Communications, Technology, and Management (CTM)

# February 2020 - Communications, Information, Technology, and Management

## THE EDITOR SPEAKS - Ecosystems Must Be Designed and Managed

As a general statement, the business climate has moved away from the conglomerate business model where one organization manages the entire business process to a model based on ecosystems where clusters of companies work together to achieve the desired result.  The ecosystem model allows each organization to focus their attention on a part of the problem thereby allowing them to become specialists on a very specific aspect of the value chain.  Members of the ecosystem community are then free to come together to bring their collective talents to bear on an issue that may exceed the scope of any individual member.  Further, the way these companies work together is adaptable allowing the collective organizational structure to reflect the needs of each unique opportunity.  The open innovation movement reflects an ecosystem based approach to finding solutions for complex problems that require innovative solution development.

There should be no debate that communities (or ecosystems) that work together can achieve much more than individual organizations.  However, the process by which these communities are constructed is often underappreciated.  The effort required to construct a working ecosystem that can survive and thrive is significant.  The value of the ecosystem is based on the composite value of the participants and as a result, the larger the ecosystem the greater the collective value of the participants.  However, at the same time, the larger the ecosystem, the greater the potential for conflict and such conflicts have the potential to bring down any ecosystem – no matter how large.

As ecosystems grow, they will inevitably include competitive organizations within their community.  As members of the community succeed, they will expand into areas where they compete with each other.  As new members join the community, they may find they compete partially or completely with other members of the community.  Since it is impossible for members of a common ecosystem to be assured that future competitors will not appear within their ecosystem, they may even conduct themselves as though there is a competitive threat even when one has yet to materialize.

In theory, each member of the ecosystem must be focused on their unique skill set and should be self-assured in the knowledge that their talents are understood and valued by the other participants.  Ecosystems often fail if the communications structure within the ecosystem fails to allow the participants to interact with one another in a way that allows the community members an equal opportunity to promote themselves.

Pursuit of opportunities by the ecosystem requires that members of the community work with one another toward a common goal.  In our data driven world, such coordination requires that the members exchange data with one each other about the opportunity, the collective solution being pursued, and progress during the development, deployment, and support processes.  If the community members are fearful of the potential competitive threat represented by the other community members, information will not flow and as a result the potential for success can be completely undermined.

The adaptive nature of a properly structured ecosystem is remarkable.  Different ecosystem members fluidly come together to translate a perplexing problem into a valuable opportunity for growth.  New participants can join (or leave) the solution team as a better understanding of the nature of the problem is gained.  However, in ecosystems where these relationships are controlled or managed from outside forces, partners with components that might be a part of the optimal solutions can be dismissed or suppressed which will cripple the end-result.

Yes, ecosystems can achieve wondrous things but a successful ecosystem must be carefully crafted.  It cannot simply emerge organically based on a common desire.  Too much or too little governance can turn a promising venture into an empty shell.  Ecosystem must be properly managed and driven by both its member companies and the customers it intends to support.  Do not underestimate the amount of energy required and constantly reinforce the message that while the potential for the ecosystem might be great, their individual outcomes are proportional to the energy they put into the community.

## UPCOMING EVENTS

- **Feb 24-27, 2020**, Mobile World Congress, Barcelona, Spain
- **Feb 24-28, 2020** RSA Conference, Moscone Center, San Francisco, CA
- **March 13-22, 2020,** South-by-Southwest, Austin TX
- **March 17. 2020**, Future Festival, Landmark Theater. Los Angeles, CA
- **March 23, 2020.**  I3 Working Meeting, USC, Los Angeles CA
- **March 23-27, 2020**, Business Transformation and Operational Excellence Summit, Orlando, FL
- **March 28-29, 2020.**  USC IoT Hackathon, USC Campus, Los Angeles CA
- **March 28-31, 2020,** Horasis Global Meeting, Cascais Portugal
- **June 5-6, 2020**, International Conference on Smart-Cities, Transportation, and Buildings, San Francisco, CA

*If you have an event that you would like us to include in our newsletter, please send an email to manager@i3-iot.net*

## NOTES OF INTEREST: I3 Systems Inc

In December 2019, USC released version 1.0 of the I3 software as opensource.  The I3 software acts as a data stream management system that is especially useful when a community of independent data users wish to utilize IOT data or enriched data streams to work on problems/applications together.  The I3 software (1) facilitates data governance between and across organizational boundaries, (2) provides incentive and trust management facilities, and (3) creates a vendor neutral flex point that is important to manage evolving IoT based data networks.  The software, the SDK, and documentation can be found at the following repositories: https://github.com/ANRGUSC/I3-Core, https://github.com/ANRGUSC/I3-SDK, https://i3admin.readthedocs.io/en/latest/, and https://i3user.readthedocs.io/en/latest/.

With this, the first public release of the I3 software, I3 enters a new stage where it shifts from being a research/development effort to a program that will provide operational support services for users who require such services.  To address this need, we have created a new company, I3 Systems Inc, which will serve the needs of those building next generation IoT networks.  While I3 Systems can tackle company specific issues, part of the company's mission will be to drive incremental research/development projects of interest to the larger I3 community back to the universities.  Please feel free to reach out to us at manager@i3-iot.net if you wish to talk about your specific needs or if you are interested in participating in the early funding process

## NOTES OF INTEREST: March IoT Hackathon

An IoT specific Hackathon is being planned for the weekend of March 28 and 29 on the USC Campus.  Interested parties can apply to participate as an individual or as a member of a team.  While the event is targeted to USC students, others can apply and will be considered as space permits.  Tools, equipment, and workshops will be provided for IoT novices.  To apply goto https://docs.google.com/forms/d/e/1FAIpQLSeUou9xS4VvRfsKswK2O1gQAKf8_X2YpQspDM2jr1WzGLQx6g/viewform.

If your company/organization is interested in participating in the event, ieee@usc.edu is looking for sponsors who will help with food, prizes, or providing hardware that might be incorporated into the projects.  This is a great way for a company to raise its visibility among the student-engineers that will be shaping the IoT industry of tomorrow.

## READER CONTRIBUTION: Residential IoT : The Brand Entropy
## by by Jerome Baccelli, Chief Technology Officer at ShareTracker

Jerome is a Telecom engineering executive with a successful record in multiple segments of the mobile telephony industry, gaining expertise in both startups and Fortune 100 companies, such as Orange, Vodafone, Verizon Wireless, Cisco Systems and the Nielsen Company. He has managed large teams and multi-year long projects, invented and successfully implemented many innovative performance measurement methods for telecom analytics.

**Introduction**

Back in 2016, some of our US Fortune 500 customers asked us to quantify the IoT growth. As a company whose mission for the past 18 years has been to measure trends for pretty much everything in the telecom industry, it seemed like a natural ask. We have been measuring the Internet of Things for over eight quarters now, and wanted to share with you some of the fascinating findings we made by looking at over 45 Million devices spread over 3500 brands and over 100 device families across the United States.

**How should we measure IoT ?**

A lot of quantitative market research on IoT today comes from surveys. But this methodology is proving to be increasingly inadequate for measuring an industry that happens to be the most diverse in history: how can a five question survey cover thousands of brands and over a hundred different device types, some of them maybe created as you are reading this paragraph? It seems impossible, and it is.

Another way of following IoT trends has been to count device shipments from electronic retail stores. However, when an increasing 50% of electronics are purchased online by consumers, this approach is unfortunately missing half of the picture, and notably almost all the enterprise segment, whose devices are very rarely purchased in retail stores.

Finally, Internet and mobile app data (the famous Big Data) is not of help in this case either : contrarily to its name, Internet of Things never sees the Internet, and if mobile IoT applications can reveal the controller side of smart home ( smart things, Alexa, Google etc.) they do not provide enough end device granularity.

One common denominator that almost all IoT residential devices share is their wireless, Wi-Fi connectivity (some sensors use Zigbee or other wireless protocol, however due to the economy of scale of wi-fi adapters their relative presence in the residential IoT population has shown to slowly decrease ). That’s how the ShareTracker WIoT reporting product was designed. ShareTracker WIoT drives through residential areas in major cities, captures millions of anonymized Wi-Fi signal with enhanced device information, processes it through more than 100,000 custom mapping rules and quantifies the findings from one period to the next, from one market to the next, from one type of devices to the next, from one brand to the next. But before diving into the findings, let’s organize things a little in the Internet of Things.

**Organizing Things in Internet of Things**

The name IoT covers very different meaning depending on who is talking in the industry, so we see the need to provide a quick taxonomy to the plethora of devices deployed in US homes.

- For instance, routers, access points and modems seem to belong to the same category - providing access to the end devices.
- Another natural segment is the population of “old screens” : PCs, tablets, cell phones, which remains relatively stable in size compared to the other ones, and can serve as a useful referential to measure growth.
- Even though we are focusing more on residential IoT in this paper, we also define an enterprise segment that splits itself in multiple sub categories.
- Looking closer into the residential IoT comes the video segment, split itself between smart TVs, streaming devices and other video display devices. We also see an audio segment, made of speakers, headsets etc.
- Gaming has its own segment, so do office peripherals such as a printer or a wireless mouse.
- Security is separate as well, split between cameras, door bells and other detectors.
- Looking into what we call the Smart Home segment, WIoT defines the following subcategories : smart speaker or digitally triggered controller, wireless appliances such as refrigerator or cleaning robot, baby monitoring and toy devices, wireless furniture, smart plugs and smart lights, exercise and health/medical equipment, smart thermostats and weather stations, water control.
- More granularity is always achievable, if for instance there is a need to dive down into the solar installation trends, like we will do in a moment.

**First Findings: Quantifying the IoT Growth**

A lot in market research is about confirming with data what common sense and intuition tell us: we do indeed see all IoT segments grow in total, except maybe the “traditional screens” which have reached a plateau and a form of saturation. Here are 4 general findings from the past two years:

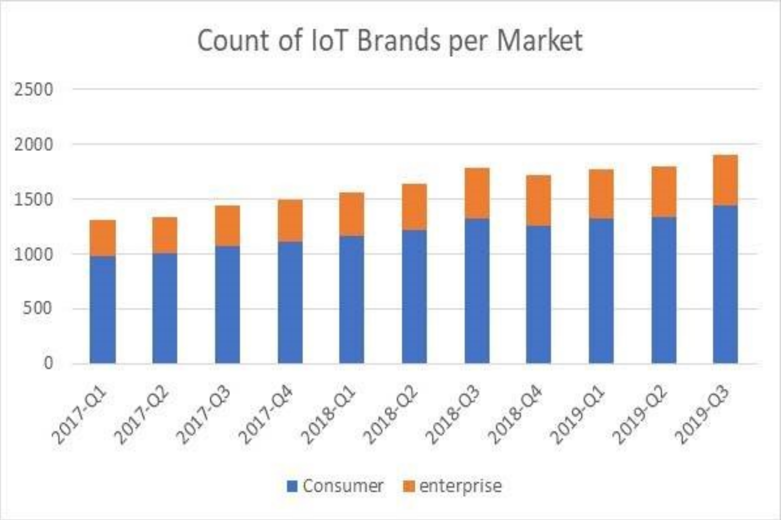
- An increase in residential access points by 20%, due to the expansion of meshed networks in residences (think Google Wi-Fi)
- A Video streaming devices and smart TVs increase of 50%
- The automotive, audio, enterprise, gaming, home security, device segments each doubled in volume.
- The smart home segment has seen a 5 time increase in volume.

At a market and socio demographic level, here are also 4 key findings:

- First, even at a time where most electronics purchases are done online, a brand will generally see a higher penetration in the surroundings of its headquarters: a good example is the Santa Barbara based Sonos, well deployed in Northern California. Also, confirming common sense thinking and in line with the state funded rebates, a climate dependent segment like solar is mainly deployed in California, and almost 3 times more present in San Diego than in San Francisco
- Some segments appear income and demographic agnostic, such as video, home security, or even smart speakers. Some others, like appliances or smart plugs and switches are more present within a younger and high-income population.
- Interestingly, the IoT adoption appears less dependent on the income level than on the available space. In other terms, the larger the median price house, the more smart home devices in the house. A good example is the small but very fast increasing cleaning robot population (Ecovacs, Euffy, Roborock mainly): its share is the highest in Atlanta and Dallas, and the lowest in Philadelphia.
- More and more brands are launching IoT products, with more or less success. We are going to look further into that in the next section.

**The concept of brand diversity**

Counting devices within a segment tells a good part of the story, but not all of it. Looking at the number of main brands that dominate a vertical enables also to measure its fragmentation, its diversity and maturity

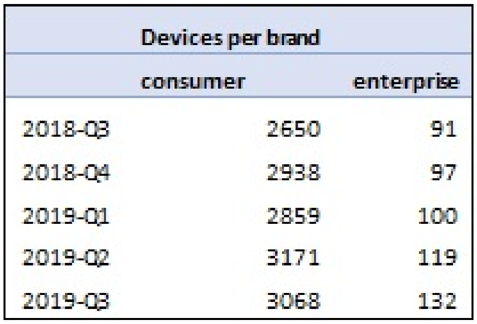


ShareTracker identified 1300 IoT brands in early 2017, against almost 2000 in October 2019. The 5% steadily increase in brands every quarter, a 38% uptake in two years, illustrates the speed at which companies are entering the ecosystem: steady, but not extreme. Note that a brand can be counted multiple times if it appears in multiple device families : for instance, Samsung who makes cell phones, tablets, smart appliances, security cameras, smart plugs and switches, smart TVs and video streaming devices, audio speakers and automotive media players, printers and access points among other device families, is counted many times.

The first overall observation comes from looking at business versus home: As seen in the chart below, there are on average 3 consumer brands for 1 enterprise brand.

However, one average there are 9 times less devices per brand in the enterprise vertical than in the consumer vertical, illustrating a highly fragmented enterprise IoT eco system, with a lot of specialized tools.

Now, we still see a brand consolidation in both the consumer and in the enterprise verticals over time: almost every quarter, the average count of devices per brand increases, by over 10% in enterprises, and at a slower, sometimes negative rate in consumers.

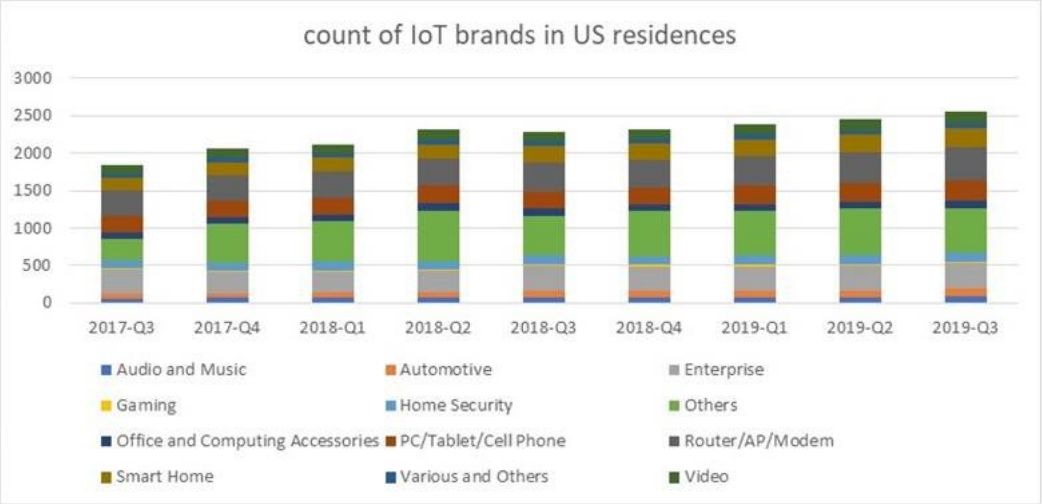


| Devices per brand | | |
|---|---|---|
| | consumer | enterprise |
| 2018-Q3 | 2650 | 91 |
| 2018-Q4 | 2938 | 97 |
| 2019-Q1 | 2859 | 100 |
| 2019-Q2 | 3171 | 119 |
| 2019-Q3 | 3068 | 132 |

**Brand diversity in residential IoT**

Depending on the IoT residential segments, the brand growth varies drastically over time:

- The category of traditional screens went up from 221 to 282 within two years
- The router/access point/modem category went up from 342 brands to 433
- Video streaming brands went from 118 to 149
- And the Smart Home segment went up from 162 to 261 brands in two years.



Now, when looking at the brand diversity we can see that routers and modems count over 5000 devices per brand, followed by the traditional screens, and then the PC accessories. In each case, a few brands dominate the segments.

At the bottom of the chart is a very fragmented enterprise vertical, with lots of brands specializing in networking, network security, telephony, video conferencing, optical fiber, electrical, lighting, fleet location, industrial machinery, medical, military, packaging, robotic, point of service, smart city, water control, testing… and an average of 132 devices by identified brand in this past quarter.

The graph also shows which segments are fragmenting (declining line) and which are consolidating (increasing line).

**Other notable findings**

A further analysis shows a gradual consolidation of video streaming and smart TVs, as well as the appearance of a consolidation of smart home devices, mainly due to the overwhelming spread of smart speakers from mainly two brands (Amazon and Google). But once these are taken out of the analysis, we see a strong brand fragmentation for almost all sub families of the smart home segment, the highest being electrical and lighting (smart plugs and smart switches).

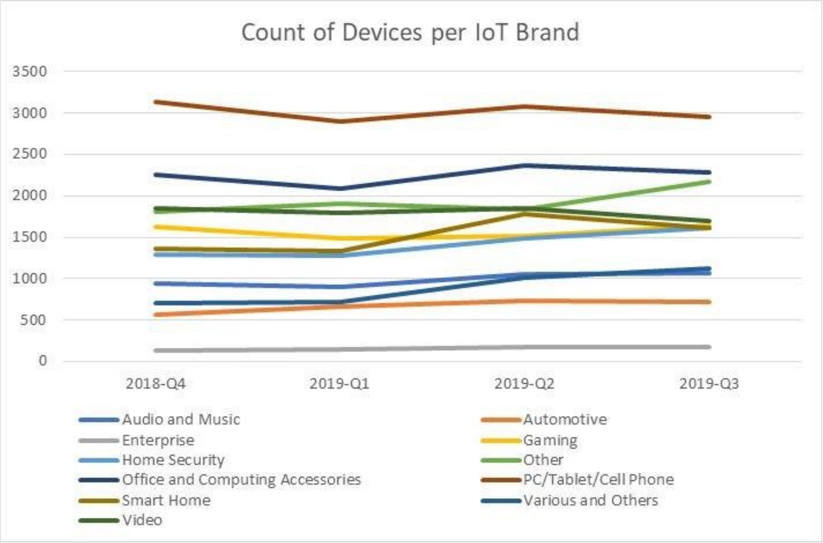
Finally, IoT has always been the theater of a crucial battle for the control of the house, first dominated by smart thermostats (Ademco, Honeywell then Nest…), then by digital controllers (Samsung being a major player). The battle seems to be now in favor of the low cost, sometimes free, smart speakers Google and Amazon (with very little competition so far).

**Conclusion**

The findings mentioned in this paper show that IoT is an extremely fragmented eco system within enterprises, and relatively fragmented within consumers, with most segments dominated by a handful of brands followed by a long tail of smaller players. Brand consolidation varies greatly from one segment to another. One battle to pay a lot of attention to is the control of the house, increasingly in the hands of Google and Amazon.

WIoT data enables to quantify intuitive facts about the IoT growth and provides new insights that had otherwise been difficult to identify. In addition to measuring IoT growth in both consumer and enterprise verticals, this type of data-driven research enables to drill down into a specific segment, or a specific brand, and to link device volumes with brands.  Correlations between brands, device families, markets, socio demographic profiles can be easily made by linking the data within WIoT. For more information, please feel to contact Jerome Baccelli, Chief Technology Officer at ShareTracker (jbaccelli@sharetracker.net)

.



### THE $I^3$ CORNER (I3.usc.edu)

On January 21, 2020, The I3 Consortium held another event in its series of IoT Conferences/Workshops that focused on defining and serving the next generation of Smart Cities and IoT driven data networks in general. Presentations from the County of Los Angeles, the City of Los Angeles, and the City of Long Beach provided a framework that shaped the proceedings of the entire day.  (Many thanks to Bill Kehoe, Miguel Sangalang, and Ryan Kurtzman).

Interestingly, while not planned as a formal theme of the event, similar messages continued to reoccur throughout the day.

- The common practice is to look at IoT devices as data generators where the data is destined to drive a specific application.  While such linear thinking reduces process complexity, it results in a compartmentalized network architecture that is not efficient.  Efforts like I3 represent a necessary shift in philosophy as we begin to build next generation information networks.
- CIOs and IT departments as a whole are evolving from acting as operations driven cost centers which are tasked with keeping our networks running to becoming the strategic center of an organization’s entire enterprise.  The network architecture serves as either a innovation accelerator or an inhibitor and this change is requiring that IT departments become much more strategic in the way they perform.
- As IT departments (and other tech related departments) become more strategic. they also have to become more agile.  Improvements in the platform and tool space create the opportunity for these departments to become more agile, however, if one department attempts to increase its agility inside a staid organizational structure, potential gains can be easily suppressed.  The efforts of a tech-centric department to evolve to meet the challenges of a fast pasted world have to be linked to a larger cultural change that cuts across the entire organization before results can be maximized.

In the future, true smart cities will no longer look at data as a consumable resource but will adopt the perspective that data is one of the key strategic assets that provide the foundation upon which any smart enterprise is built.  As an asset, the IT department must focus on maximizing the returns the organization is able to drive from their assets.  In the case of a smart city, a return can take the form of improving citizen satisfaction (the customer experience), operational efficiencies, or by increasing the externally generated revenue base.

This evolved organizational structure represents a significant cultural shift in the design of operational networks. Cities must move away from building networks a series of application silos that share a common communications system to become an organization that builds a data infrastructure that provides managed access to data when and where it is needed.  Such a shift requires that even the definition of infrastructure must change from being an end-to-end bit delivery system to becoming a much more complete information management system.

Changing an organization’s information/technology culture is no small feat, in fact such cultural changes are often the most difficult challenges people face in their career.  However, the benefits of these activities must not be ignored.  Besides the immediate and strategic benefits for our internal and external customers, such a change makes it much easier and faster to develop and deploy applications because a significant portion of the applications data management function has become incorporated into the infrastructure that supports the entire organization.  Arguably, the recent regulatory movements such as GDPR and CCPA all but force an organization create a common data management infrastructure layer that provides the organization with a common system that is necessary to ensure compliance across an entire organization.

At the I3 January event, while all the presentations covered issues related to enabling this next generation of information-centric managed networks, the County and City of Los Angeles along with the City of Long Beach, all talked about their efforts to evolve the IT cultures within a city, to change the way the city itself thinks about information and data as a whole, and to change government so that it is better able to meet the needs of citizens that continue to become more data savvy.  It was especially gratifying to hear these tech leaders in the government sector talk about the citizens they serve as customers that have the expectations for government shaped by their networked interactions outside the government sector - not by their legacy experiences with traditional bureaucratic systems.

Let’s all offer USC’s Viterbi School of Engineering a virtual round of applause for making the version 1.0 of the I3 IoT opensource software publically available via GitHub.  The software was officially released on December 19, 2019 and can be downloaded from https://github.com/ANRGUSC/I3-core.  This is a momentous event as the I3 software would not have been realized without the efforts of the entire I3 Community.  All involved provided the ideas, suggestions, and the support that was needed to create the first release of an I3 node.  This system will eventually evolve to support a large scale IoT driven data network.  With the accolades and words of appreciation behind us, now let’s all dig in and begin work on release 2.0.

### The Illusion of PII (Personally Identifiable Information)

It is clear that malicious behavior in cyberspace is on the rise.  Fortunately, corporate efforts to combat these trends have increased, and legal/regulatory issues are receiving increased attention.   This is all well and good.  While the framers of some regulations and industry guide lines attempted to provide a framework that allows a clear line to be drawn between sufficient and insufficient privacy measures, by explicitly defining Personally Identifiable Information (PII), technologies cannot rely on these definitions as a legal shield.

Privacy legislation generally provides the position that people should be able to control the information about themselves.  If a company receives information from someone, that person should be able to determine what the company is authorized to do with the data as a condition of their obtaining the data.  On the surface, this principal seems relatively straight forward.   Personal information often contains data about its source (the identity of the person who supplied the data).  Logically, if the company strips away all identifying information that links the data to a person, the data could be treated as being anonymized.  The definition of PII varies widely depending on the statue.  A potential composite definition of PII based a several laws and industry guidelines might include an individual’s first and last name (also maiden names), street address, email address, a telephone number, a Social Security number, credit-card/banking information, Userid, passwords, or any other information that permits a specific individual to be contacted physically or online. The term often includes sensitive details such as a race/ethnicity, politics, relation, philosophies, trade union membership, genetic information, biometric access information, health, weight, marital status, sexual orientation, dependent or family information, person’s birthday, employer, passport, patient ID,  MAC or IMEI identifiers, vehicle or other asset identifiers, license numbers, photographs, education, height, weight and hair color.

While an organization might attempt to argue that hair color should not be included in a definition of PII, it is important to understand that if a person is the only person with red hair that lives within a block of town square, the hair color is indeed PII because when it is used in conjunction with neighborhood data, it allows a specific person to be identified.

The company may not have even collected data about the neighborhood where the person lives but if there is a data breach and a third party can combine the company's hair color data with data from a third party to identify a person, then by extension hair color is indeed PII.

To truly understand the nuances of PII, the data does not actually have to allow identification of a specific individual. If the company's data, when combined with other data, allows a sufficiently small pool of potential individuals to be identified so as to allow someone to 'guess' someone's identity, then that data too is considered as PII.

Being fair, most of the regulations dealing with PII were originally written many years ago when the technologies available to us were not as advanced as the tools that are readily available today. When written, it was inconceivable that a common hacker could easily combine multiple data sources and conduct the statistical analysis required to identify individuals within a large data set that has masked key values. Researchers have demonstrated that given commonly available technology, individuals can be identified by triangulating on the individual with a surprisingly small amount of supposedly anonymized data.

As technologists, this means we cannot assume that by simply masking out key data elements identified in some legal statute we have protected ourselves in a court of law or that we have protected our customers (and our company) from embarrassment. The available laws and industry standards provide a starting point for a much deeper conversation. Each company must analyze the data they are holding and consider any of that data can be cross-linked with other data by a third party to cause harm to the company or its customers. The true definition of PII will always be as unique to the company as the data it holds. Of course, the safest thing is to assume all data received from a customer is PII and therefore permission must be sought and received before any data can be utilized.

If this topic is of interest to you, you might want to check out "Researchers: Anonymized Data Does Little to Protect User Privacy" or "Anonymized Data is not Anonymous"

### READINGS FROM THE EDITOR'S DESK

- **Innovation without integration** New products can be brought to market based on an assimilation model where the product is fit into an existing operational model or alternatively based on an errant model where it envisions a more forward-looking operations model will emerge.
- **Agile software development is dead. Deal with it** Agile developments are useful when applied properly for appropriate problems but the process does not scale and is difficult to sustain. The same is true for business plans - a plan that constantly pivots without a true north fails to produce results.
- **Don't be fooled: Blockchains are not miracle security solutions** Blockchain is a cool technology but the distributed control features come at the expense of performance. This is a good trade-off in a low trust environment but it does not eliminate the need for an organization to build trust within its community.
- **How to avoid the mistakes made in the UN data breach** The July-2019 UN data breach exposed shortcomings in their cyber defense plans. Awareness of such attacks serve as educational opportunities for all and point to the importance of making cybersecurity part of an organization's core culture.
- **Digital Transformation And The Danger Of Leading With Efficiency** KFC pursued a digital transformation program designed to impact the customer experience. Results show customer driven transformation projects have better results than efficiency driven projects - the customer must be the driver.
- **How three wireless technologies will soon ignite the edge computing revolution.** 5G & WiFi6 will bring big benefits, especially when coupled to AI, big-data, and IOT. Some suggest the benefits are overhyped. The truth is that the benefits are understated if anything BUT the complexity and time needed to reap the benefits is not trivial.
- **ROI in cybersecurity.** Investments in cybersecurity have to be justified by a positive business ROI. ROI has to consider probability of an attack and the cost of the attack. Cost comes from 1) impact to ongoing business, 2) , impact to current customers, & 3) impact to brand.

### LET's CONTINUE THE CONVERSATION

Please feel free to forward this email to your friends and colleagues who you believe would benefit from participation in our community. For those of you who wish to be included among those who believe that technology is a tool and that business success is achieved by skilled wielding of the tools available to us, feel free to reach out to us. If you have suggestions, topics you want to see included in future newsletter updates, or other general inquiries, feel free to email me at manager@i3-iot.net.

The ideas expressed in this newsletter are intended to stimulate conversation and dialog that will lead to a better understanding of our collective future. The opinions may not necessarily reflect the opinions of any other member of our community of interested people.

## ABOUT CTM

*Originally founded in 1985 under the guidance of USC, the Institute for Communication Technology and Management (CTM) was originally formed to support the newly deregulated US telecom industry. Over time, the telecom industry evolved from being a voice focused service to become a backbone element of the internet. As the internet grew and shifted from being a digital exchange network to become a consumer focused social/media distribution system, CTM grew to include entertainment and network companies both domestically and abroad interested in serving these expanding network need. These efforts to understand and embrace transformational disruption led to the emergence of The CTM Newsletter, a vehicle to foster continued conversation about transformational issues that transcend specific technologies and specific industries. In time, CTM conducted some foundational research in the blossoming Internet-of-Things arena and this led to the creation of a community driven IoT network vision. Working with the engineers at USC's Viterbi School of Engineering, the cities of Long Beach, Los Angeles, the County of Los Angeles, and a host of supporting companies, academic institutions, and private individuals, this vision was turned into a opensource software development project that resulted in the public release of the I3 software in December 2019. Operational management of the I3 program was spun out of USC in 2020 as the I3 Consortium to allow the university to focus on needed research programs while the consortium works to support the operational needs of the I3 community.*