Communications, Information, Technology, and Management (CiTM)

**April 2021**

## THE EDITOR SPEAKS - A May Rebirth?

This year, May Day and in fact, the entire month of May has a special significance given the challenges of the prior year. May Day traditionally represents a celebration of spring and rebirth. Maypole dancing and song often mark festivities that can be traced back to Roman times. May is also the time for finals and graduation where students mark their accomplishments and move on to a new stage in their lifes' journey. May includes Mother's day, a time to show appreciation to those who brought life into this world and put up with the many youthful indiscretions of their children . But this May is special. It is distinctly different in that it marks the transition from a period when human behavior was controlled by the COVID-19 virus to one where the actions of everyone in the community determine the future impact of the virus.

This is not to say the virus has been vanquished or that society can now revert to pre-pandemic behaviors. But May does feel like a momentous turning point. Prior to May, the prevalence and ferocity of the virus drove the population to social distancing, mask wearing, and other measures needed to ensure the safety of all communities. With the release of the vaccine and the success of mass inoculation programs many countries, including the United States, witnessed the effectiveness of these measures at controlling the spread of COVID-19. Despite the fact that variants of the virus are out there and more variants can be expected, there appears to be a way out and the means to fight back rather than to simply accept changed norms.

The vaccines should not be looked upon as a silver bullet but as an important component in the effort to combat the virus. As the number of inoculations increase, social distancing and masking rules will be decreased. The more people who decide against the vaccination, the longer the rules will remain in place.

As businesses return to normal, the expectation should be that the resumption of pre-pandemic activities will be gradual. Businesses should plan for periodic resurgences but hopefully these will be localized surges that can be contained with community level support. This makes it important to not abandon the strategic programs that were undertaken at the onset of the virus simply because vaccines are now available. Merchants who had to improve their online presence in order to stay in business during the pandemic should not abandon those efforts. Restaurants that shifted to take away and deliver based business models should not abandon those efforts as the summer months approach. This projects should continue to move forward as an adjunct to established business practices. And by all means, efforts to improve infrastructure and government support systems must not be abandoned. The pandemic may have crystallised the need for many such private and public projects, but that does not mean the projects were not important on their own. It is difficult to identify a pandemic driven project that does not serve to create incremental value in a post-pandemic world. Maybe that is the silver lining of the pandemic, it forced the population to do things the should have been doing all along.

On a more personal note, I got my second vaccine shot at the end of April so I am now fully vaccinated. As I look back over the last 15 months, I realize that I never got the winter cold that I am usually afflicted with, I saved a lot of gas money, and my dietary habits improved as I steered away from processed foods in favor of home cooking. I am planning to carry as many of these beneficial behavioral changes forward with me into the post pandemic world as I can. Do not be surprised if you see me continue to wear my mask on the street as I embrace a healthier lifestyle.

## UPCOMING VIRTUAL EVENTS

- **May 4, 2021.** Smarter Cities: At the Intersection of People, Data, and Devices. Smart cities have the potential to make amazing contributions, but there are important issues to resolve including data privacy/ownership, public-private partnerships and infrastructure resilience just to name a few.
- **May 5, 2021.** The Urban Revolution, Innovation, and the Future of Cities. An exploration of the relationship between technology, real estate investment and the making of future cities.
- **May 10-12, 2021.** Data Sumit Connect. Covering the latest strategies and technologies in data management and analytics.
- **July 6-8, 2021.** Data 2021. Brings together researchers, engineers and practitioners interested on databases, big data, data mining, data management, data security and other aspects of information systems and technology involving advanced applications of data.
- **July 14, 2021.** Data Architecture Online. K**ey strategies and technologies you need to know in order to build and manage a modern Data Architecture.**
- **Sept 17-19, 2021.** Data Con LA. One of the largest data conferences in Southern California.

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

## THE I$^3$ CORNER

I3 Systems is close to releasing the first version of their I3 Software. The software release is currently scheduled for May 17, 2021. Compared with prior POC versions of the software, this new software release will feature an enhanced user interface system, greater scalability, improved reliability, and an improved data logging system. While prior iterations have served us well as the basis for research and concept exploration, this latest release is ready for real-world operational deployment. As we approach the launch date, the software will be listed for purchase on the I3 Systems web site - I3-IOT.com for online sales. And, by all means, feel free to reach out to contact us if you are interested in the partners program we will be creating after the software launch.

The next I3 Consortium meeting is scheduled for early June. It will be a virtual meeting that is planned to run for approximately one hour. We are planning to have the June session focus on efforts to bridge the digital divide in Los Angeles County. If you are potentially interested in attending these sessions, be sure to register on the I3 Consortium's list server by sending an email to i3-join@i3-iot.org.

## READER CONTRIBUTION: Building the Culture of Data Sharing with Data Trusts

By Anna Artyushina, York University

The public trust in platform companies hit its historical minimum in 2018 when the Facebook-Cambridge Analytica scandal erupted. The ramifications of the data breach for Facebook have been significant, and some are yet to come. In 2019, the company was fined by the US Federal Trade Commission, the European Commission, and the UK Information Commissioner's Office. According to the 2020 financial statement, Facebook set aside $366 million for the fines related to the eight ongoing investigations by the European data protection authorities. In North America, Facebook continues to lose active daily users and advertisers.

While Facebook took the heat, the entire industry has suffered immense reputational damage. Shoshana Zuboff's book *The Age of Surveillance Capitalism* became an international bestseller, as it highlights the connection between the extractive data collection practices and the behavioral modification techniques employed by platform companies. A growing number of research and journalistic investigations have drawn attention to the economic challenges brought about by the monopolization of the data economy: companies like Google, Apple, and Amazon manipulate the markets they've created to promote their own products and suffocate the competitors. In December 2020, the US Department of Justice and three dozen states filed three antitrust lawsuits against Google.

For the general public, the Facebook-Cambridge Analytica affair has opened up a timely conversation about the true value of data. Surveys conducted by the Pew Research Center show that over the last four years, American internet users have recognized privacy online as a value and have become more reluctant to share their data with the websites and apps they are using. The COVID-19 pandemic has further heightened the public interest in data governance as the health researchers and public officials collect and reuse the breadth of heterogeneous data to manage lockdowns and the vaccination. A recent study published in the *Harvard Data Science Review* shows that, contrary to the earlier belief that the mass consumer is not ready to take control over their data traces, Americans are open to the idea of sharing personal data for a public purpose.

Obviously, there are limits to what an individual can do when the entire digital infrastructure of the internet is staged to covertly track the users. Latest privacy laws, however strict, fail to suppress the shadow data economy. For instance, in its *2020 Implementation Report,* the European Commission admits to having significant problems with the enforcement of the General Data Protection Regulation (GDPR). In the Unites States, the recently passed California Consumer Privacy Act (CCPA) is estimated to cost the US companies $55 billion, yet some critics say it has already become a matter of compliance.

The bigger change is already underway and it comes with the professionalization of the data stewardship. Over the last three years, the industry of private data trusts has been steadily growing with the markets for personal and nonpersonal data emerging in the US, Canada, the UK, and Japan. Financial and medical institutions have been rather successful in adopting new data governance models, as they have had previous experience with the data reuse through contractual agreements and have their own data governance protocols in place. Some data intermediaries have already been a financial success. Mastercard established its first data trust, Truata, in 2018 to manage the data collected from European residents. Truata successfully operates as a data controller, generates €30 million annually, and takes external clients.

Several nations perceive data trusts as a way to achieve the leadership in artificial intelligence. In the United Kingdom, the AI Council and Cambridge University just launched the Data Trust Initiative. The Canadian Digital Charter explicitly names data trusts as a means to boost digital innovation. Belgium has just launched the AI Institute for the Common Good (FARI), which will operate its own data hub. In 2020, Australia launched its own AI and data intermediaries program. As the concept of the data trust becomes a geopolitical instrument in the new AI arms race, it gains significant political and economic power.

The transition to the responsible data economy will not be easy or cheap. To make the data economy work for everyone, we will need to decouple data from companies that trade in data. A new physical and digital infrastructure is needed, which will allow individuals and organizations to share digital information safely and create a level playing field for the businesses. This may require significant public investments and policy adjustments. Certainly, the European Union has been a trendsetter here. It is expected that when the European Cloud Initiative is implemented, companies like Facebook will not be able to move the data from the continent, and the extent of Facebook's engagement with the user's information will be closely monitored through the new program interfaces. The European Data Governance strategy offers establishing the niche markets for personal and nonpersonal data and instituting the industry of professional data stewards, which will help individuals protect privacy and realize their rights under the GDPR.

Building public trust in data trusts is the key to success here. In the UK, two markets of personal data went bankrupt as they failed to attract enough data donors. On both sides of the Atlantic, public officials have been rather reluctant to partner with the private data trusts, seeing data reuse as a privacy threat. Therefore, the European Commission is speaking about establishing the culture of data sharing. Digital literacy programs for the responsible data economy mean creating novel, more detailed concepts for data and transparent legal mechanisms for the data reuse. Creating secure public and private storages for data should be accompanied by the new licensing systems, which will ensure that all data intermediaries operate in good faith.

## New Data Rules Drive Operational Changes<br>by Jerry Power

Last November, California passed the California Privacy Rights Act (CPRA) which largely serves as an update to the California Consumer Privacy Act (CCPA) that was originally passed in 2018. There are those who argue that a patchwork of privacy laws makes it difficult for companies to do business; but the reality is that when these companies adhere to the most stringent requirements and apply them across the board, this issue largely goes away. CPRA has the potential to become one such lighthouse issue that drives action beyond the borders of the state of California borders.

CPRA properly recognizes that privacy cannot be ensured unless the data has been properly secured. Data security is a prerequisite that must be considered before an effective data privacy policy can be put in place. The law requires that companies that store personal information implement reasonable measures to detect security incidents, resist malicious or illegal actions, and aid in the prosecution of malicious individuals responsible for such actions. The requirement that companies aid in prosecution of individuals implies the need to keep detailed records about such attacks. On the surface, this may not seem like an onerous requirement, given that most data security systems logs detected security events; however, by linking security to privacy, CPRA has created a need for security threats to be correlated to data repositories and then to potentially impacted individuals.  Most organizations do not have a complete (and auditable) directory of the data held within their organization and this issue may be a major obstacle in meeting these new requirements.

CCPA required consent before an organization could begin collecting personal information.  CPRA has made the definition of consent more specific.  For example, consent requests cannot be incorporated into broad and general statements of policy.  Consent agreements must be explicit, self-standing so the request and its limitations are clear to the individual.  CPRA also requires consent agreements to be reasonably specific as to the purpose of the data collection, the type of data collected, and how the data will be utilized.  In addition, organizations cannot assume any general activity on the part of the user can be construed to imply consent.  For example, by simply putting the consent form on the screen, the organization cannot assume the person would agree based on making the consent information available to them.

CPRA  expands the definition of what is considered personal information.  Technologies that monitor a person’s behavior through heat maps, mouse tracking, historic use patterns, etc are not prohibited but they are considered personal information.  As such, organizations have to obtain a user’s consent before these technologies can be used.  CPRA also goes as far as to set organizational limits to consent agreements.  For example, if the user consents to allowing Budweiser to collect data about them, it does not mean that they have agreed to allow Corona access to that data even though both companies are part of the InBev group.

CPRA serves to extend the regulatory reach of these agreements into the data supply chain.  If an organization provides data to a third party and the user later asks to be deleted from the data set, that request must be passed on to all third parties who received the data, directly or indirectly, from the source organization.  This implies that any organization who provides data to a third party must also track their data distribution systems.  Further, any third parties that accept data from another source are bound to the conditions that the original organization established when the data was first collected.  This requires that not only must a company track (and presumably audit) the data that is held within the organization, this data directory must also be capable of tracking third party data as it enters or leaves the organization.  Essentially, the organization must track the provenance of the all data within and flowing through the organization.  If an organization discovers that a down-stream partner is not using the data in accordance with the established consent agreements, the organization is expected to take reasonable steps needed to remediate use of that data.

CCPA required organizations to disclose the type of information collected about individuals. CPRA expanded this requirement to allow individuals to request organizations disclose the exact information they hold about them and the retention policy associated with their data.  As a part of this process, individuals can request that erroneous information be corrected or deleted.  The law also mandates that retention periods cannot be unreasonably long and should be tied to the use case described when consent was obtained.

CPRA put additional clarity around the activities that are covered by the law.  As originally written, CCPA rules applied to the sale of data between two entities.  CPRA clarified this point by establishing that other non-commercial transfers of data are included under these regulations.  The consent agreement must also indicate any expected data sales/sharing arrangement that might make use of the collected data.  If, by chance, the organization decides to share data with a third party after the data has been collected, the original consent agreement must be modified and sent to the affected individuals in order to affirm their continued consent .

Despite the fact that the ‘C’ in CCPA stood for Consumers, the CPRA laws also applied to employee data held by the company.  CPRA makes it clearer that these privacy rules apply to any personal information held by the organization, not only ‘customer’ data.

CPRA also created a new state agency, the California Protection Agency, which is tasked with enforcing the CPRA laws.  This agency can levy fines and it also has the authority to audit an organization's privacy (and security) practices.

CPRA only applies if an organization is a for-profit entity that has either more than $25M in revenue OR if 50% of its revenue comes from its data sharing activities.  While small companies and nonprofits are not covered by the law, these other organizations should consider adopting the CPRA practices as a normal market expectation.

CPRA won’t be enforceable until 2023 permitting organizations some time to get their house in order; but once it does become effective, it will cover all data that was collected from January 1, 2022 onward.  These requirements have driven many organizations to designate a Chief Security Officer (CSO) or a Chief Data Officer (CDO) that is intended to establish and then oversee the organization’s efforts to secure the data they hold.  These personnel have 2021 to get their strategies defined and in place so they can begin monitoring data systems within their organization at the begining of 2022.

## READINGS FROM THE EDITOR'S DESK

**Putting digital at the heart of strategy.**  Technology began its life as a support system that increased business productivity. Technology evolved and became an enabler of business strategy. Most recently, technology has become the lynchpin where strategies are built around tech innovation.
**The blistering pace of digital transformation is only going to get faster.** Digital transformation programs refer to efforts to increase customer activities in a connected world and/or reduce operational costs. The pandemic has accelerated these efforts for everyone and in some cases the programs have become critical projects.
**The US Intelligence Community’s Harrowing Take on Our Possible Futures.**  The US National Intelligence Council issued the Global Trends 2020 report which forecasts an increasingly dynamic world. Such an environment will require business agility. From a tech perspective, it implies an increased focus on tech infrastructure.
**HIPAA, the health privacy law that’s more limited than you think, explained**.  HIPAA was designed for data portability and governance in the healthcare industry. It is not a panacea for all health related data. As a portability framework, it's incidental references to privacy and its limitations should be better understood.
**5 ways new monitoring technologies can help cities combat air pollution**.  Overview of London's tactical plan to combat air pollution via IoT. Response tactics that drive data collection activity was considered up front and then the data was utilized to actions that impacted results.
**Future of IoT: 6 trends and predictions to watch**.  The IoT market is capable of growing at a CAGR of 30% but only if continual progress is made in business drive use cases, privacy, security, standardization, AI, and efforts to evolve the architecture to support a common data framework.
**How smart buildings can take care of themselves and help the environment**.  Smart buildings must to be approached as an ecosystem where multiple independent participants cooperate and share data in order to achieve meaningful results that reduce the operating expenses of the building.

**Why Target Thinks Enterprise IoT Has Finally Arrived**. Companies that have many data streams are beginning to move away from point solutions to create managed data platforms. At some point we will stop thinking about the network as a connectivity tool and begin to think of data as part of the infrastructure.

**Self-Driving Cars Head Toward Collision With Insurance Status Quo**. Self driving cars will impact to the insurance industry, an industry based on risk management. Autonomous cars can reduce risk reducing premiums. Sensors and data could also reduce risk in other areas changing the way we think about business.

## 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. If you have suggestions, topics you want to see included in future newsletter updates, or other general inquiries, feel free to email us 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 members of our community of interested people.

## ABOUT I3/CiTM

Originally founded under the guidance of USC, the Institute for Communication Technology and Management (CTM) was formed to support a deregulated telecom industry. Over time, computer and networking technologies evolved and grew changing the way we do business and live our lives. The CTM Newsletter was created as a vehicle to foster continued conversation about tech associated issues that transcend specific technologies and specific industries. CTM conducted foundational Internet-of-Things research and created 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, along with a host of supporting companies, academic institutions, and private individuals, this vision was turned into Open Source software that was released in December 2019. I3 Systems was formed to pursue commercial opportunities based on the work of the I3 Consortium and the concepts published in the newsletter. With this grass roots tech movement, the newsletter evolved and continues these conversations even further.

*If you wish to be removed from our distribution list, click here unsubscribe*

I3 Systems, 1146 N Central Ave #687, Glendale CA 91202, www.i3-iot.com