DTS DanTech Services
Computers under control!™

Technology Times July 2019 Issue

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

What's Inside:

All links in this Newsletter are safe and tested for viruses

Got IT Problem? - Click Here!

The Truth Doesn't Always Have to Hurt

By Greg Eisen

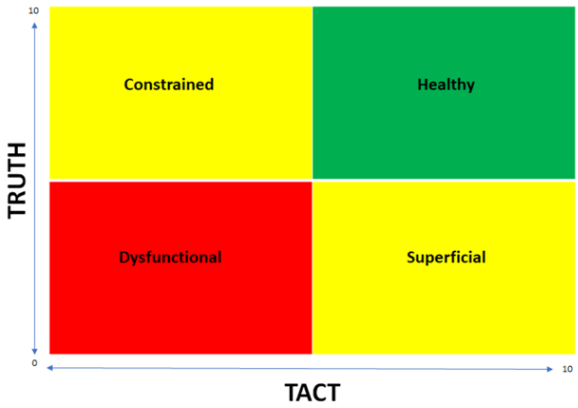
We've all heard the expressions. "The truth shall set you free" (John 8:32). "The truth is rarely pure and never simple" (Oscar Wilde). "The truth hurts" (everyone).

Unfortunately, accepting the truth is easier said than done. People tend to prefer justifying the daily mistruths rather than challenging them. Many simply avoid confrontation out of fear of making others uncomfortable or feeling uncomfortable themselves.

However, I'd like you to consider that the truth doesn't have to hurt. In fact, the truth may just be the competitive advantage your organization needs. Instead of simply accepting existing behavior, you can realize major gains by directly addressing the truth and building an organizational culture that does the same.

The Truth/Tact Matrix

Now, don't misunderstand me. I'm not suggesting you say whatever is on your mind without a filter. Tact is an essential component of telling the truth, one that requires practice, thoughtfulness, and restraint.



As an entrepreneur and business coach, I have observed that the quality of the relationships within and culture of an organization can often be judged by examining the intersection of truth and tact in that organization:

When relationships are high on truth but low on tact, they are constrained. People generally shut down when they are talked at instead of talked to, which limits trust and prevents open discussion. I see this situation often in circumstances where people know each other really well, get too comfortable, and fail to use tact. Despite their truthfulness, these interactions can cause company cultures and individual relationships to break down.

Relationships that are high on tact but low on truth are superficial. Consideration is shown and exchanges are cordial, but these interactions lack substance. These high tact/low truth environments put on a good show, but they are unable to thrive because deep care is missing. Real issues don't get resolved. I see this situation often in bureaucratic organizations where folks don't have any stake in the outcome, nor do they feel connected to a core purpose.

- Continued on Page 3

Is your organization Safe?
Lets get back to basics.

Online security is a massive problem in 2019 so making sure you are protected is a must.

Malware is defined as:

- any software intentionally designed to cause damage to a computer, server, client, or computer network.

Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software.

Request an Assessment

Click here to request Network Assessment and learn how we can make your technology worry-free!

Got more questions—check out our **Frequently Asked Questions Section**

If you have urgent IT problems or concerns -

Call us at 907-885-0500

Google Chrome Has Become Surveillance Software, It's Time to Switch

Chrome has become like spyware for Google, allowing more tracker cookies than any other browser. My tests of Chrome versus Firefox unearthed a personal data caper of absurd proportions.

By Geoffrey A. Fowler

You open your browser to look at the Web. Do you know who is looking back at you?

Over a recent week of Web surfing, I peered under the hood of Google Chrome and found it brought along a few thousand friends. Shopping, news and even government sites quietly tagged my browser to let ad and data companies ride shotgun while I clicked around the Web.

This was made possible by the Web's biggest snoop of all: Google. Seen from the inside, its Google Chrome browser looks a lot like surveillance software.

Lately I've been investigating the secret life of my data, running experiments to see what technology really is up to under the cover of privacy policies that nobody reads. It turns out, having the world's biggest advertising company make the most-popular Web browser was about as smart as letting kids run a candy shop. It made me decide to ditch Google Chrome for a new version of nonprofit Mozilla's Firefox, which has default privacy protections. Switching involved less inconvenience than you might imagine.

My tests of Google Chrome versus Mozilla Firefox unearthed a personal data caper of absurd proportions. In a week of Web surfing on my desktop, I discovered 11,189 requests for tracker "cookies" that Chrome would have ushered right onto my computer, but were automatically blocked by Firefox. These little files are the hooks that data firms, including Google itself, use to follow what websites you visit so they can build profiles of your interests, income and personality.

Chrome welcomed trackers even at websites you'd think would be private. I watched Aetna and the Federal Student Aid website set cookies for Facebook and Google. They surreptitiously told the data giants every time I pulled up the insurance and loan service's log-in pages.

And that's not the half of it.

Look in the upper right corner of your Chrome browser. See a picture or a name in the circle? If so, you're logged in to the browser, and Google might be tapping into your Web activity to target ads. Don't recall signing in? I didn't, either. Chrome recently started doing that automatically when you use Gmail.

Chrome is even sneakier on your phone. If you use Android, Chrome sends Google your location every time you conduct a search. (If you turn off location sharing it still sends your coordinates out, just with less accuracy.)

Firefox isn't perfect - it still defaults searches to Google and permits some other tracking. But it doesn't share browsing data with Mozilla, which isn't in the data-collection business. At a minimum, Web snooping can be annoying. Cookies are how a pair of pants you look at in one site end up following you around in ads elsewhere. More fundamentally, your Web history - like the color of your underpants - ain't nobody's business but your own. Letting anyone collect that data leaves it ripe for abuse by bullies, spies and hackers.

- Continued on Page 4

Dark Web ID Theft Protection & Monitoring Service is more important than ever!

The term "Deep Web" refers to all Web pages that that are unidentifiable by search engines. The "Dark Web," meanwhile, refers to sites with criminal intent or illegal content, and "trading" sites where users can purchase illicit goods or services. In other words, the Deep covers everything under the surface

that's still accessible with the right software, including the Dark Web. Knowing what is known about you personally that can be bought by criminals for nefarious purposes allows you to better protect yourself. Our tools tap into these hidden markets to find where your email address is found and, quite often, which breach of information leaked it.

DanTech Services new web-site **darkwebexposure.com** is now online and ready to provide you valuable information about data breaches that put your ID at risk. DTS clients will have the opportunity to get this same information directly from us, your support team. Because of the sensitive nature of this data, there will be restrictions in place to control its release.

Start Monitoring your Online ID Today!

"The Truth Doesn't Always Have to Hurt "
- Continued from page 1

When we are low on truth and low on tact we have dysfunction. Environments where we are not honest and direct and we are tactless in our interactions generally don't produce much success or fulfillment. These cultures are toxic, and turning these environments around requires significant change from the top down.

When we are high on truth and high on tact — where great trust and respect exist — we have healthy relationships and cultures. This is the zone you want to live in, both personally and professionally. I'd encourage you to use this matrix to score your most important relationships and your company culture as a whole. Where do you stand? What can you do to improve? I

f you want to take the first steps toward adding more truth and tact to your own leadership style, here are a few tools and tactics for doing so:

1. Coaching Like a Leader

Michael Bungay Stanier wrote a book, The Coaching Habit: Say Less, Ask More, and Change the Way You Lead Forever, about the benefits of utilizing coaching as a leadership style. Stanier's book covers the importance of asking the right questions and provides seven essential questions you can use to optimize communication and relationship development. I have personally found these questions essential to my communication with my own team.

2. Sharing Experiences vs. Giving Advice

If you're an Entrepreneur's Organization (EO) or Young Presidents' Organization (YPO) member, you are likely already familiar with this philosophy. Generally speaking, people don't like to receive advice. They do, however, love to hear stories about others' experiences. Instead of telling people what they should do, share something that has happened to you that is related to the situation at hand. This allows people to draw their own conclusions and learn their own lessons from your story.

3. Positive Before Negative

Studies show that although you may feel better when you get good news last, you are more motivated to do something about the bad news when you get the bad news last. Improved development and long-term results almost always trump instant gratification.

All of the tools I utilize in my business communications revolve around the tough and sometimes awkward task of telling the truth. However, if you can muster up enough courage to tell the truth to your employees, colleagues, family, and friends, you have taken the first big step toward improving your relationships for the better.

Shiny New Gadget

Of The Month

Ever wish **you could buy a 1TB microSD** card for your phones and various devices? Well, you're in luck.

SanDisk has launched one, in the form of a new Extreme card that's available to buy through its own store or on Amazon (when it's in stock). This card packs a lot of oomph, too, offering read speed up to 90MB/s and write speed of up to 60MB/s. It's capable of 4K Ultra HD and Full HD video recording and playback no less, and meets proper UHS Speed Class 3 for 4K UHD standards.

The primary caveat, of course, is the price. This 1TB card currently costs $450 on Amazon US (£454 on Amazon UK) - effectively double the cost of the 512GB card, but you are getting twice the storage amount. Its price may go down eventually, but probably not for months or even a year.

So, if you think your Android phone or other gadgets don't have enough room, this is the beast to get. The best part is SanDisk's new 1TB microSD card is water proof, shock proof, and X-ray proof. It can also withstand extreme temperatures. What's not to love about that?

Google Chrome Has Become Surveillance Software, It's Time to Switch
—Continued from Page 2

Google's product managers told me in an interview that Chrome prioritises privacy choices and controls, and they're working on new ones for cookies. But they also said they have to get the right balance with a "healthy Web ecosystem" (read: ad business).

Firefox's product managers told me they don't see privacy as an "option" relegated to controls. They've launched a war on surveillance, starting this month with "enhanced tracking protection" that blocks nosy cookies by default on new Firefox installations. But to succeed, first Firefox has to convince people to care enough to overcome the inertia of switching.

It's a tale of two browsers - and the diverging interests of the companies that make them. A decade ago, Chrome and Firefox were taking on Microsoft's lumbering giant Internet Explorer. The upstart Chrome solved real problems for consumers, making the Web safer and faster. Today it dominates more than half the market. Lately, however, many of us have realized that our privacy is also a major concern on the Web - and Chrome's interests no longer always seem aligned with our own.

That's most visible in the fight over cookies. These code snippets can do some helpful things, like remembering the contents of your shopping cart. But now many cookies belong to data companies, which use them to tag your browser so they can follow your path like crumbs in the proverbial forest. They're everywhere - one study found third-party tracking cookies on 92 percent of websites. The Washington Post website has about 40 tracker cookies, average for a news site, which the company said in a statement are used to deliver better-targeted ads and track ad performance. You'll also find them on sites without ads: Both Aetna and the FSA service said the cookies on their sites help measure their own external marketing campaigns.

The blame for this mess belongs to the entire advertising, publishing and tech industries. But what responsibility does a browser have in protecting us from code that isn't doing much more than spying?

In 2015, Mozilla debuted a version of Firefox that included anti-tracking tech, turned on only in its "private" browsing mode. After years of testing and tweaking, that's what it activated this month on all websites. This isn't about blocking ads - those still come through. Rather, Firefox is parsing cookies to decide which ones to keep for critical site functions and which ones to block for spying.

Apple's Safari browser, used on iPhones, also began applying "intelligent tracking protection" to cookies in 2017, using an algorithm to decide which ones were bad.

Chrome, so far, remains open to all cookies by default. Last month, Google announced a new effort to force third-party cookies to better self-identify, and said we can expect new controls for them after it rolls out. But it wouldn't offer a timeline or say whether it would default to stopping trackers. I'm not holding my breath. Google itself, through its Doubleclick and other ad businesses, is the No. 1 cookie maker - the Mrs. Fields of the Web. It's hard to imagine Chrome ever cutting off Google's moneymaker.

"Cookies play a role in user privacy, but a narrow focus on cookies obscures the broader privacy discussion because it's just one way in which users can be tracked across sites," said Ben Galbraith, Chrome's director of product management. "This is a complex problem, and simple, blunt cookie blocking solutions force tracking into more opaque practices." There are other tracking techniques - and the privacy arms race will get harder. But saying things are too complicated is also a way of not doing anything.

Please click HERE to complete reading this article