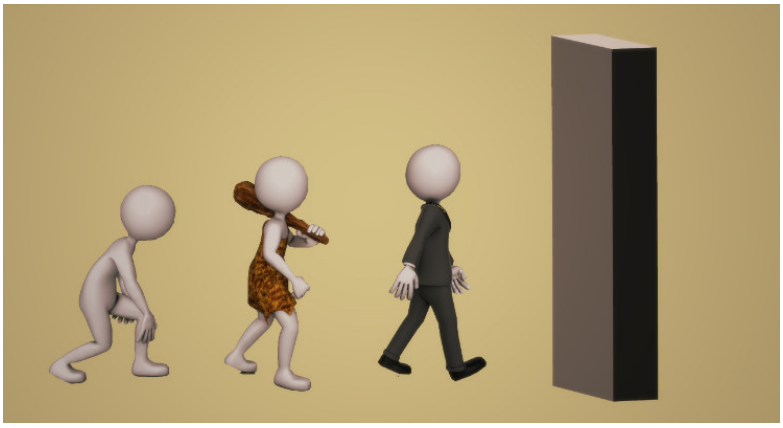


This does not excuse lax security and privacy in business… but it should make us think.

*We **ALL** have a role in the privacy equation, and it is an important one.*

Appendix F - The First Digital Evolution

Published on January 31, 2018



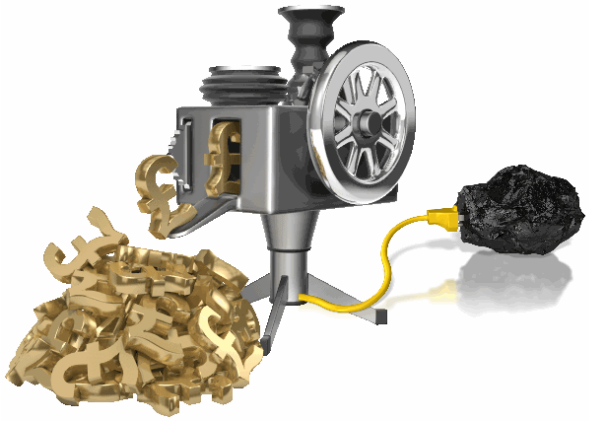
Are you ready? Blink and you might just miss this one.

The First Industrial Revolution;

In the 18th and early 19th century, we discovered how to automate and collaborate with machines to change the way society worked. This was assisted by the introduction of the steam engine. The power and the knowledge was fiercely protected by industry to maintain control. Professionals with access to that knowledge were sought and revered.

It was the start of industry so the focus was industry. People could not own personal factories at their home. People were therefore the secondary market.

The Second Industrial Revolution;



The 19th and early 20th century saw the expansion of automation and the harnessing of electricity, steel and other technologies expanding the power of industry to meet the needs of the people i.e. customers and workers. To further ensure power and the knowledge could be controlled, we saw the introduction of laws and organizations controlled by industry, government and professionals.

This was an expansion of industry so again, the focus was industry. The new machines and tools were not available for home use or home-based businesses. They were controlled by industry for the primary benefit of industrial powerhouses. People were again the secondary market.

The Third Industrial Revolution - or the First Digital Industrial Revolution?

Starting mid-late 20th century until the early 21st century, computers and digital technology expanded at a rapid rate. Although some of these tools were put in the hands of the public, the primary focus for new technology was industry. The access to some of the resulting technology helped spark the next revolution as the public started to gain access to tools and knowledge that had, to this point, been restricted.

It was the start of a Digital Revolution. Again the focus was industry first. People could not own chip manufacturing facilities at their home or install industrial robots to build things. People were the secondary market but this was now driven by a new digital age. It was more than factories and mass manufacturing. The things being manufactured propelled us towards the day when people could become the primary market for new technology.

The Fourth Industrial Revolution - or the First Digital Revolution and the First Digital Evolution?

Technology, biotechnology, computing power, software and manufacturing is now being targeted at industry and people simultaneously. This is no longer an Industrial Revolution as its focus is not just on industry. It is no longer just a revolution as we move into AI, Biotechnology and more. We are hurtling towards the first Digital Evolution.

For thousands of years, humanity edged forward (then backwards in the 'Dark Ages') before reaching the First Industrial Revolution. This lasted almost two centuries before the changes marked the Second Industrial Revolution which lasted almost another century. The Third Industrial Revolution was less than a half a century old before we needed to 'invent' another. Now we have moved through a Digital Revolution that

has bypassed industry; it places power in the hands of people in the blink of an eye, followed by what can only be described as the Dawn of the Digital Evolution. Now technology replaces biology, encompassing everything from implants and enhancements to AI.

In previous revolutions, we were the watchers and overseers. Unions were formed to ensure workers' rights. Regulations and safety codes were created to protect workers' lives. Laws were created to protect everything including our privacy.

Above all, we monitored what was happening and made decisions on what was right and wrong. This led to obvious abuses by those in power but the will of the people still had some impact on the powerful. As with everything, human greed and other fallibilities made for an imperfect world but we never took our eye off the ball, so to speak. During the Third Industrial Revolution, the most powerful men in the world met to prevent an escalation of power and divide that brought us closer than ever to annihilation. In a world that was facing a rapid evolution of digital technology, people made the ultimate decisions. That meeting of East and West gave us the famous words 'Trust but Verify' .

Knowledge is powerful and has been controlled, used and misused by those in government, industry and professional spaces throughout these Industrial Revolutions, dating back to the dawn of humanity. Those who knew how to build tools, tell stories or make fire were those in control. Now there is instant access to all knowledge with the command 'Siri..., Alexa… or Google…,' is power back in the hands of the people? Or, to quote a Japanese proverb;

"Knowledge without wisdom is a load of books on the back of an ass."

I looked that up on Google. I have no idea if it is true… but it sounds good. And it is on the internet so it must be true!

We live in a world of fake news and social engineering through social media. Technology and simple AI such as Siri, Alexa, Google etc. are the fountain of all knowledge, despite the known algorithmic and data driven bias. Ironically, in a world based on science, we no longer question...

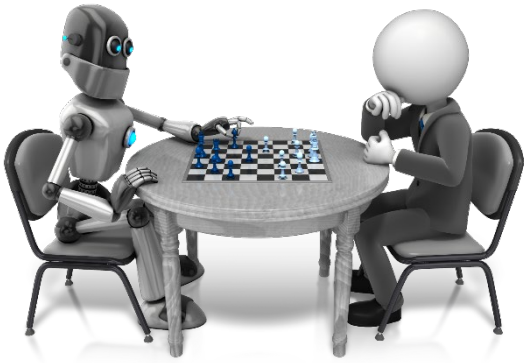
we blindly accept the all-knowing black box. Now that is железный in its truest form. Who just pasted железный into Google?!

We may no longer need ‘experts’ to gain knowledge but we should never lose sight of the need to apply wisdom to that knowledge. After all, what is fake knowledge without wisdom!?

The role of the 'expert' is changing from font of knowledge (or keeper of the keys), to purveyor of wisdom and filter for the truth. As consultants, professionals or 'experts', our role is changing. Our clients are no longer uninformed, they do not lack knowledge and they do not assume we are all seeing and all-knowing to be believed without question. This is a good thing but it comes at a price. We now have to filter the good from the bad, the fake from the real and not only be knowledgeable but be able to demonstrate the application of that knowledge with wisdom.

The age of consultant, professionals and 'experts' will not be replaced with the coming of AI and the evolution of the digital information age. However, it will be forever changed. We must adapt quickly or be swept away in a tsunami of unchecked information.

We need to be the child from the Han's Christian Anderson's, Keiserens Nye Klæder (The Emperor's New Clothes).



When confronted with the latest technological attire, have the wisdom and courage to exclaim;

'He hasn't anything on!'

The First Digital Evolution is upon us. Blink and you just might miss it. The access to knowledge is back with the people. But are they ready for that responsibility? Blind faith in technology will not set us free. More likely it will enslave us to the new digital keepers of knowledge and wisdom. Maybe when I post this article, it will be rejected by a chatbot saying;

“I’m sorry, Dave, but I’m afraid I can’t do that”.

Appendix G - Social Media or Social Engineering…

Published on February 6, 2018

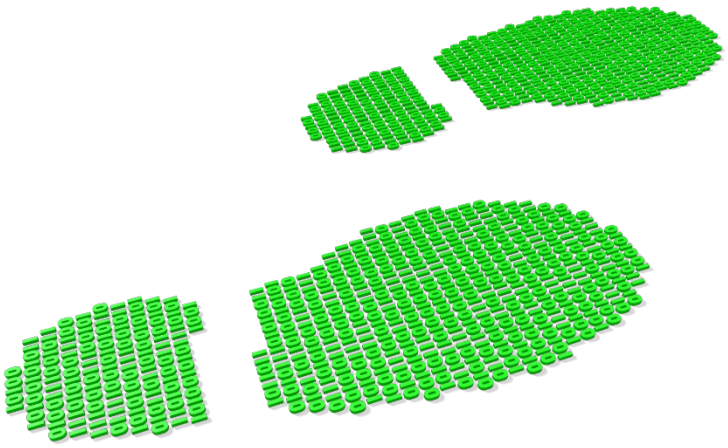
When they know more about you than you do about yourself.

We all worry about protecting our privacy but surprisingly we give it up daily. If the supermarket clerk asked to see your driver's license you would think twice. You stand at the checkout wondering if anyone can see that 4-digit PIN you tap in. However, we give away private details without a thought all through the day. If the clerk 'liked' your PIN, would you let that clerk or anyone else see it?

In addition, social media and the internet is grabbing and analyzing data about us on a scale that could not have been imagined a few years ago.

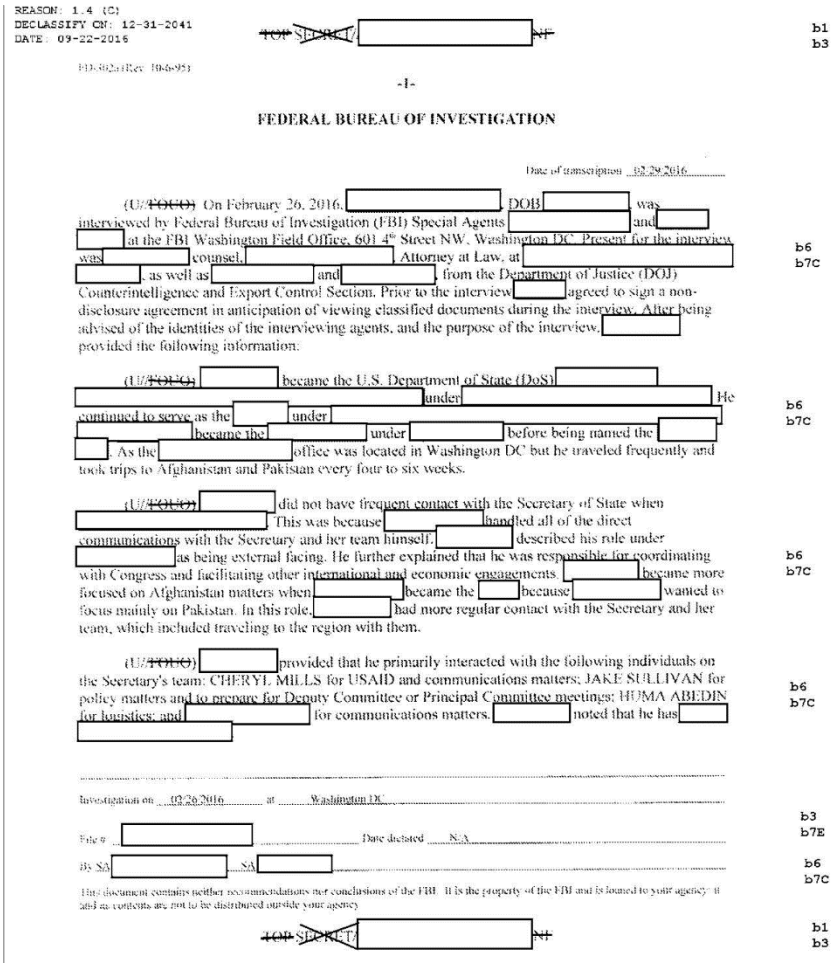
You sit down to watch the latest series on Netflix. You open your browser. You log onto Facebook. You check your email. You spit into that 23 & Me or Ancestry DNA test tube. Have you noticed how all of these companies know what you like, what you have been looking for and how targeted emails, suggestions and advertisements keep popping up? This isn't magic or coincidence. It is big data analytics, Machine Learning and AI all building a profile of your every digital breath.

We all have a digital footprint that is shared online. This can be used to cross reference all the information available to build bigger and better profiles. All in the name of marketing. In some cases, it is even the absence of information that can help build a better profile. In my years analyzing redaction (the art of removing identifying information from documents etc.) or 'black lining' as it is sometimes called, I have seen how missing information is easily extrapolated.



This is just the tip of the digital iceberg though. Without data, AI and Machine Learning would starve. So, they need more data to feed the beast. Luckily for them, we are happy to oblige and provide a veritable feast of personal information with abandon. In most cases we don't even know we are doing it. Social media and all of the electronic devices we invite into our lives, are purposely designed to provide the feedback we all crave.

A quick look at the much-publicized FBI redacted meeting notes from 2016 shows how even professionals can still get it wrong. We assume that just the Personal Information or PII (as it is still called outside of newer privacy legislation such as the GDPR) needs to be removed to protect our identity but fail to understand that we are more than just an email and date of birth. We are what we do and say and we share that information without a thought.



REASON: 1.4 (C)
DECLASSIFY ON: 12-31-2041
DATE: 09-22-2016

~~TOP SECRET~~ [redacted] ~~NF~~ b1 b3

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/29/2016

(U//~~FOUO~~) On February 26, 2016, [redacted], DOB [redacted], was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] at the FBI Washington Field Office, 601 4th Street NW, Washington DC. Present for the interview was [redacted] counsel, [redacted], Attorney at Law, at [redacted], as well as [redacted] and [redacted], from the Department of Justice (DOJ) Counterintelligence and Export Control Section. Prior to the interview [redacted] agreed to sign a non-disclosure agreement in anticipation of viewing classified documents during the interview. After being advised of the identities of the interviewing agents, and the purpose of the interview, [redacted] provided the following information: b6 b7C

(U//~~FOUO~~) [redacted] became the U.S. Department of State (DoS) [redacted] under [redacted]. He continued to serve as the [redacted] under [redacted] became the [redacted] under [redacted] before being named the [redacted]. As the [redacted] office was located in Washington DC but he traveled frequently and took trips to Afghanistan and Pakistan every four to six weeks. b6 b7C

(U//~~FOUO~~) [redacted] did not have frequent contact with the Secretary of State when [redacted]. This was because [redacted] handled all of the direct communications with the Secretary and her team himself. [redacted] described his role under [redacted] as being external facing. He further explained that he was responsible for coordinating with Congress and facilitating other international and economic engagements. [redacted] became more focused on Afghanistan matters when [redacted] became the [redacted] because [redacted] wanted to focus mainly on Pakistan. In this role, [redacted] had more regular contact with the Secretary and her team, which included traveling to the region with them. b6 b7C

(U//~~FOUO~~) [redacted] provided that he primarily interacted with the following individuals on the Secretary's team: CHERYL MILLS for USAID and communications matters; JAKE SULLIVAN for policy matters and to prepare for Deputy Committee or Principal Committee meetings; HUMA ABEDIN for logistics; and [redacted] for communications matters. [redacted] noted that he has [redacted] b6 b7C

Investigation on 02/26/2016 at Washington DC

File # [redacted] Date dictated N/A b3 b7E

By SA [redacted] SA [redacted] b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~ [redacted] ~~NF~~ b1 b3

Digital photographs contain mammoth amounts of detail from the location, time taken, who you are with, type of camera/phone used and more. Upload that photo and it gets tagged to your own digital profile after which it is liked (or disliked etc.) connecting it to many more profiles.

In those innocuous posts to Facebook, Twitter, Instagram and more, we provide detailed insight into every aspect of our lives. Political views, personal preferences, people and places we are connected to, all in a single photograph. Until recently, the text was the primary target for profiling and provided a wealth of data to create our digital profile. Now we can analyze images and other 'structured data' (documents, pictures, video etc.), read the metadata and more. This can be cross referenced to our and every other digital profile in near real time. Imagine the wealth of data hidden in the random Snapchat image that really has no value to you, other than to allow you to text a message!

I recently posted that we don't think about unstructured data enough. Consider the following example. Someone emails (or posts) a picture of you in front in a doorway holding a birthday cake saying "Happy 30th, Dave!" Photo taken on smart phone weeks earlier. How much Personal Information does this image disclose?

- Name
- Age
- Date Of Birth (from the timestamp of the picture and the image of the cake).
- Sex
- Eye colour (just zoom in)
- Hair colour
- Approximate weight and height (just compare to the standard dimensions of that door frame),
- Location (GPS data embedded in the picture).

With enough data (easily obtained in our 'selfie-obsessed' age) and technologies such as point clouds i.e. Photosynth, we can even work out the exact spot the photographer was standing in and who else was in the room.

If anyone has watched ‘The Circle’, you may be shocked to know that even without those little cameras, your digital profile is working against you. Now add in the Internet of Things (IoT), voice and video enabled devices and we open ourselves to even more data collection. Ask Google for the local pizza store and suddenly you are bombarded with pizza coupons. Sometimes you don’t even have to interact to be targeted. In some countries, the cell towers are weaponized for marketing. Just being in a location can trigger geolocation texts. All this information goes back to be stored and analyzed at a later date. As AI gets smarter, the information that can be gleaned grows exponentially.

At present, it isn’t perfect because multiple people can use multiple devices. I, for one, would rather not have Netflix assume I am an avid Paw Patrol watcher and so push more programs like that. However, when my grand-daughter comes to stay, Paw Patrol rules! These nuances on whose data belongs to whom will soon be extrapolated as more data is analyzed and AI learns. In the meantime, we are exposed to potentially unfair bias, misleading (and annoying) advertisements and suggested posts/shows. What if that misinformation gets tagged to your credit score though (spoiler…it probably already has to some

extent)? Now what happens when there is yet another security breach? Would you rather criminals (or governments) had correct or incorrect data on you?

We trust that all that data is secure. We assume it is unusable beyond its original purpose for disclosure. However, large companies are looking at ever new ways to use that data to build a better profile. These profiles are more valuable than the best Cryptocurrency in circulation. The more detail they contain, the more valuable they are. It is frightening enough just thinking what a marketing team might use these profiles for… what about your insurance company? Now what about all those data breaches that keep happening?What if your whole life is stolen and becomes available? You can change your credit card number, you might even be able to get new ID or even a new gender but can you really change the fundamental way you are and how you behave?

Imagine you are using Facebook and Google for the first time. You provide both with an email address and password. At this point they know nothing of you…or do they? They will know where you logged in from, what type of devices you use and have access to the history of the devices including websites, apps and more. This is before you even send an email or make your first post. Fill in the complete profiles they ask for and they already have enough information to fill out more than just a basic credit card application.

What if you use a different email and password for each? Do you also use different devices? The answer is probably no. So, the digital profiles get connected and now they have even more information about you. At this point you still haven't done anything.

However, once that first email comes back, you get a warm fuzzy feeling…'somebody cares about me'. Post your first photo or status and wait for the likes. The feedback starts to become addictive, as it was designed. How do I get more likes? Make more posts, provide more information, make controversial statements. Each of these adds to the detailed picture of you. Then you like someone else's post and suddenly you are seeing posts that are similar in your daily feed. You see one that says, "So and So likes Diply". Did you like that post because they

liked it? Did you notice that it didn't say "So and So likes this specific post"? Probably not. However, the system now knows a little bit more. Sometimes you ignore the feed it gives you. That provides a wealth of information about you also. As these systems talk to each other and exchange information they get to know you piece by piece. But they provide anonymous data, I hear the professionals say. I will again point to the exercise in redaction. If enough information is shared, you don't need an obvious Personally Identifiable Information (PII) connection to have exposed Personal Information.

Digital profiling is like the world's biggest game of Clue (or Cluedo for the Brits out there). No-one knows who is in the envelope but if you ask enough questions you can narrow it down really quickly.

For an example of this see my article on the Einstein Puzzle Rebooted.

Now imagine the wealth of information attached to some of the most sophisticated analytical systems imaginable and it is easy to see how vulnerable we can be.

AI and Machine Learning is now taking that one step further in order to 'guess' what you will do next, even before you do it. A company recently created a profiling system to 'guess' if a realtor's contact is likely to sell their house soon. All the realtor has to do is upload his contact list. Did his contacts (maybe not all clients) give him permission for that? Now suddenly they are receiving posts on house renovations, moving companies and more. They have no idea where these came from though.

So, before you make that next post, upload that next picture or even send that next email, consider what you are giving up. Read those privacy policies a little more carefully. Even if the company that collects the data does no harm, when a security breach occurs, ***the new possessor of your information probably didn't read the privacy policy either.*** They may also have breached multiple systems so are able to build digital profiles more sophisticated than Google or Facebook could dream of.

The genie is out of the bottle and is not likely to be put back anytime soon. It is critical that we have enforceable privacy, compliance and security in place to protect the ever-growing knowledge pool about every digital breath you take...

Appendix H - Is it time for the Scarecrow to visit the Wizard again?

Published on March 17, 2018

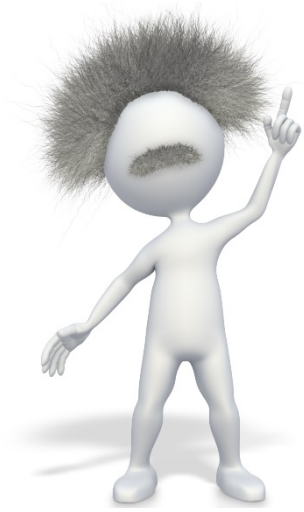
Professional discrimination and AI.

Following on from the evolving role of the professional (“The First Digital Evolution”), it is time to address the growing discrimination towards many of these professionals. There has been a gradual shift in the perception of what it means to be a professional.

In recent years, there has been an increase in job postings requiring mandatory qualifications such as a degree or professional qualification. These “qualifications” appear to have less to do with the ability to perform the work but are more to filter out resumes (C.V.'s). Add to this the obvious age discrimination that is apparent and it should raise a red flag. This blatant discrimination would be challenged if it targeted an easily identifiable 'protected class'. However, on more careful examination, it does indeed filter out people within many protected classes.

Whilst there are many positions that require the appropriate demonstrated training and qualifications such as doctors, nurses etc., the reality is that the use of ‘filters’ to cut down on resumes is, by its very nature, discriminatory.

Ironically in the field of academia, where the very qualifications are ‘born’, we see more and more ‘adjunct professors’ with no teaching qualifications running university courses. So, the unqualified teach to provide qualifications to discriminate against those without qualifications.



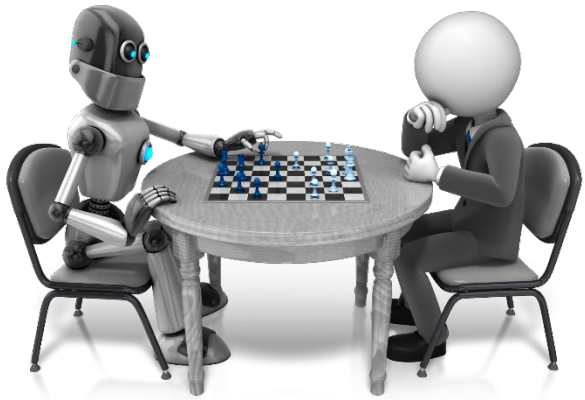
Has there ever been a successful Project Manager without a PMP or PRINCE2 qualification in your organization? Likely this is the case. Has there ever been an unsuccessful Project Manager with a PMP or PRINCE2 qualification? Can any large organization respond with anything other than an affirmative? So, the qualification does not preclude an ability to perform the role. Why then is it a mandatory requirement? The same can be argued for Post Graduate qualifications. Some of the most successful people on the planet do, in fact, “fall short” in their “qualifications”. The early resumes of Richard Branson, Larry Ellison, Mark Zuckerberg and more would be excluded by most hiring ‘AI’ algorithms along with many of their peers. Are you filtering out the next Bill Gates or Steve Jobs because of a discriminatory bias?

But surely discrimination must relate to a ‘protected class’? Not necessarily. This is where the focus on a clearly defined connection to ‘protected class’ is a blinkered view. The connection is socio-economic and demographic. There are two generally accepted paths to a career; one is educational involving post-secondary education, the other is experiential through the military, police, apprenticing or general hard dedicated work resulting in promotion through the ranks. Once you have taken the non-academic path, it can be hard to move back into the post-secondary route due to financial and time constraints.

Education is expensive and post-secondary education was and is not necessarily a path open to everyone. Looking at the demographics for post-secondary education over the years, it is disproportionally weighted in favour of or against certain socio-economic backgrounds. That socio-economic grouping can be further split by gender as women have been historically under-represented in academia, especially where socioeconomic factors have not provided the financial stability to provide them with opportunities for career advancement. Look deeper into demographics and patterns start to appear here too. This is because people of certain socio-economic and racial backgrounds tend to live in similar areas. Disabilities are also disproportionate to these socio-economic and demographic groupings. Add to this the acceptance

that the age groups in the Baby Boomer and Gen x category (Steve Jobs and Bill Gates fit here), did not have as many opportunities to obtain a purely academic path.

We can now see how these socio-economic and demographic groupings are unfairly discriminated by the filter of 'mandatory' (but not justifiable) paper 'qualifications' versus experience.



If you filter out potential candidates by socio-economic or demographic boundaries, you are unfairly impacting a large portion of these 'protected classes'. People should not be judged by sex, race or disability. Equally, they should not be pre-judged by an AI designed to filter out by socioeconomic group due to a bias on unnecessary filtering criteria. People are not too old or underqualified, they are either suitable or not suitable for the position. As AI tools continue to learn from this obvious bias, we will see an acceleration of this discrimination in the blink of an eye. To combat this, we now see people tweaking resumes that provide less and less information about the candidate and more focus on fooling the AI. This has even gone to the point of resumes with hidden (white on white) text containing keywords. In the past, anyone misrepresenting themselves on a resume would not only be fired but would be ostracized. Now we are effectively encouraging deceit to get past the electronic gatekeeper that is the recruitment AI.

Remember, as this discrimination progresses, you could find yourself with the wrong type of degree or professional qualification just as easily.

Make sure that next job description includes all the things that are truly required to do the job. This just might help to reduce the turnover of staff, costs and make for the success of projects.

Soon the perfect resume will be a single page with contact details and a large smiley emoji 😊. Underneath will be metadata filled with AI friendly keywords, the page filled with hidden white on white micro text. When did it become more important to lie to AI than to present who you truly are to an employer?

RESUME for AI Purposes

A person

123, Letsbe Avenue,

Newtown

Person view

RESUME for AI Purposes

A person

123, Letsbe Avenue

Newtown

AI view

Appendix I - The Einstein Puzzle REBOOTED

Published on June 26, 2018

How does a puzzle from the early 20th century impact GDPR, AI, Deep Learning, Forensic investigation and more? Read on and see. Then watch the accompanying video (Puzzle and Solution together). Be careful though as the solution is included. Click here for a stand alone video of the Puzzle and here for a stand alone video of the solution.

The following is a revisit to this puzzle allowing you to try again using ONLY YOUR MIND.

1. There are 5 houses in five different colors.
2. In each house lives a person with a different nationality.
3. These five owners drink a certain type of beverage, eat a certain food and keep a certain pet.
4. No owners have the same pet, eat the same food or drink the same beverage.

The question is: Who owns the horse?

Possible Nationalities

- Scottish
- Canadian
- American
- Swiss
- French

Possible House Colours

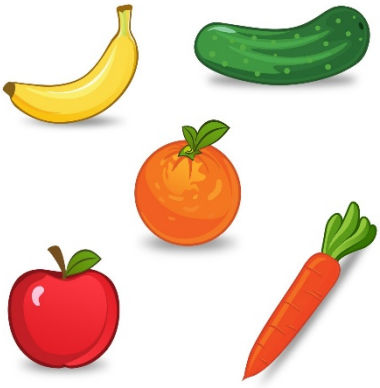
- Blue
- Green
- Purple
- Yellow
- Red

Possible Beverages

- Coffee
- Milk
- Tea
- Water
- Soda

Possible Food

- Apple
- Orange
- Banana
- Carrot
- Cucumber



Possible Pets

- Fish
- Dog
- Horse
- Cat
- Bird

Some hints were provided in the original so here they are updated;

1. the Scott lives in the blue house
2. the Swiss keeps a fish as a pet
3. the American drinks coffee
4. the yellow house is on the left of the purple house
5. the yellow house's owner drinks milk
6. the person who eats cucumber has a dog
7. the owner of the red house eats apple
8. the person living in the center house drinks tea
9. the Canadian lives in the first house
10. the person who eats banana lives next to the one who keeps a bird
11. the person who has a cat lives next to the person who eats an apple
12. the person who eats orange drinks water
13. the French person eats carrot
14. the Canadian lives next to the green house
15. the person who eats banana has a neighbour who drinks soda

Have fun and let me know how you do.