katzscan®

Enterprise Resource Planning (ERP) / Electronic Data Interchange (EDI)
Supply Chain Vendor Compliance
Internal Controls / Fraud Detection & Reduction
Business Analysis / Data Analysis / Systems Analysis

Since January 1996

Retailers are facing fraud head-on.

For those of you – like me – who are old enough to remember the show and the tag line, "Smile, you're on Candid Camera", the next time you walk in to a retail store you may want to do the opposite instead.

According to a McClatchy DC article in the May 28, 2018 Miami Herald newspaper, retailers are facing down shoplifting fraud by implementing facial recognition technology into their camera systems. By scanning the faces of people entering their stores and matching to databases of convicted or admitted shoplifters, retailers are seeking to block entry of nefarious persons into their brick-and-mortar establishments.

Well … at least online shopping is an option for these fraudsters.

Such facial recognition technology – which relies on proper lighting and superior camera resolution – is impressive. Within the first two steps of someone entering a retail establishment – in less than one second – a face in a crowd can be scanned and matched against a database of 25 million entries.

But what if errors or glitches occur? What if an innocent person is targeted and tagged as a shoplifter and excluded from entry to a store? The liabilities against the retailer for such a mistake can be considerable. Liabilities include not just the money won in a lawsuit but the company's reputation when this is exposed to the public. And companies – retailers – are not required – there is no law necessitating – that facial recognition scanning signage alerting customers to the use of this technology be posted. Stores can deploy and use this technology without the consent and permission of any of us. And the technology accuracy varies based on skin color and gender.

Retailers are desperate for anti-theft solutions. The nation's 3.8 million stores suffered $48.9 billion dollars' worth of losses in 2016. On the average, a store will suffer between 1 and 3 percent of revenue loss to theft annually.

However, once the theft type is analyzed, shoplifting theft is believed to be responsible for less than half of the above numbers, with more losses coming from employees typically at the checkout counter. Still, with the annual loss numbers so significant, reducing the shoplifting portion would be a significant achievement for retailers.

But how else could this technology be used … or abused? Could faces be shared among retailers in the same way that sales data is shared today by companies that monetize their customer information? Could a company one day sell their facial scans to a marketing company that would compare these scans to those of another company to determine these people's shopping habits, and then try and identify these people through social media sites like Facebook and LinkedIn, after which they would send targeted advertising messages?

(Hey – looks like I just created a not-so-futuristic business model if anyone is interested!)

[SIDEBAR: Amazon – the powerfully potent online (and now intrusively brick-and-mortar) retailer has a nifty little piece of software developed by its Amazon Web Services (AWS) group called Rekognition. (AWS' $5.4B Q1 2018 revenue make up for the majority of Amazon's overall profits.) Rekognition will not only recognize up to 100 faces in a crowd at a time, but also discern the emotional state of each person based on the face's characteristic (cheeks, lips, eyes) attributes (e.g. slant, opening). So, not only is there facial recognition software, but emotional state recognition software. Forget about walking in to work with a sour puss on your face because you had a bad commute or are a disgruntled employee due to something beyond your control: Big Brother may very well be monitoring and keeping a checklist of your behavior … possibly for your next performance review.]

The article does point out that inasmuch as the technology is in use today by some retailers, there are legal and ethical considerations that are already being thought out. How secure are these facial databases from hacking? I am one of those people who would never give up his DNA to a commercial company for testing. That my facial features are in various commercial company's databases is uncomfortable enough. I am all for fighting fraud, but there has to be less personally intrusive ways to do so than such wide net casting.

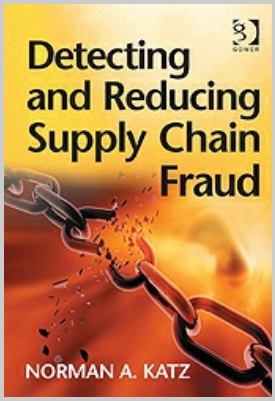
Thanks for reading.

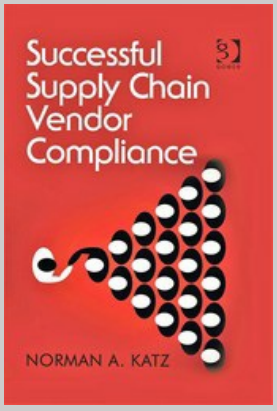
Interested in either of my two books?

Contact me for an author discount code before ordering from my publisher.

Both book titles make for engaging conference and event speaking topics.

Contact me to speak at your next conference or event.





Both books are the first titles on record on

their respective topics!

Norman Katz
Lean Six Sigma Black Belt
Certified Fraud Examiner
Certified Controls Specialist
Microsoft Office Specialist
Katzscan Inc.
954-942-4141
http://www.katzscan.com

Executive Advisor
Data Analyst
Operations Specialist
Project Leader
Software Expert
Supply Chain Authority