The Road Toward Behavior-driven Automation

By Andre Fuetsch, AT&T

If 2020 taught the world something it is that adaptability is essential, and flexibility is key to social and economic stability. In times when health safety is paramount, with small IoT devices producing unimaginable amounts of data and automation driving productivity, the world is on the evolutionary path toward a more integrated knowledge-driven society. The next chapter of technology evolution is bringing together existing technologies such as the Internet of Things (IoT), data analytics, artificial intelligence (AI) and 5G, making it possible to enact human behavior changes and enabling context-based decision-making to augment worker productivity as well as safer and healthier communities.

The COVID-19 pandemic accelerated a global shift toward a mobile, location-agnostic society and the rise of a nomadic generation. Social distancing does not mean social isolation, and the need to understand user behavior is more critical than ever. From co-working to remote work or just to collaborate and interact with business partners and friends, it is becoming quite clear that the trend is here to stay and it opens up a new way of looking at perimeter security as well as the need for ubiquitous seamless connectivity.

Behavior-driven network selection is essential, and users should be presented with access network choices based on their "persona" allowing them to securely switch between work, study, or entertainment. Seamless broadband fiber and wireless network integration in the home and office will allow them to share a printer, pause streaming movies or control smart devices. This seamless network access comes with challenges, especially in the shadow of several high-profile cyber security attacks on national infrastructure. Hard wired, rigid security policies are not effective in hybrid working or learning environments where devices are moving in and out of enterprise networks. This demands a new approach where user-based context-awareness allows applying zero-trust policies across multiple network domains. Zero-trust is a paradigm shift in network security and assumes that the network has already been breached, therefore requiring authentication and access control checks as users access internal systems. This type of authorization needs to be frictionless and effortless on the user's part so companies are looking at multifactor, password-less authentication mechanisms coupled with context-awareness checks such as location, device or even the access network identity where the user is connecting from.

And it is not only for network security; all the context and behavior awareness are driven by data. Data is also becoming more critical than ever from defining health policies to evaluating human impact on the environment. While data is an essential ingredient in process improvement and progress in general, the sheer amount that is generated via technology makes it unusable in a raw format. Through data analytics, we turn data into information, adding structured ways to evaluate and use it. Information-in-context becomes knowledge, and when combined with behavioral psychology, generates wisdom.

As a result, a new trend is emerging and is expected to grow in the years to come. Enter the Internet of Behaviors, a concept first coined by Gote Nyman, a retired professor of psychology at the University of Helsinki in 2012 and elevated to stardom by Gartner as one of the emerging technologies of 2021. Internet of Behavior makes use of the data generated by the vast IoT networks of sensors and smart devices to influence behavior. It has the potential to change the way we use technology, how we share data, and more importantly how we look at privacy.

At the very high level, IoT is a network of networks of devices and sensors under various administrative domains. Internet of Behavior brings user centricity and adds "human nodes" into the mix to combine and correlate data from devices with the power of social networking. The ability to gather, aggregate, and utilize data to influence or analyze behavior is the new way of interacting with customers and employees. By attaching behavior to a user's profile, companies can provide a better user experience in retail, transportation and other industries, while allowing them to proactively identify and resolve issues. It should enable marketers to better understand customers and offer relevant products and services as well as empower users to make health, safety, or product decisions by placing data-driven options in their hands.

The concept of altering behavior using data is not new. Probably one of the simplest examples is the use of speed displays on specific accident-prone spots on roads. Chosen locations are already the result of data analytics collected using smart city sensors aggregated with weather information and vehicle demographics. Alerting the driver of their speed and making that data highly visible on the road proves to be effective at enforcing the speed limit by leveraging behavioral psychology.

Computer-vision, coupled with data analytics, can drive the enforcement of safety regulations such as the use of masks, and it can be used in conjunction with thermal sensors to track peoples' temperature in public places such as malls or stadiums as well as in the workplace. There's no better example of an expected behavior-altering application than police body camera solutions. Another computer-vision use case is applying facial recognition for customer demographics analysis used in conjunction with location and behavior aware preference selection for consumers. These are also good examples for real-time, low-latency and privacy sensitive applications that call for deployments as close as possible to the data-sources, making these prime candidates for Edge Computing. Edge Computing brings compute, storage, and memory resources closer to the Edge of the network, allowing the offload of latency sensitive workloads from the cloud data centers. Due to privacy sensitivity, typical solutions would have to process raw data, anonymize, and aggregate without storing or transferring any individually identifiable data.

Health applications are another great example of user-driven behavior-changing solutions. Unlike previous use cases, the user is the aggregating hub of raw data from sensors such as scales, blood pressure meters, fall detectors in addition to location data, environmental data available from municipalities on air or water quality to allow the users to adapt and adjust their behavior toward improving their health.

A special category of use cases are collaboration robots or cobots. These are a new generation of robots designed to help in the automation of processes. Unlike typical robots programmed to perform a very specific task such as painting a car or attaching a windshield, their specific goal is interacting with human counterparts, understanding their behavior, and helping them by increasing safety and productivity. One example, for instance, is a cobot that is designed to enter toxic areas, lift heavy objects, or bring parts to a team of workers. We can think of them as non-human apprentices. While manufacturing is a significant sector benefiting from their applications, other industries (retail, logistics, etc.) are adopting collaboration robots and they are expected to take advantage of the deploy-

ment of non-public 5G enterprise networks supporting low latency and high bandwidth.

As with any technology, the Internet of Behavior and related user-centric context-aware solutions are not without headaches. In fact, they highlight and elevate the importance of addressing issues modern society is already facing.

Since at the foundation of digitizing user's behavior is the ability to aggregate and understand patterns, the use of AI and machine learning (ML) is essential. The risk of introducing bias into the models has already been identified as a major societal concern and has the negative potential to exacerbate the existing racial or economic divide.

In addition, anything involving user data collection by private or governmental entities, while it brings huge benefits for individuals and the society in general, has the potential to be abused and used for other than the intended purposes. Privacy is a major concern with more and more personal data being used as a digital commodity by various parties. The lack of regulations and geopolitically fragmented laws only exacerbates the issues and adds complexity for implementors and confusion on the user's part. Add data correlation by third-parties and it becomes obvious how some data elements that otherwise might look benign, such as the installed set of fonts in the browser, combined become extremely powerful tools for fingerprinting users and accurately identifying them on the Internet without their consent. The problem is aggravated by the extended retention practices which with the help of data analytics tools, ML and heuristic algorithms allow third parties to add digitized behaviors to users. This type of covert data collection and aggregation without the user's awareness creates aversion toward the technology in general, eroding the value proposition for legitimate and user-consented use cases.

Recent data breaches and cyber-attacks add another risk dimension for user-centric behavioral digital data. Criminals capable of acquiring, using, and sharing enhanced user data will have new tools for social engineering attacks such as phishing, as well as more sophisticated, targeted physical crimes based on the user's behaviors such as their walking or commuting schedules and travel plans.

Turning data into knowledge and leveraging it to track or modify behavior is not a science fiction topic. To a certain extent and as illustrated by the examples above, this is possible today and being used for targeted advertising, health monitoring and manufacturing efficiency. The next decade will see an explosion of applications that put users and their behavior in the center by leveraging the myriad of devices and sensors deployed. The vast amounts of data collected and corelated will require high bandwidth reliable and secure network connectivity solutions such as 5G and processing power closer to the edge of the network. Technology leaders need to be prepared to embrace the benefits of this new wave of user-centric solutions but also address the potentially negative side effects.