Ten Things to Watch for in 2019

Levine, Blaszak, Block & Boothby (LB3) and TechCaliber Consulting (TC2) are the preeminent technology legal and consulting teams dedicated to helping companies maximize the return on their investment in information communication technology. Together we've compiled the ten things that enterprises need to watch for in 2019 that will impact your technology and purchasing roadmap.

5G: Separating Myth from Reality

Just as it did with 4G, AT&T has once again jumped the gun and announced that it was deploying 5G (well, actually, they call it "5G *+*") in twelve cities and rolling out 5G*E* in several more markets, all of which made Verizon, Sprint and T-Mobile scream "foul." They – and many industry observers – claim that AT&T was merely re-branding a faster version of 4G as 5G and misleading the public about the technology.

AT&T did the same thing with 4G several years ago, and it received the same sort of criticism, but apparently, it has a short memory. Let's be honest about what AT&T has really done. First, "5GE" isn't 5G at all, but instead is just faster 4G, also known as "Gigabit LTE." Second, while AT&T claims 5G+ can achieve speeds of 200-300 Mbps, it says that the technology is "delivered over millimeter wave spectrum," which is one, but only one, aspect of the 3GPP 5G New Radio Standard for true 5G. That standard also includes small cells, beamforming, and MIMO, all of which are missing from AT&T's own description of 5G+.

In full-page ads in major cities' daily newspapers, Verizon has challenged the wireless industry to be honest about 5G to avoid confusion and misleading the public; but despite its sanctimony, Verizon Wireless' own version of "5G" isn't based on the 3GPP 5G New Radio Standard, but rather Verizon's own homegrown version of 5G, which it calls "5GTF." In the meantime, Sprint (the number FOUR carrier) claims to be the first U.S. carrier to use real 5G technology (i.e., based on the 3GPP standard) on a test basis in San Diego in January. So, as is often the case with wireless services, the only thing we know is that we know very little. Industry analysts predict that widespread commercial rollout of true 5G service won't happen until 2020.

Meanwhile, the global battle for 5G leadership rages on between the U.S. and China. China's Huawei Technologies, a manufacturer of wireless devices, network infrastructure, and components, is aggressively seeking world dominance in 5G as both a standards setter and an equipment provider, particularly in Asia, Africa, and parts of Europe. The U.S. government has banned Huawei's products from government procurements, fearing that the Chinese government can use those products to spy on Americans, and it is urging U.S. carriers and U.S. allies to do the same. Canada, Great Britain, and Germany are already on board with U.S. concerns. Nevertheless, analysts predict that China will be the first country to achieve large-scale 5G deployment, followed by South Korea, and then the U.S. American wireless carriers and electronics manufacturers have to spend more on R & D and need more spectrum to be competitive. Even so, some experts report that U.S. carriers plan to invest $275B in 5G, which could boost the nation's GDP by $350B and create 3 million new jobs. In short, when it finally happens, 5G will truly be revolutionary.

Takeaway: What all this means for enterprises in 2019 is *caveat emptor:* Don't rush out and replace all your old iPhone 8s or Xs and Samsung Galaxies with new devices promising 5G connectivity

until the market works out what 5G really is, and the industry works out the bugs. Furthermore, as exciting as the new technology promises to be, costs for early adopters are certain to be much higher than those available later.

GDPR Will Eventually Become Global Privacy Standard

Enterprises all around the world have begrudgingly accepted their heightened data privacy obligations to European Community residents and regulators under the General Data Protection Regulation (GDPR), which took effect in May 2018. Any business handling the personal information of a European citizen is subject to the GDPR, regardless of where it is located. So sweeping in scope are the new regulations that other jurisdictions, including Brazil, Japan, and India, are considering adopting copycat legislation. In the U.S., where data breaches are a matter of state, rather than federal, law, privacy compliance professionals would love to replace this patchwork of requirements with a single nationwide privacy standard with which their employers would have to comply, as discussed in our companion piece on U.S. privacy legislation.

The obvious template for that standard would be the GDPR, as virtually all global enterprises have already invested millions (possibly more) in understanding their obligations and adopting practices and procedures to minimize the risk of violations, which can carry fines up to 4% of a company's global revenues. The problem in this country, of course, is our fractured democratic system and the clout wielded on Capitol Hill by tech giants and other large corporations.

Takeaway: We anticipate that several other jurisdictions around the world will adopt GDPR-style privacy laws this year and next, while the U.S. will get bogged down in political maneuvering and do very little on the federal level to protect consumers' privacy. Widespread adoption of GDPR-style laws would be a serious matter: The French data protection authority levied a fine of €50 million earlier this month against Google for alleged GDPR violations, and while that amount is not trivial, under the GDPR it could have been in the billions of Euros. Take this stuff seriously.

The Internet of Things Continues to Take the World by Storm

Last year we saw the continued growth of enterprise adoption of Internet of Things ("IoT") solutions, with companies harnessing the power of wireless data collection, analytics, and connectivity to enhance productivity and efficiency in ways we could previously not imagine. Analysts expect corporate spending on IoT in the U.S. to approach $200B in 2019, with global spending exceeding $800B this year. As adoption has grown, privacy and security advocates have called for regulation of the Internet of Things to enhance personal privacy and to strengthen the security of IoT devices and services. Several high-profile data breaches in the past few years were the result of hacks that used unsophisticated, vulnerable IoT devices (such as nanny cams) to get into secured computer networks. (Researchers have hacked into home computer networks using Wi-Fi connected "smart" IoT lightbulbs as the gateway.)

Despite the hype and some hearings before Congress and the Federal Trade Commission, no legislation or regulations have been adopted at the federal level to regulate IoT devices or services. Three bills were introduced in Congress in 2017 – the Cyber Shield Act (which would have made IoT security voluntary); the Internet of Medical Things Resilience Partnership Act (also voluntary, but focused on IoT medical devices); and the Internet of Things Cybersecurity Improvement Act (which

would have set product standards for devices sold to the government) – but none of them ever became law.

Indeed, lawmakers on both sides of the aisle have advocated taking a hands-off approach to IoT, attributing the rapid growth of the Internet in the '90's to a lack of governmental interference. In our view, that's a good thing – at least for the moment – because IoT holds so much promise for new innovation and economic opportunity, and because premature regulation could hobble its development. Issues such as security vulnerabilities in unsophisticated sensor/radio devices will undoubtedly be addressed by market forces: purchasers will demand greater security and suppliers will respond accordingly.

As we mentioned in last year's predictions, one important issue underlying the Internet of Things that producers and commercial customers still have to resolve is: Who is responsible to end users who may be harmed when an IoT device or transmission service fails or is compromised by a bad actor? The current industry approach is for providers of IoT equipment and wireless data service to shift that responsibility to their corporate customers, who buy IoT devices and service, repackage them for a variety of consumer and business applications (e.g., health care, security, energy transmission, transportation), and sell them to other businesses or individual consumers. Although those "middle man" businesses have the direct relationship with the ultimate consumers of IoT services, they are neither the device manufacturers nor the providers of wireless data service, so they depend upon their suppliers for reliable products and services. In our view (as representatives of many of those businesses), the underlying equipment manufacturers and service providers need to assume more responsibility to end users for performance failures. As the market matures, suppliers and users will eventually resolve this issue, though it will almost certainly come at an increased cost for IoT devices and wireless service.

Takeaway: Companies who purchase IoT devices either for internal operations or for resale to customers should proactively explore what additional security measures they should implement given the vulnerability of IoT devices that are interconnected with their networks. And companies that use IoT devices to collect personal information, such as health-related information or location information, need to be cognizant of their obligations under the GDPR and other privacy laws when they handle that personal information.

Will Congress *Finally* Adopt Federal Privacy Legislation?

With the exception of sector-specific legislation, such as HIPAA (for health care providers and insurers) and Gramm-Leach-Bliley (for financial services providers), Congress has never enacted comprehensive privacy legislation, leaving it to the states to protect their citizens. In the wake of the shocking disclosures of personal data collection and brokering by Facebook, Google, AT&T Mobility, and Verizon Wireless (among many others), there has been an outcry for Congress to do something to protect unwitting consumers from having their personal information collected, shared, and used by service providers and unknown third parties in ways they cannot imagine. But is Congress likely to do something in 2019? Considering that it can't even agree on funding for border security, leaving almost a million federal workers and contractors without pay for more than a month, we predict that we will be asking the same question this time next year. Weighing down any hope for progress on this issue is the

lobbying clout of the tech industry and the naivete of most veteran lawmakers about how the Internet and the digital economy really work.

We hope we are wrong. For one thing, the lack of a nationwide data privacy regime makes U.S.-based businesses less competitive in global markets and provides little incentive for companies to voluntarily do the right thing. (For example, a recent FTC fine imposed on Google for privacy violations, touted as one of the largest ever, was only $22.5M, which Google earns in less than four hours. In contrast, GDPR violations can be punished with fines as high as 4% of a company's global revenues.)

Secondly, as noted above, the patchwork of state data breach laws is enough to drive compliance officers to madness; a single federal mandate that preempts inconsistent state laws would be a godsend to those whose job is to ensure that their employer complies with all applicable laws, including state privacy laws. Interest groups from the U.S. Chamber of Commerce to the Internet Association, as well as leading individual companies, are all urging Congress and the Administration to take action to preempt state privacy laws. Privacy advocates, on the other hand, are concerned that any federal legislation that preempts state laws would weaken, rather than strengthen, consumer privacy protection.

The new California Consumer Privacy Act, enacted in June 2018, is a good example of the proactive measures states are taking to fill the void left by federal lawmakers – and the challenges those state laws pose for companies. The California law, which takes effect next January 1, is fascinating because of its provenance: California state legislators rushed to enact the law to prevent it from being a ballot initiative which, if adopted, could not be modified by the state legislature but only by other ballot initiatives.

The Act applies to all California residents and it is similar to the GDPR in many ways except one important aspect: Instead of requiring companies to obtain consumers' opt-in before using their personal information, California's law takes the less controversial opt-out approach, whereby a company has to give consumers an opportunity to opt out from data collection and use, failing which the default is that the company can use the consumer's personal information. The law also requires businesses to disclose on their home pages whether they sell consumer information to others and to provide a link entitled "Do Not Sell My Personal Information" for consumers to opt out. Companies are prohibited from selling personal information concerning persons aged 14-16 without their affirmative consent (or opt-in), and may not sell information about children 13 and younger without the affirmative consent of their parents or guardians. Privacy professionals predict that enterprises will struggle as much to tailor their business practices to comply with the California law as they have struggled to comply with the GDPR. The time, effort, and money U.S. businesses have invested in GDPR compliance have been nothing short of remarkable.

Takeaway: Until Congress marshals the gumption to enact a federal privacy law (don't hold your breath), enterprises will be forced to continue dedicating significant resources to compliance with 51 unique state (and DC) privacy regimes. Congress needs to hear from corporate America on this one.

FCC Proposes New E911 Rules for Enterprises and Others

The gold standard for E911 emergency communications is to have uniform dialing patterns (i.e., 911), regardless of where you are calling from, and for calls to accurately transmit a call-back number

and the specific location of the caller to Public Safety Answering Points ("PSAPs"). In the absence of any of these features, individuals in emergency situations may be unable to reach first responders or, if they do, fire, police, and rescue personnel may be unable to locate the callers or call them back if necessary. In recognition of these challenges to public safety, many states and foreign countries have enacted legislation and regulations imposing requirements for emergency calls, and the Federal Communications Commission (FCC) has adopted some weak regulations that have created more confusion than confidence.

Congress has enacted the RAY BAUM'S Act (yes, that is an acronym as well as a name), requiring the FCC to adopt rules requiring the transmission of accurate location information with emergency calls, regardless of the technology used to make the call, and the so-called "Kari's Law," which (among other things) attempts to standardize dialing for emergency services regardless of location (e.g., to eliminate the need to dial a prefix, such as 9 or 1, prior to 911). The FCC is in the midst of a rulemaking proceeding to adopt regulations implementing these laws, and the outcome will have significant impact on most businesses, equipment manufacturers, and possibly telecom carriers.

For enterprises and telecom carriers, the issue of emergency calling has always posed thorny issues of liability allocation should an individual require emergency services and be unable to complete a call for help or should emergency personnel be unable to find the caller. Telecom companies disclaim any liability for callers' failure to complete emergency calls and routinely try to make their corporate customers accept full liability to both individuals and the carriers should something go wrong with an emergency call. Corporate users of multi-line telephone systems (e.g., PBXs, in use by almost every business), mobile devices/Wi-Fi, DAS, or VoIP that allows nomadic use (calling from one's computer anywhere in the world) face technological challenges providing reliable emergency calling services to their employees, customers, and visitors.

The FCC's pending rulemaking could provide some ground rules for telecom providers, equipment manufacturers, and enterprise customers regarding expectations, obligations, and liability. FCC Commissioners have publicly stated that measures to enhance public safety are a top priority, so we expect this otherwise de-regulatory Commission to adopt rules that will impact the business community. Several pro-business advocacy groups, most notably the Ad Hoc Telecommunications Users Committee, have filed comments urging commonsense, balanced rules that protect the public without imposing unnecessary costs on businesses. For example, rules that would require new or upgraded equipment, services, or software need to be carefully tailored to serve the public interest without going overboard. At the same time, some participants in the rulemaking have asked the Commission to repeal certain rules that have never worked or been practical, such as the notification stickers requirement, and to require interconnected VoIP providers to immediately update their Registered Location databases upon notification of a location change from VoIP users. Currently, there may be a lag time between notification and database update during which the wrong location information about a user could be transmitted to a PSAP.

Takeaway: It's difficult to predict how the FCC's rulemaking will come out, but we expect the new rules later this year. In the meantime, businesses with multi-line telephone systems or VoIP/SIP trunking should become familiar with the issues and possibly make their views known to FCC decisionmakers.

SD-WAN on the Radar

When enterprises develop their network strategies and technical roadmaps for 2019, one of the hot network technologies that will be on the radar will be Software Defined Wide Area Networking or SD-WAN. SD-WAN is a significant transformational solution in the networking space and a major change from the MPLS *status quo* that most enterprises have deployed.

One reason SD-WAN has gained traction so quickly with enterprises is that it is based on many established technologies that have been brought together in a much more accessible way. SD-WAN solution providers continue to enhance their product offerings as take-up of SD-WAN by enterprises accelerates.

SD-WAN is an edge solution where software instances at all connected sites create a virtual overlay network on the network transport underlay physical circuits. These on-site instances, which can run as virtual machines, are managed by centralized orchestrators that reduce the complexity at the edge and enable more rapid reconfiguration and quicker stand-up of sites.

A major benefit of SD-WAN is that the increased separation of the overlay and the underlay networks provides the opportunity to use lower cost circuits, particularly in place of MPLS. SD-WAN allows enterprises to reduce their dependence on expensive MPLS connections and replace them with Internet transport, either dedicated Internet access or business broadband. This can result in significant network transport cost reductions.

SD-WAN also provides better network alignment with business applications. Other attractive benefits of SD-WAN include enhanced performance through rapid-failover, easier aggregation of available bandwidth, more effective tuning of policies and prioritization to applications' needs, and vastly improved network visibility and analytics.

Takeaway: Before committing to an SD-WAN solution, be sure to check your contractual obligations with your network service providers and value-added resellers. While your SD-WAN business case may show you need less MPLS network transport and don't require expensive routers, you may still have revenue commitments tied to your legacy network.

More Broadband for the Buck in 2019

An interesting development that will surely benefit enterprises in 2019 is the use of Internet transport services in the wide area network. Global demand for Internet transport has been skyrocketing due to changes in network edge technology, greater use of cloud services that don't necessitate backhauling all traffic to your data center, and just generally greater adoption of the hybrid WAN. Enterprises can expect these trends to continue in 2019.

But how does using more Internet transport benefit the enterprise? Over the last couple of years, we've observed that enterprises can procure broadband transport connections with up to ten times the bandwidth that they currently have by paying slightly more. That means, for example, that a site can upgrade its 10 Mbps broadband circuit to a 100 Mbps broadband circuit without blowing up the network budget.

This ability to procure more bandwidth for the buck is a global trend. The pace of bandwidth increases for the same or lower cost will likely accelerate in 2019, regardless of whether it's dedicated Internet access circuits with the highest bandwidths – 100's of megabits and upwards – or lower speed business broadband based on consumer-type access technologies.

Takeaway: Enterprises will find buying internet transport services much easier due to the number of transport aggregator options now available. Many traditional telecom service providers are also starting to realize this is the new normal for network services and are fighting to compete. To benefit from this new network dynamic, enterprises will need to develop a view of their future state network and use it as the target for establishing the right bandwidth mix and the suppliers that can provide it.

Telecom Expense Management Will Get a Makeover in 2019

As telecom billing became more complex and increasingly prone to errors, an entire cottage industry was born to help enterprises manage their telecom. Telecom Expense Management, or TEM, used to provide just that – a valuable tool that touched all aspects of an enterprise's telecommunications lifecycle. But in 2019, expect TEM to get a makeover.

Most of our clients use externally provided TEM services and lately we've seen TEM providers expanding beyond the traditional boundaries of wireline and wireless services and offering support for other technology and services, such as managed services, maintenance, hosting, and cloud services. As enterprises retire legacy technology and network services, expect TEM providers to continue to expand their service offerings to meet changing enterprise requirements.

The TEM marketplace is ever-evolving. Countless TEM providers have merged and many have expanded into supporting new services and extending their global reach. Enterprises can expect more consolidation in this space in 2019 as TEM providers look to close gaps in their service offerings.

If you're shopping for a TEM provider, you will be surprised to learn about the TEM providers' capabilities around integration with ServiceNow and other service management systems. You'll also be surprised at the expanding capabilities of many TEM providers and the array of options available for buying TEM solutions – from SaaS, host and load, host and process for payment, host and pay, to the full BPO outsourcing model.

Takeaway: Approach your TEM decision the same way you purchase other technology services – by doing your market research and then competitively sourcing the solution you need. TEM used to be about finding billing errors. In 2019, expect the TEM providers to bring a new game plan.

Vendor Management Will Get Harder as Vendors Reduce Support Staff

It's a truism that how you feel about your vendor is largely a reflection of how you feel about your account team and how they respond when there is a problem. It is with this in mind that the recent (and anticipated) layoffs and outsourcings at AT&T, Verizon and CenturyLink, as well as other telecom vendors, spell trouble for enterprise customers, who can expect a rough patch in vendor support and management in 2019.

AT&T announced in January that it plans further cuts to its workforce – on top of last year's reduction in force of 10,000 jobs and the closing of more of its call centers. AT&T is responding to its

heavy debt, which it took on in part to acquire Time Warner, as well as its need to focus on growth areas – recently AT&T stated that it was prioritizing investments in new technology and content offering over legacy services. While AT&T has claimed it will hire additional personnel as a result of last year's tax cut, it does not refute that it is cutting personnel.

Last fall, Verizon offered 44,000 employees, a quarter of the company's total workforce, a voluntary severance package. Verizon also inked a $700 million deal with Infosys to outsource much of its IT operations. Verizon explains that the reduction in its workforce is needed to help finance the rollout of the 5G network.

CenturyLink continues to trim its workforce (last year it announced it would layoff roughly 2 percent of its workforce so it could invest more in growth), as it tries to "right size" after the Level 3 acquisition, and news reports indicate that several senior level CenturyLink heads have left for greener pastures.

Takeaway: Enterprise customers should examine their existing contracts to see how much, if any, protection they have against losing key account team support, and whether they have safeguards that would prevent critical information from being shipped offshore as the result of a vendor outsourcing. Watch out: Vendors are seeking to charge for support services that previously had been "baked" into service charges in the past. If you have to pay separately for support (and you shouldn't) you should see significant reductions in the cost of services. Enterprise customers should also consider adding SLAs on response and repair times as well as other common sources of headaches in anticipation of a reduction in support.

Net Neutrality Will Continue to be a Battlefield

The Net Neutrality wars continue. In case you took a year off the news last year (and we wouldn't blame you), here is a quick update on Net Neutrality:

Net Neutrality is the principle that all traffic on the internet should be treated equally and that ISPs can't favor their own content over others. The Federal Communications Commission ("FCC") adopted Net Neutrality rules in 2015 to support those basic principles. The Net Neutrality rules included provisions to protect companies from ISPs demanding payment for delivery of a company's content to the ISP's customer and prohibited the slow transmission of lawful data based on its content or originator ("throttling"). The rules also reclassified broadband so that it was subject to greater regulation, similar to traditional telecom services. Last year, the FCC, under a new chairman, repealed the bulk of those rules and reclassified broadband service so that it was subject to fewer regulations. Not surprisingly, the FCC's decision was appealed, and last year Congress unsuccessfully attempted to reinstate the FCC's rules through the Congressional Review Act. The D.C. Circuit heard the appeal on February 1, 2019, after denying the FCC's request for a delay because of the government shutdown. It is likely that the D.C. Circuit will issue an opinion this summer.

Although many news accounts focus on the impact on consumers, Net Neutrality is important for enterprise customers, particularly because without Net Neutrality rules, the consumer's ISP can demand (and historically monopoly providers have demanded) payment from parties trying to communicate with its subscribers. (Think access payments by long distance providers to local phone companies.) Right now, the consumer pays for its internet service, gets online and accesses your

website to place orders, report problems, and inquire about products. The subscriber's ISP does not charge you or your provider. However, the consumer's ISP an absolute monopoly over access to the consumer via the ISP's internet connection. Without Net Neutrality rules, the ISP is free to exploit that monopoly by demanding payments from enterprise customers or interconnecting providers as a condition of letting their data be downloaded to the ISP's subscriber or be downloaded quickly. The provider may not want to charge the consumer more, but the customer's ISP could say that, in order for the customer to enjoy unthrottled access to the enterprise's (such as a retailer, insurance provider, etc.) website, *the enterprise* must pay as well – they would do this by charging the enterprise's ISP to get access to the end user and then the enterprise's ISP would pass those charges along to you. We all know (and studies confirm) that traffic delays thwart sales in online markets. An Amazon study found that every 100ms of latency costs it 1% in sales. And would they do it? Almost certainly. Some ISPs have already expressed an interest in charging such "gatekeeper" fees and, historically, charging non-subscribers for access to subscribers has been the business model of both the telco and cable worlds. This explains why companies like Facebook, Netflix and Amazon, as well as many small businesses generally supported the original Net Neutrality rules.

Net Neutrality puts a check on the ISPs' monopoly power, and unchecked, enterprises will need to remain vigilant as to other ways that an ISP could monetize its monopoly in ways adverse to enterprises' bottom lines. In addition to the examples above, enterprises that have significant telecommuting workforces may care about the outcome, as the worker's ISPs control their access to the internet.

How this will ultimately work out is unknown; what is known is that regardless of who wins the D.C. Circuit appeal, there is a lot of money at stake. Thus, there will be a subsequent appeal to the Supreme Court and the market will remain subject to tremors and uncertainty until the Supreme Court definitively rules or Congress passes legislation (that the President will sign).

Takeaway: While Net Neutrality works its way through the court system, pay attention. Make sure you include protective provisions in your contracts and guard against any attempts to increase your rates in order to allow your customers (or prospective customers) "fast" access to your sites.

Network World recently published articles on IoT, 5G, and SD-WAN written by Kevin DiLallo, Joe Schmidt and Laura McDonald, which have been incorporated into this article. You can find these articles at www.networkworld.com.