

Pipeline

SURVEY RESULTS:
**THE ROAD TO
TRANSFORMATION**

+
**THE
SIGNALING
SECURITY
PROBLEM**

WIRELESS
Security Standards

**MOBILE
IMPACT**
ON ENTERPRISE
COMMUNICATION

Kito-Lyn's
GREAT MOBILE
ADVENTURE

AT&T's
Millennial Mobile
EXPERIENCE

THE RETURN OF
THE SMALL CELL

THE **BIG BET**
ON CONTENT

> The death
of cellular voice

**MOBILE & CLOUD
GAMING**

TAKING AIM:
Automated
Infrastructure
Management

MOBILE EVERYTHING



Focused Forward.



To move forward, you need to focus in one direction – the direction your customers are facing. Focused forward means taking steps to become nimbler and more important to your customers today, while preparing for an uncertain future.

We have the expertise, the culture, and the technology to help you take your most important step ... the next one.

Find your focus at Booth # 2H31



Focused forward

IN THIS ISSUE

AT&T's Millennial Mobile Experience

By: Vishy Gopalakrishnan

It's 2016. The network is on demand. Your office is mobile. The cloud is highly secure. And your smartphone may even be surgically attached at this point – sometimes, it's hard to tell. We've grown more dependent on technology for work and our personal lives. As the workforce becomes more mobile and ...

8

The Road to Transformation

By: Scott St. John

If you think about it, service providers should be transformation experts by now. Remember, we're talking about an industry today that was, just 20 years ago, a monopolistic, government-controlled utility. I can't think of any other industry that has to contend with as many monumental shifts, with such ...

11

The Signaling Security Problem

By: Iliia Abramov

Mobile World Congress 2015 was a record-breaking event, with more than 94,000 attendees and 2,100 exhibitors convening in Barcelona for the tenth year in a row. As we head into this year's conference, a number of sessions and discussions around emerging mobile trends will all echo a resounding ...

15

The Return of the Small Cell

By: Renuka Bhalerao and Tom McQuade

Not a long time ago, in a galaxy not far away – in fact this one – small cells made their first appearance on the scene. In a 3G network, small cells were primarily used for in building coverage where it was needed. It was an important role, but not a glamorous one. According to Stefan Pongratz, Senior Director ...

18

Wireless Security Standards

By: Alan Zeichick

Security standards for cellular communications are pretty much invisible. The security standards, created by groups like the 3GPP, play out behind the scenes, embedded into broader cellular protocols like 3G, 4G, LTE and the oft-discussed forthcoming 5G. Due to the nature of the security and other cellular ...

21

Mobile Impact on the Enterprise in 2016

By: Steve French

Today's connected customers expect interaction with preferred businesses to be three things: quick, easy and secure – and most importantly they want this communication to occur via mobile. As consumers become increasingly receptive to interacting with enterprises through their smartphones, ...

24

Pipeline

The Big Bet on Content

By: *Tim Young*

Behold: a look at the future, from the past. "Mobile-phone companies are always trying to sell you the next big thing," wrote Rana Foroohar in Newsweek. "Phones that can stream football games, send you movie clips, download a new song or snap pictures are what beleaguered telecom operators hope will ...

26

The Death of Cellular Voice

By: *Chris Piedmonte*

There are clear indications that we are beginning to see the slow, certain death of cellular network-based mobile voice services. Across the globe, customers are using their mobile devices to access data networks far more than they are to place mobile voice calls. When they do use their mobile devices for ...

28

Mobile and Cloud Gaming

By: *Wedge Greene*

The call is received in the payment inquiry center: "What is this two hundred dollar charge on my Visa?" Pay-to-Win games are monetized by user interaction with an in-game threshold: pay a little money and get a helper artifact or hint that enables the gamer to complete a level and advance. Most of the time these ...

32

Kito-Lyn's Great Mobile Adventure

By: *Wedge Greene*

As post-millennials live and work, they will expect everything to be networked, connectivity to be integrated, access to information immediate, and monitoring of activities real time and continuous. International cultures amalgamate in the Internet-driven society. The IoT evolves from artifacts accompanying life to the ...

36

Automated Infrastructure Management

By: *LeaAnn Carl*

Automated Infrastructure Management (AIM) automates discovery and documentation of network cabling infrastructure in the data center, central office or commercial building. By adopting an AIM solution, network administrators can streamline provisioning and monitoring of network connectivity, gain an accurate ...

42

Industry News Digest: February 2016

46

Members Directory

49

Pipeline

Scott St. John

Publisher and Managing Editor
scott@pipelinepub.com

Tim Young

Editor-In-Chief
tim@pipelinepub.com

Chris Piedmonte

Senior Editor
cpiedmonte@pipelinepub.com

Lindsay Nester

International Sales and Marketing
lnester@pipelinepub.com

Judy Porter

Account Manager – North America West
judy@pipelinepub.com

Christina Graves

Account Manager – North America East
christina@pipelinepub.com

Joe Golarz

Account Manager – North America Central & Latin America
joe@pipelinepub.com

Letter from the Editor: February 2016



"My restless, roaming spirit would not allow me to remain at home very long."
— William "Buffalo Bill" Cody

When I think of the most glamorous, idealized version of the American "Wild West," my mind goes to Buffalo Bill. He lived the iconic western experience—he was a Pony Express rider at age 14, fought in the American Civil War, and was a civilian scout during the so-called "Indian Wars."

While not every aspect of his early adult life was above reproach when viewed through a modern lens, it's what he did next that truly stands out as his major contribution to the myths of the American West.

Bill packaged up the glossiest, most romantic elements of the western experience—horsemanship from members of the Pony Express; stagecoach robberies; bloodless battles—and made them a part of a traveling show that drew in millions of spectators through the years. He toured Europe and met Pope Leo XIII. He introduced the world to Annie Oakley and Calamity Jane. He set up an independent exhibition in the shadow of

the famed Chicago World's Fair and drew in countless spectators. His exposition was responsible for honoring the legendary west while simultaneously creating many of the Wild West tropes we still imagine today.

Why was Buffalo Bill so successful; and what on earth does he have to do with mobile communications and entertainment? He was successful, in part, because his show was a safe, convenient way for the average resident of New York, Boston or London to transport themselves to the unconstrained, mythic, unfettered west. He wasn't selling a show; he was selling freedom. For the duration of his show, the audience was no longer penned in by crowded streets, stark factories and filthy gutters. They were running, full speed, across the open terrain of the great beyond.

Is this an overly grand metaphor for what mobile communications offer to the average subscriber? Maybe, but not by much. Buffalo Bill couldn't remain at home for long, he says, but he traveled the world surrounded by all the trappings of home. He brought the Wild West to the people; but in doing so, he was also constantly enveloped in a slice of the life that had become familiar to him in his unfettered youth. And that's sort of what we all want, isn't it? We want to be free to do what we want, but not without sacrificing certain comforts of home.

The promise of mobile communications has, from the start, been the idea that you can go anywhere without severing your ties to certain comforts. Your restless, roaming spirit can see the world... but you don't have to miss an episode of Top Chef. Maybe that's not as glamorous as roping and riding and feigned gunplay; but while Buffalo Bill might have changed his spectators' afternoons and inspired their imaginations, mobile technology is changing our daily lives in an increasing number of ways.

This issue of Pipeline explores the modern realities and emerging promises of the mobile experience. We hear from AT&T on the ways in which millennials are changing the mobile landscape, and look at the impact of mobile communications on the enterprise space. We explore the state of the small cell and talk about how the quest for content is shaping M&A activity. We discuss wireless security, mobile gaming, automated infrastructure management, and the state of mobile voice communications. We also touch on business transformation and bring you lots of other news and opinion from the world of integrated communications and entertainment (ICE) technology. Enjoy, and stay wild.

A handwritten signature in black ink that reads "Tim Young". The signature is written in a cursive, flowing style.

Tim Young
Editor-in-Chief



AT&T's millennial mobile experience

BY VISHY GOPALAKRISHNAN

It's 2016. The network is on demand. Your office is mobile. The cloud is highly secure. And your smartphone may even be surgically attached at this point – sometimes, it's hard to tell. We've grown more dependent on technology for work and our personal lives. As the workforce becomes more mobile and connected, Millennials are surging into it. They're fueling the growth of mobile workers. Our mobile workforce should see an **increase** from 96.2 million in 2015 to 105.4 million in 2020.

Fresh Eyes, Fresh Perspectives

Don't be afraid of those who question you. Fresh eyes and fresh perspectives can help point out inefficiencies. What was once the best, can now be better. My teams – and, I'm guessing, many of your teams – are getting some fresh perspective from our Millennial colleagues. They now make up 27% of my colleagues at AT&T. By 2020, they could make up 50% of the U.S. workforce.

As tech-savvy as those of older generations may be, Millennials remain “digital natives.” They have never known a world without personal computers, cell phones and Internet. They rely on technology to fulfill basic social needs. Technology also gives Millennials the voice required to help create change.

Millennials are calling for major changes in the workplace and looking to technology to make this possible. They want remote work options, flexible hours, and more intuitive communications tools. These desires are pushing their employers toward a more efficient, more intuitive – and more mobile – work experience.

With their fresh perspective, Millennials are spotlighting processes that have room for improvement. Whether pulling the team toward a cloud-based file storage and sharing system, campaigning for email or text voicemail delivery, or wondering why one system doesn’t work with another, they’re asking questions. And these questions point toward all-in-one, collaboration solutions.

Evolution of Collaboration

Our default business processes rely on using separate communication tools for each function. We hardly realize its inefficiency. Take a conference call, for example. One person takes notes in a Word document, shares it via email, and each participant breaks off to complete their tasks. At the follow-up, each person has to separately open the notes and check off what they’ve done. Then they can update the group. I’m exhausted just typing it... And this process can easily take up half – or more – of the meeting. It’s the default process, but it doesn’t have to be.

Without Unified Communications and Collaboration (UC&C) solutions, your working materials and your conversations may be disparate. Your files may be in your email, your shared drive, your conference call system, your colleague’s computer, your video conference rooms – they’re potentially everywhere. UC&C solutions make “picking up where you left off” possible. Your materials are available in the same place you “go” for calls, video chats, IM and email. And since file access functions unite with communications functions for many platforms, you can tie together documents with relevant communications context (like email chains, calendar reminders, IM conversations, and recorded video or voice calls).

When UC&C operates in the cloud, these capabilities are available on-the-go, just as accessible from a mobile device as from a computer. And when UC&C is fully adopted and

Millennial communication habits pull us toward more flexible workplaces.

implemented, a team’s collaboration will look very different than it did 10 years ago.

Changing the Way We Work

With time, UC&C will help revolutionize the inevitable weekly team update. More than any other generation, Millennials are on-the-go. Work will fit more conveniently into Millennials’ busy schedules. But for now, how do we make progress toward all work materials available virtually wherever, whenever, from whichever device? Here are the first steps:

1. We’ll see a drop in voice calling, and an increase in IM and video calling. **Nearly half of Millennials feel more comfortable communicating electronically than face-to-face or over the phone.** “Talking” means more than just speech. It is increasingly visual for Millennials. And the amount of visual clues needed may change over the course of a conversation. Millennial workers embrace collaboration tools that let them switch conversation modes. What starts as a simple question via IM, may require a more detailed answer over a video call. I believe video will become the new voice.
2. **Mobile offices will become increasingly common. Millennial communication habits pull us toward more flexible workplaces.** That’s good news for those of us who like to work from home or have colleagues cross-country. **Nineteen percent of Millennials say that flexible working hours are most important, second only to training opportunities.** Access to information and communications modes from any device will be a must.
3. **Work will shift toward assembling the best team, no matter their locations. Sixty-five percent of Millennials say that rigid hierarchies fail to get the most out of employees.** Access to UC&C capabilities means HR

departments can re-align to focus on assembling teams that work well together, regardless of who sits where. To respond to dynamic business demands, teams will assemble quickly and virtually from all corners of the country—or even the globe.

4. Millennials will not just want, but need their IT departments to be innovative and collaborative. They have grown up in a “beta world”, and are comfortable with working around tech problems. Millennials also have little patience waiting for the next functionality. IT will need to stay on their toes to offer Millennials highly-secure, business-ready, user-friendly options.

5. Finally, collaboration will happen on a global scale. Today’s businesses have to be able to communicate across platforms and over geographical boundaries. They need to connect with colleagues, partners, suppliers and customers from their mobile devices, which they can do using both internal and external collaboration tools.

Growth in Mobile Collaboration Will Guide Providers

Changing the way we communicate and collaborate in the workplace will require changes from everyone involved. Networks, service providers and carriers will all have to reassess. The communications modes that Millennials favor are far more data-intensive than traditional emails or landline phone calls. In order to reach this level of collaboration, carriers and infrastructure will need to step up their game:

1. Networks and infrastructure providers will need to accommodate more video traffic and more real-time communication, such as IM and presence tools. Millennials have shown that they prioritize access to technology and reliable broadband, and are willing to switch providers if their service is sub-par. Connectivity and QoS will need to remain high and consistent.

2. Service providers will need to build with the future in mind. New collaboration solutions rely on strong connectivity and high-capacity networks to keep traffic flowing smoothly and quickly. In the last 8 years **AT&T’s network** has seen a traffic increase of 100,000%, driven largely by video. As more and more work conversations shift to video, networks will have to expand. We’re planning to shift over 75% of our network to software-defined networking technologies to meet the demands of data and video users. We’re already servicing millions

of wireless users this way, and we see it as the **basis** for 5G networks and beyond.

3. Security will be imperative. Millennials experience “FOMO” (fear of missing out, for the rest of us) in their professional as well as personal lives. Sharing information back and forth is routine. IT departments and carriers will need to help ensure that this sharing is safer. We’re addressing this with AT&T NetBond®, which extends VPN and isolates traffic to and from the cloud.

4. Hardware, software, and network providers must all work together. Interoperability between solutions “stacks” will become a “must have.” Millennials expect apps within a given piece of hardware (such as a smartphone) to “talk” to each other and share data. They’ll expect the same from their collaboration solutions. Whether communicating between departments, offices, or other companies, using a different solutions provider should not be a barrier to the act of collaborating.

Road to the New Collaboration

With so much potential to change the way we work, solutions providers are racing to help customers embrace new technologies and collaboration tools. We’re working with established best-in-class partners to offer UC&C solutions that fit each customer’s needs, equipment investments and budget.

Above all, these tools are transforming the office from a place to a state of mind. We’re getting closer to working from wherever, whenever. Work will better fit into our lives, rather than requiring a distinct 9-to-5 block. For Millennials on-the-go, collaboration solutions will connect them to work on their schedule, with access to files, real-time communication and face-to-face video conversations with colleagues from virtually any device. With emerging technology solutions, Millennials may finally be able to have work that revolves around them.





The Road to TRANSFORMATION

BY SCOTT ST. JOHN

If you think about it, service providers should be transformation experts by now. Remember, we're talking about an industry today that was, just 20 years ago, a monopolistic, government-controlled utility. I can't think of any other industry that has to contend with as many monumental shifts, with such frequency, that have had such a fundamental impact on their business.

Milestones and Game Changers

In the U.S., the 80's saw [the final break-up of AT&T](#) into 8 separate, but still closely-regulated, entities: the introduction of the first consumer wireless service and the dawn of the commercial Internet. In many ways, this laid the groundwork for the modern telecommunications landscape. The breakup of AT&T led to new competitive markets, the introduction of wireless services un-tethered voice communications from fixed-line service, and the introduction of the Internet paved the way to mass digital communication and commerce.

The 90's saw the [deregulation of telecom](#), the introduction of new calling features (e.g. call waiting), the advent of Wi-Fi, Voice-over-IP (VoIP), Internet Protocol Television (IPTV), the launch of the Iridium satellite network, and the adoption of commercial and consumer broadband. These were the catalysts for innovation, enabling [new competition](#) across traditional boundaries. The Internet had now entered the homes (e.g. DSL and Cable) and businesses (e.g. ISDN and T1) of mainstream consumers ushering in an [era of competition](#) and consumer demand that created an environment so fierce, many service providers struggled just to keep up.

This era of IP transformation changed the game, entirely. Cable companies were now offering telephone service (VoIP). Telephone companies were now offering video service (IPTV). Both were offering broadband Internet to residential and business customers. New competitors began to emerge, offering PC-to-PC and PC-to-Phone telephone services using the Internet as the backbone (VoIP).

The Hallmarks of Transformation are Opportunity, Investment, Innovation, and Fuel.

We also saw the launch of cloud sites and applications during this time such as Ebay (1994), Napster (1999), and Salesforce.com (1999). And quietly, wireless services began to take root, dropping in price and increasing in popularity – including the birth of a cult-like Blackberry community. Wireless subscribers would grow from 5 million in 1990 to 100 million by the year 2000; and virtually every public place was becoming speckled with mobile users more entrenched in their device than their local surroundings.

In the years that followed, we watched the proliferation of mobile computing and the launch of social networking, communication, and sharing sites and software such as Vonage (2001), Skype (2003), LinkedIn (2003), Facebook (2003), YouTube (2005), Twitter (2006), Netflix (2007, streaming service) and Dropbox (2008) – culminating with the launch of the iPhone in 2007 and followed by the iPad in 2010. We witness the mobile boom, the phenomena of “cord cutting,” and the erosion of the traditional communication revenue streams. The demand for data was insatiable; the need for ubiquitous connectivity became an absolute necessity.

To keep up, service providers deployed a smattering of fixed and wireless operational infrastructures. DSL gave way to Fiber. 2G evolved to 3G. An IP Multimedia Subsystem (IMS) was introduced as an evolutionary path to all IP-based wireless network architecture. 4G was introduced to meet customers growing need for speed, proselytizing the hopes of 1 gigabit per second peak rates of data transfer for mobile consumers. Speed became a competitive differentiator and the 4G brand war ensued. LTE began to appear as a “better than 3G but not quite 4G” caveat to overzealous marketing claims. Soon, the rafters of factories, office buildings, coffee shops, and arenas became littered with wireless routers and small cells. The skyline obscured with cell towers.

By the end of this year, **6.4 billion connected devices** are predicted to be in use and **mobile payments** are expected

to reach 617 billion dollars worldwide, according to analyst firm Gartner. Not too shabby for what started out as a stodgy old utility.

Hallmarks of Transformation: Opportunity, Disruption, Innovation, and Fuel

Regardless of where you are in the world, this transformation is continuing to occur. The Digital Age now spans virtually every corner of the globe and, arguably, the only thing that differs is where you are in the transition. But if we look at the transformative journey itself, there is a certain commonality that can be derived and applied to almost every scenario. If you are just beginning or restarting this journey, perhaps these key learnings that can be applied to navigate the pitfalls, overcome the hurdles, and avoid the mistakes of those that have successfully navigated this path.

In the former example, the break of AT&T and subsequent deregulation of the telecommunications market spurred new opportunities. As did the introduction of wireless services and the Internet. These new opportunities were transformative changes that spurred unbridled competition. The discord, collaboration, and transformation that followed lead to the advent of such innovative technologies and applications that it redefined how we communicate as a global society. This transformation continues to be fueled by communication, collaboration, and commerce – things so fundamental that they have been at the root of every human society that has ever been recorded.

Whether we're talking about a mother buying groceries with a mobile phone in Africa, a millennial catching up on their favorite show on the way home from work, a soldier in Afghanistan video calling his family at home, or an automated emergency dispatch call from a connected car – this technical evolution now touches all of us and it would not have been possible without the opportunity, transformation, innovation, and fuel that occurred along the way.

In fact, this transformative path may be more of a cycle which can be applied to new transformations and reapplied to environments prone to change. If we look at the stabilization of political climates and deregulation throughout parts of Latin American and Asia, the transformation is just beginning. But, if you look at more mature markets such as the U.S., Europe, Japan, and South Korea – there appear to be subsequent cycles of transformation around each new innovation. By looking into the state of global digital transformation today, perhaps you can gauge where you are in this cycle and even contemplate what's ahead.

Global Perspectives

When CSG International commissioned *Pipeline* to conduct a global survey of service providers to gauge their state of digital transformation we were certainly intrigued by the opportunity to pull back the curtain and gain a perspective from inside the companies that have been and are struggling to transform. *Pipeline* collected responses from key decision makers within service providers from every major market spanning all stages of transformation. However, the results were remarkably uniform and provided keen, invaluable insights into the state of transformation today.

“So many opportunities in life come from being in the right place at the right time,” Ken Kennedy, CTO of CSG International provided in a statement to Pipeline regarding the survey results. “When it comes to offering digital services to consumers on-the-go, the communication and entertainment services industry is in a state of transformation to capitalize on the ‘right place, right time’ opportunity.”

Opportunities

The availability of high-speed, reliable bandwidth and connectivity has opened the door to a new realm of possibilities. The majority (73 percent) of service providers surveyed indicated that they anticipate all or most of their services to be digital within the next three years. Industry leaders, such as CSG International have called this reaching DSP state, or becoming a Digital Service Provider. The survey revealed a 17 percent increase from those that have reached a DSP state today and those that plan to within the next three years. This illustrates significant growth in a very short time frame, indicating an aggressive focus on digital transformation by key service providers globally.

At the same time, wireless connectivity has become more pervasive and embedding that connectivity into devices has become less expensive. This has led to a boom in connected devices, encompassing Machine to Machine (M2M) and the Internet of Things (IoT). [According to research firm IDC](#), the IoT market is predicted to exceed 7 trillion dollars by 2020. The majority of service providers indicated that they view the M2M/IoT opportunity as having the most significant revenue opportunity in the next three years.

Respondents also indicated vertical growth into new markets as a key, short-term revenue growth opportunity. Partly fueled by the proliferation of connectivity and new

A recent Pipeline survey indicates service providers are acutely aware of the opportunities in front of them.

connected devices, it seems service providers globally are also exploring where they can add unique value outside of the traditional enterprise and residential industries they serve: industries such as healthcare, finance, smart grid, shipping, and so on.

Cloud services also ranked highly with service providers related to its revenue growth potential. In particular, offering cloud-based business services, which suggests that service providers see a significant growth opportunity to expand revenues from their traditional enterprise business by extending cloud-based collaboration, communication, and infrastructure solutions.

Disruption

If we look at the areas where service providers plan to invest in the next three years, it appears to be directly related to competition and innovation initiatives. This is to be expected as these new opportunities spur change, competition and subsequent transformation cycles.

An overwhelming majority of service providers who participated in the survey (nearly 70 percent of responses) indicated that investing in creating a differentiated multi-device experience was a top priority in the next three years. As connectivity itself continues to become commoditized and the number of connected devices continues expand, ensuring a consistent, quality, and unique experience across these devices – such as homes, phones, cars, and computers – is critical, and perhaps a little obvious. How service providers plan to do so, however, is most likely the bigger question.

In a related press release Kennedy also stated, “While CSPs cited offering services across devices as a key investment area, they also acknowledged that there is much work to be done to align systems and processes to create a truly differentiated digital service experience. We believe that the combination of cloud-based systems that provide a faster

route to monetizing digital services along with specialized expertise in aligning processes, systems and resources are the keys to transforming the entire organization to fully capture the revenue opportunities of the digital era.”

Not surprisingly, the next highest investment priority area was optimizing and consolidating IT infrastructure to reduce cost and complexity. Convergence is essential to differentiation, as it can be defined in this context as the ability to collectively leverage their systems, infrastructure and data – in a cost-effective, automated and accurate way – to create innovative new services and a differentiated customer experience. If done properly, of course.

Lack of agility, lack of integration, and updating existing systems topped the list of transformation challenges. Only 28 percent of respondents indicated that their current support systems could support next-generation digital services, and 52 percent indicated that their in-house teams lacked the right knowledge and expertise. An overwhelming 76 percent indicated that they lacked confidence their internal teams could simultaneously support both existing infrastructure and digital transformation. This is indicative of the discord transformative change creates and opens the door to collaborative partnership to augment skills and re-purpose existing resources.

“The survey findings indicate that service providers worldwide are struggling to capitalize on revenue growth opportunities while taking strides to transform their business model to become DSPs. We expect that the dual priorities of running both today’s and tomorrow’s business models will continue to squeeze CSPs and drive a new need for the expertise needed to transform a very complex business model,” Kennedy added.

Nearly (97 percent) all survey respondents indicated that they would find value in collaborating with a third-party, managed service provider like CSG International to help them with their transformation. The vast majority of respondents (68 percent) currently rely on third parties, and 56 percent indicated they are either considering using or increasing the use of third parties. Not surprisingly, service providers stated they would add the following skills to augment their existing teams to support the transformation to a DSP state:

1. IT infrastructure and business process alignment,
2. Customer experience management (CEM), and
3. Billing and other BSS systems support.

These correlate directly with the investment areas indicated earlier in the survey, as service providers try to capitalize on these new, short-term opportunities.

Focusing on Innovation

Respondents also indicated a concerted focus on innovation, and a reliance on third parties to do so. The vast majority (77 percent) of respondents indicated their organization plans to establish a department of innovation within the next 5 years. The majority of service providers said they would be able to recover 10-50 percent of their team’s time to focus on innovation by leveraging a third-party partner. An additional 13 percent indicated they would recover more than between 50-100 percent of their team’s time to apply toward innovation. Collectively, 67 percent of service providers indicated significant time recovery through the use of third-parties so that existing resources could focus on innovation. Coupling this with the majority sentiment of using and continuing to expand the role of third parties indicates not only a reliance, but a dependency on third-partners to innovate.

Fueling Change

The results of Pipeline’s recent survey indicate service providers are acutely aware of the opportunities in front of them. Literally, trillions of dollars could be up for grabs. The winners will be those that can quickly transform to embrace this change. For many, it seems that the reliance on third parties to help manage existing systems, add additional expertise, and help to integrate technology, strategy, and processes is essential. But, this is just the beginning.

Fueling the demand for next-generation digital services will be paramount to success. Augmenting resources to focus on innovation is arguably table stakes already. The key will be bringing in the right expertise so that service providers can collectively leverage their unique systems, infrastructure, data, and access to content to deliver a truly unique experience across devices. This is the catalyst that has the potential to increase demand and continue to fuel innovation.

For more information about the Global Business Transformation survey, or to download the survey materials, [click here](#).



THE SIGNALING



SECURITY PROBLEM

BY ILIA ABRAMOV

Mobile World Congress 2015 was a record-breaking event, with more than 94,000 attendees and 2,100 exhibitors convening in Barcelona for the tenth year in a row. As we head into this year's conference, a number of sessions and discussions around emerging mobile trends will all echo a resounding sentiment that reflects the conference's theme: "Mobile is everything." After all, mobile technology continues to enter, dominate, underpin, partner with other industries and enterprises at an unstoppable speed.

So it's no surprise that 2016 will also be a transformative year for more connected opportunities. With this evolution towards the "connected everything" world, comes more sophisticated hackers and fraudsters, which demonstrates vulnerabilities and weaknesses in once secure networks. In addition, innovation brings about a focus on data privacy, which has – and will continue to be – a major topic as we head into this year's MWC show (and beyond).

One security hot topic which received widespread publicity in 2015 is the vulnerabilities associated with SS7 Signaling,

Hackers with a moderate level of technical skill and malicious intent can easily exploit the mobile network and its subscribers.

as well as other signaling protocols such as SIP and Diameter. Although designed as ‘trusted,’ the network is not always as secure as was earlier believed. Potential threats to signaling systems, like SS7, are increasing across many sources, and continue to be exploited by fraudsters and hackers with ill intent. Recent news articles have revealed that unauthorized access to the network is not only possible, but easier than ever before.

This unauthorized access leaves mobile networks vulnerable to fraud and misuse, shaking consumer trust in the operator’s ability to provide privacy and prevent fraud. To date, loopholes in the SS7 protocol have been exploited to steal money, listen in on conversations, monitor messages, track a subscriber’s location, manipulate network and subscriber data, and generally disrupt services.

Given that there are more users of the SS7 network worldwide than there are of the Internet, concerns about SS7 security by operators and subscribers alike is widespread, serious and should be treated with utmost importance.

As you catch up with fellow MWC attendees and listen in on different sessions at this year’s conference, here is a brief history of mobile security, SS7 vulnerabilities and how you, the mobile industry’s most influential leaders, can help solve this emerging problem.

A Vulnerable History

Signaling networks have gone through multiple stages of evolution. Originally, SS7 networks were specific to mobile operators and required specialized equipment to arrange for simple connectivity on a physical layer. This closed circle of users combined with overall complexity of protocols ensured very controlled access to signaling

networks, making it nearly impossible to obtain access to a SS7 network through a remote, unauthorized host.

However, as early as 2008, SS7 vulnerabilities were openly discussed at the [Chaos Computer Club Conference](#) in Germany. A German researcher demonstrated how the location of a mobile phone could be determined. We now know, prior to that, telecom engineers warned of possible risks; even high-level government officials were aware of the threat and voiced concern. Again, in 2013, these issues came to light when it became known that a network had been exploited for surveillance purposes and exposed SS7 vulnerabilities.

While the technology dates back to the 1970s, the process of placing voice calls on modern mobile networks is still based on the same SS7 technology. New signaling transport protocols known as SIGTRAN are deployed, which allows SS7 to run over IP. The ultimate goal of SIGTRAN was to move from converged TDM/IP network to an all IP network, taking advantage of bandwidth, redundancy, reliability and access to IP-based functions and applications.

Additionally, newly-deployed 4G networks use the same concept of an all-IP network and have adopted Diameter as the signaling protocol that runs over IP. The technological concept for providing end-user services within the Evolved Packet Cores (EPCs) enables similar procedures as SS7-based networks.

Yet, moving onto IP has not resolved the issues; it has, in fact, unfortunately provided new points of vulnerability. Important information has become exposable beyond the circle of trust within mobile operators, and the risk of privacy intrusions can quantify in the millions, depending on the case. This can lead to huge damages not only to the operator, but also affect direct revenue due to the loss of VIP customers, enterprise customers and legal exposures.

The Central Nervous System of the SS7 Network

Think of the mobile network as the human anatomy. Signaling is the central nervous system of the mobile operator’s network, with mission-critical real-time data on subscriber identity, status and location traversing the network. This data enables the authentication of subscribers and their devices, performs call setups, authorizes charging, enforces data policies, manages quality of service and enacts roaming or interconnection agreements. Gaining access to such pertinent information can be extremely beneficial for commercial purposes, but it can also be very risky if used by the wrong people.

Hackers with a moderate level of technical skill and malicious intent can easily exploit the mobile network and its subscribers. Hacking into networks is not as nearly as difficult as we had previously thought, proving in today's world that keeping the mobile network secure is pertinent for both public safety and privacy.

How it Happens

Attackers with the right expertise build nodes to emulate network elements while acting within a mobile network or on behalf of the network. Simulated elements range from Base Transceiver Stations (BTSs) to Mobile Switching Centers (MSCs), Gateway GPRS Support Nodes (GGSNs) to Short Messaging Service Centers (SMSCs). While location data is used by the operator to perform certain legitimate and acceptable functions (think of mobile banking services), the IP as transport layer was not designed to detect acceptable versus unacceptable traffic. There are a number of entry points in a Signaling network which can be exposed at various levels.

With each exploitation, hackers have specific goals for targeting subscribers. For operators, it is important to recognize these threats before they become full blown attacks and result in business revenue loss, customer dissatisfaction and fraud.

Solving the Signaling Security Problem

The mobile ecosystem has begun to define recommendations, building and implementing solutions to detect and prevent potential attacks. Operators need a solution that is easy to deploy yet comprehensive, and ideally one that overlays the existing architecture. That means integration should be flexible and eliminate the need (and expense) of redesigning the underlying signaling network architecture. The objective is not to merely block suspicious traffic but to use global threat intelligence and advanced analytics to secure the network against privacy and fraud attacks.

Simplistic IP firewall protection methods are not sufficient to detect and resolve the large majority of these vulnerabilities. Instead, a comprehensive layer-distributed solution in the form of a signalling firewall is required. The firewall should contain a powerful rules engine that enables screening of traffic by exposing parameters from all relevant SS7 stack layers for comparison and validation between each other and preconfigured parameters combined with the techniques mentioned above. It must also address not only today's threats but be sufficiently flexible and dynamic

to be capable of addressing those that are yet to come. Ideally, the solution would provide an easy to use interface, real-time access to information, predefined and just-in-time filters and underlying support from a world-class data engine.

Given that mobile communications is a prime target for hackers who desire to penetrate critical infrastructures and businesses, operators need to be aware of the types of attacks and tools that are used by spammers, scammers and fraudsters, but also show how a network can be audited and protective measures put in place quickly before subscribers, organizations, and even governments fall prey to misuse and are severely impacted.

As a community convening on this year's Mobile World Congress, it is imperative that we continue to build out our mobile ecosystem, working together to build critically needed solutions and put protection in place.



2016
INNOVATION AWARDS

NOMINATE YOUR COMPANY
SPONSORSHIPS AVAILABLE

CLICK HERE >

THE
RETURN
OF THE
SMALL
CELL



Not long ago, in a galaxy not far away – in fact this one – small cells made their first appearance on the scene. In a 3G network, small cells were primarily used for in building coverage where it was needed. It was an important role, but not a glamorous one.

According to Stefan Pongratz, Senior Director of Carrier Economics and Mobile Radio Access Network (RAN) Market Research for Dell’Oro Group, the business case for 3G small cells in 2016 and beyond will remain meager, with 3G small cells expected to account for less than one fifth of the small cell market by 2020.

So what awakening in the force is calling for a return of the small cells now? First, the demand for mobile data took over the world, leaving operators with overloaded networks and scrambling to add both coverage and capacity. Rolling out LTE networks for mobile traffic was the first step, but these networks are already being strained.

Strategy Analytics predicted in its report, [Mobile Data Traffic Forecasts 2014-2018](#), that by 2018 mobile networks will carry 56.2 Exabytes of data, up from 21.3 Exabytes of mobile data traffic in 2014. This growth in traffic is being driven by both strong performance on 4G/LTE networks and rapid growth in smartphone data subscriptions, with future growth driven by tablets, consumer electronics and M2M devices contributing to a larger share of the total data traffic.

There are a number of ways that operators can add capacity to their networks, including acquiring new spectrum, which leads us to our second point – LTE spectrum is both scarce and expensive. Mobile operators are turning to a Heterogeneous Network model – or HetNet – to maximize their spectrum. A HetNet is composed of a combination of macrocells, Wi-Fi, distributed antenna systems (DAS) and small cells. By using a layered network model with deployed small cells, mobile operators not only address coverage concerns between macrocells and in indoor environments, they can also add much needed capacity to the network and improve the overall end user experience.

Provisioning Small Cells

The addition of small cells to the mobile network adds complexity when it comes to RF network planning as compared to a macrocell-only network; therefore, efficient and autonomous coordination between macrocells and small cells is key.

Self-organizing Networks (SON) techniques provide the real-time self-configuration, self-optimization and self-healing capabilities that are becoming mandatory features for the HetNet to work as a cohesive network. SON offers the promise of reducing costs in initial rollouts, enabling more effective coordination of time and frequency resources, providing dynamic interference management, and adapting to changing network conditions.

Interference Management and Carrier Aggregation

Mobile operators are deploying LTE-Advanced capabilities such as carrier aggregation and interference management techniques to make their networks even more efficient. Here again, small cells remain critical to operators’ overall strategy as they provide additional capacity in dense indoor environments where a majority of data traffic will be generated.

In a HetNet scenario combining small cells with Wi-Fi and macrocells, mobile operators are rolling out a number of interference management techniques to ensure the network is optimized for capacity and coverage.

- **Enhanced Inter-cell Interference Coordination (eICIC)** works as the interference manager for small cells as part of a HetNet. It uses advanced time domain scheduling to reduce radio interference and increase the coordination between network cells to ensure a streamlined flow of information.
- **Multiple Input and Multiple Output (MIMO)** is an approach which serves to increase efficiency across the spectrum by leveraging smart antenna technology that analyzes how base stations, antennas and user equipment communicate.
- **Coordinated Multi-Point (CoMP)** is a technique that ensures that even greater performance is achieved at the edge of the network, by increasing coordination between small cells, and between small cells and macro cells.
- **Relay Nodes** are low-power base stations that reduce the site-to-site distance in the macro network. They were added to the LTE Release 10 specification.

Mobile operators are currently focused primarily on deploying eICIC and MIMO. Relay nodes add additional complexity to the network and will be rolled out at a later date.

Carrier aggregation aggregates mobile operators’ 3G spectrum freed up by LTE roll-outs along with LTE and LTE-Advanced spectrum to add increased throughput to the

Small cell revenues will account for 16% of the total RAN market by 2020.

network. The scarcity of spectrum has led to faster adoption of carrier aggregation by mobile operators as compared to other LTE-Advanced capabilities. Carrier aggregation is also being used for both LTE-FDD and LTE-TDD modes, allowing mobile operators with both network assets to adopt the technology to gain even more performance.

Carrier Aggregation and LTE-Unlicensed

One of the biggest innovations in driving the return of the small cells is LTE-Unlicensed technology, also known as LTE-LAA (LTE-License Assisted Access). Mobile operators are beginning to aggregate unlicensed spectrum in the 5 GHz band with their available licensed spectrum to add even more bandwidth.

As LTE-LAA is an extension of LTE-Advanced and is based on carrier aggregation, it's no surprise that small cells remain central to its deployment. Leveraging small cells for LTE-LAA provides a localized approach to carrier aggregation that helps mobile operators co-exist with the Wi-Fi community, while being able to further maximize their spectrum to increase capacity and coverage and ease network strain. Small cells are also suited to deployment in the LTE-LAA 5 GHz band as they are better suited to the band's low power requirements as opposed to macrocells.

LTE-LAA is expected to be fully standardized in 3GPP Release 13, currently planned to be finalized in 2016.

Breaking Down the Numbers

Dell'Oro Group has forecast that small cell RAN revenues will account for 16% of the total RAN market by 2020. According to Pongratz, "the indoor enterprise/public access market improved significantly in 2015, though outdoor revenues still account for the greatest portion of revenue. We expect the indoor segment to grow at a quicker pace and expect the revenue split between indoor and outdoor to be closer to

50/50 by 2020." And 5G small cells will account for close to 5% of the small cell market by 2020.

Deployments Around the World

A large proportion of the world's small cells have been deployed in Asia Pacific in Korea and Japan, with volumes picking up in China and India. In dense environments, mobile operators are deploying enterprise and residential small cells in indoor venues to add capacity locally, with the potential for a 1-to-4 ratio of macrocells to small cells.

Outdoor picocells will most likely leverage a Cloud-RAN architecture and will roll out in 2017. Cloud-RAN deployments are now out of the proof of concept stage and are currently in trials. These cloud-based access points, which are also known as virtual base stations or C-RANs, will form the base of a 5G network architecture. They will handle not only the voice and data traffic for consumers, but will also support the M2M and IoT applications that form the 'connected network' of the future.

The majority of small cells will be multi-mode, supporting both LTE and Wi-Fi in the 5GHz band, allowing operators to take advantage of cost savings due to leveraging unlicensed spectrum. By supporting the 5GHz band, mobile operators can also deploy LTE-LAA on the same small cell. .

Critical Lessons Learned

Each small cell deployment is unique – and what happens in the lab is never replicated exactly in the field. In addition, we learned that focusing on data speeds in trials wasn't enough. In real-world deployments, it's more important to make sure that the small cells gel with the network from all angles and not just provide the required data speeds.

Mobile operators also need to plan for more than just mitigating interference between small cells and macrocells. They also need to mitigate issues associated with small cell placement and acquiring the necessary real estate. This needs to happen early in the planning process to ensure a smooth roll-out.

Small cells have returned in a big way. From a role of just filling coverage gaps in 3G networks, small cells now form a major part of mobile operators' strategy as they contend with exploding mobile data traffic on their networks and chart their path towards 5G. It's all about adding capacity efficiently and economically. Now that the small cell force has awakened, we can't wait for the next sequel.



WIRELESS SECURITY STANDARDS

BY: ALAN ZEICHICK

Security standards for cellular communications are pretty much invisible. The security standards, created by groups like the 3GPP, play out behind the scenes, embedded into broader cellular protocols like 3G, 4G, LTE and the oft-discussed forthcoming 5G. Due to the nature of the security and other cellular specs, they evolve very slowly and deliberately; it's a snail-like pace compared to, say, WiFi or Bluetooth.

Why the glacial pace? One reason is that cellular standards of all sorts must be carefully designed and tested in order to work in a transparent global marketplace. There are also a huge number of participants in the value chain, from handset makers to handset firmware makers to radio manufacturers to tower equipment to carriers... the list goes on and on.

Another reason why cellular software, including security protocols and algorithms goes slowly is that it's all bound up in large platform versions. It's clear that 3G is quite different from 4G, and that 5G is something else entirely. The current cellular security system is unlikely to change significantly before the roll-out of 5G... and even then, older devices will continue to use the security protocols embedded in their platform, unless a bug forces a software patch. Those

security protocols cover everything from authentication of the cellular device to the tower, to the authentication of the tower to the device, to encryption of voice and data traffic. When 5G rolls out (the best estimates are 2020, but who knows?), we'll see new standards.

We can only hope that end users will move swiftly to 5G, because 4G and older platforms aren't incredibly secure. Sure, they are good enough today, but that's only "good enough." The downside is that everything is pretty fuzzy when it comes to what 5G will actually offer... **or even how many 5G standards there will be.**

What's Wrong with LTE?

InHas your phone ever wanted to update its "carrier settings?" That may be a reaction to a flaw in cellular security, either in the design of a standard, or in the implementation of the standard through firmware. One example of a recent flaw was published in October 2015. Called "**Voice over LTE implementations contain multiple vulnerabilities,**" the report from CERT said,

"Current LTE networks rely on packet switching, rather than the circuit switching of previous generations of the mobile

network. The use of packet switching and the IP protocol (particularly the SIP protocol) may allow for new types of attacks not possible on previous generation networks. Such types of attacks are well-known in the security community; for example, see previous attacks against Voice over IP (VoIP).”

The report went on to talk about problems with incorrect permission assignments for critical resources, improper access control, improper authentication, and session fixation (which might lead to denial-of-service attacks on the network).

The CERT report is only one demonstration of less-than-Fort-Knox security model in today’s cellular network. Daksha Bhasker of Bell Canada served up a very detailed paper, “[4G LTE Security for Mobile Network Operators](#),” in which she writes,

“...in reviewing the 4G LTE architecture, the 3GPP, next generation mobile network (NGMN) alliance and international telecommunications union (ITU) have identified security vulnerabilities and recommended mitigation strategies. Consideration and implementation of these security enhancing measures are discretionary to the many LTE stakeholders including MNOs. As a result, the security of LTE networks and services will vary widely between MNOs, subject to the MNOs knowledge of security risks and impacts, the MNOs risk appetite and wallet size among other factors. Speed to market, tight budgets, profit targets, concerns with network performance, business models, network interoperability, regional regulations and business priorities lead to further inconsistencies in security implementation amongst MNOs.”

We could go on and on... but let me point to one more source, a presentation at the RSA Conference in April, 2015, entitled, “[LTE Security — How Good Is It](#),” by Jeffrey Cichonski and Joshua Franklin, both of NIST. The paper presentation identifies several weak spots (and possible attack vectors) in the end-user device, the tower, the network core, and the IP network (i.e., the Internet).

While our focus here is on the OTA security aspects of the device and tower, vulnerabilities anywhere along the chain can compromise the whole system. That includes radios, mesh networks, packet gateways, signaling systems (i.e., the control plane), crypto, subscriber identity, and more.

See slides 25-32, which go into a wide range of possible attacks that would defeat LTE security. Scary stuff.

Cellular Network Security Protocols

There are so many standards, it’s hard to know where to begin. The standards are also embedded within other standards. Let’s take one simple set of protocols: UEA2 and UIA2, which have been around since the early 2000s. UEA2 is an algorithm that defines the confidentiality of communications. Its partner UIA2 specifies algorithms for protecting the integrity of communications. UEA2 and UIA2 are functions used by SNOW 3G, a stream cipher that generates and uses crypto keys – and is used heavily in OTA cellular security.

UEA2, UIA2 and SNOW 3G come from the **3GPP** (3rd Generation Partnership Project), a vast international consortium that defined GSM (i.e., 2G cellular), UMTS (i.e., 3G) and LTE (i.e., 4G) and which is spearheading 5G. 3GPP is truly global, and has driven the cellular industry since 1992. Every quarter, 3GPP releases new specifications. Every couple of years 3GPP releases new protocol sets; sometimes they are major, like 4G LTE, and sometimes they are minor, like the new “[LTE-Advanced Pro](#)” spec that came out in October, 2015, and which might find its way into the global cellular networks and consumer devices in late 2016 or early 2017. Glacial, remember?

Slow and steady wins the race, but threats evolve quickly. There are threats for service delivery, handling privacy, man-in-the-middle. It’s a complex landscape, and all it takes is one exploit to succeed to allow bad actors into the network. In some cases, as mentioned in the papers mentioned above, the weaknesses are in the security architecture and protocols in 4G and older cellular OTA networks.

I suspect that the biggest threat to cellular security is bugs: flaws in the firmware and operating systems embedded into smartphones and other cellular devices, as well as in towers and other carrier equipment.

Given that carriers have direct control over their towers, and can do testing and other QA, my sense is that handset vulnerabilities are the biggest problem facing the industry... well, other than directed attacks against the physical infrastructure.

The Work of the 3GPP on 5G

The 3GPP specifications are numbered according to their general purpose. Modern cellular radios, for example, are in the **25 Series** of specifications. The security work within the 3GPP is broken up into two different series: **33 Series** is for general security, and **35 Series** is for security

algorithms. UAE2 and UAE2 are defined in [35.215](#), and SNOW 3G is in [35.216](#). Browse through the 33 Series and 35 Series specifications, and see links to protocols, reports, studies and more. It's a goldmine of technical information about LTE, much of which, unfortunately, requires a lot of contextual knowledge. Note that some of those links are to industry proposals, some of which were later withdrawn.

The work on 5G is collected in another area called, "[Release 14](#)." Unfortunately, it's very sketchy, which reflects that 5G is still four years away, perhaps more. The 3GPP says that it is committed to release an initial technology submission by June, 2019, and a more detailed specification by October, 2020. We'll see; it's a big job, and a lot of information is not available.

That doesn't mean that we know nothing. One of the major participants in the 5G security work is Ericsson, which put out a [paper on the subject](#) in June, 2015. Ericsson says that that 5G's security will evolve from 4G to focus on four main areas:

- 1. New trust models:** 5G services are expected to serve safety-critical systems, such as in public safety. Devices will explode beyond phones to the Internet of Things (IoT), including shipping containers, industrial controls, and connected vehicles. The report brings up an unpleasant thought: "Devices have so far been assumed to comply with standards and not to deliberately attempt to attack networks. But how well protected are very low-cost devices? Can a single connected device be used as a stepping stone for cyber-attacks deep into the system? And what is the attack surface of a 5G system with billions of inexpensive, connected devices?"
- 2. Security for new service delivery models:** In the 4G and older cellular era, everyone assumed that a cellular end node (like a handset or tower) was a dedicated, proprietary piece of hardware. In 5G, much more will be virtualized through NFV (Network Functions Virtualization) and SDN (Software Defined Networks). New security protocols are needed to isolate virtualized services from each other.
- 3. Evolved threat landscape:** 5G devices will be part of critical infrastructure which will attract new attackers who will go beyond simply disrupting services (like destroying a cell tower). Instead, attackers may attempt to co-opt those 5G devices and networks. This will require stronger protocols for device authentication, user authentication (often clear-text usernames and passwords), and strong cryptography.

The scalability of billions of embedded devices ... is a major challenge within the field of IoT security.

- 4. Increased privacy concerns:** Users are concerned about mass surveillance, and there have been reports of rogue base stations conducting man-in-the-middle attacks. The Ericsson report also mentions the user identifiers for cellular devices, which haven't been updated in a very long time. While there are proposals for replacing new protocols, the study says, "the benefits of full International Mobile Subscriber Identity (IMSI) protection have so far not seemed to outweigh the complexity of implementing it."

More Unknowns than Knowns

While 4G LTE has good enough security for today's smartphones, it's not enough for the future especially when you factor in IoT. We will have new devices and new ways of using those devices. Oh, and scalability will be a challenge as well. To quote from "[Security and impact of the IoT on LTE mobile networks](#)," a pre-publication book chapter by Roger Piqueras Jover of the AT&T Security Research Center:

"As mobile networks evolve and transition towards 5G, the capacity and throughput of the wireless interface is scaled up to tackle the goals of massive device connectivity and 1000 times more capacity. To do so, researchers are already prototyping advanced systems at high millimeter wave frequencies and implementing massive MIMO [multiple input multiple output] systems. However, a common topic of discussion at a major 5G industry forum was how it is not all about speed, but also about scalability. The scalability of billions of embedded devices joining existing LTE and future 5G networks is one of the major availability challenges within the field of IoT security."

There's a lot riding on 5G. We need it, and we need its security. We'll continue to keep an eye on it.

MOBILE IMPACT ON THE ENTERPRISE IN 2016

BY: STEVE FRENCH



Today's connected customers expect interaction with preferred businesses to be three things: quick, easy and secure – and most importantly they want this communication to occur via mobile. As consumers become increasingly receptive to interacting with enterprises through their smartphones, Gartner took it a step further and predicted that by 2020 customers will manage 85 percent of their own relationships with enterprises without any human interaction at all.

As we enter 2016, what does this shift in consumer mindset mean for mobile technology? Below are the biggest ways we believe mobile will impact enterprises and their customers in 2016 – and how enterprises must adapt their mobile technology strategies to succeed with customers. In addition, mobile network operators should consider how they can leverage mobile to improve the experience for their own customers – both consumers and enterprises. This means supporting the mobile requirements and unique needs of their enterprise customers in order to differentiate from the competition and generate new revenue streams.

SMS and Mobile Web Communication Will Beat Out Mobile Apps

There are over **1.6 million** apps available to today's consumers; but quantity does not mean quality, or that the apps are actually being used. In fact, **80-90%** of downloaded apps are only used once and then deleted, according to **Compuware**. Whether it's poor user experience, too much required personal or sensitive information, or app overload; the results are the same: the majority of consumers are not finding enough value in most apps, and thus they are

bypassing or deleting them altogether. With the enterprise challenge of getting customers to find utility in their apps and keep the apps on their smartphones, it's important for companies to adapt and reach consumers where they want to be reached in 2016. The more efficient and direct way for enterprises to deliver information is via text messaging or the mobile web.

People spend an average of **2.7 hours** on the mobile web daily and **90% of text messages are read within three minutes of delivery**. They also prefer to communicate via text – **75%** want to receive offers sent to them via SMS specifically. Given mobile messaging's ability to directly deliver relevant and useful information that will be read within minutes, as well as consumers' preferences for communication via mobile and specifically texting, enterprises will benefit from using both channels. In 2016 we will see companies lessen their focus on mobile apps and increase the mix of mobile web and text messaging – as an optimal approach to communicate with consumers.

Enterprises Will Beef Up Mobile Security With SMS Capabilities

Each year, thousands of security breaches occur around the world – even with the biggest, most established companies. The year 2014 alone resulted in the theft of over **1 billion records of personal identifiable information (PII)**, and consumers are becoming more aware and fearful of personal ID theft. With **17%** of people using their mobile phone for most of their online browsing, it's essential for mobile communication to be secure. In fact, **more than half** of app users have uninstalled or decided to not install an app

due to concerns about their personal information. It's up to enterprises to gain consumers' trust with communication avenues that are safe and protected.

Interestingly, despite mass SMS adoption (**88% of organizations are already using text messaging in some form**); few enterprises have been leveraging its capabilities to increase customer security. By utilizing, for example, mobile pin two-factor authentication (2FA), an enterprise is able to automatically authenticate a user's ID to mitigate the risk of theft of personal information. Taking advantage of SMS for heightened security purposes will be an easy and much needed next step for carriers in 2016.

Mobile Messaging Will Give Call Centers Deep Insights

By communicating with customers via mobile, enterprises are provided with a variety of critical, individualized data – contact and transaction information, and interaction history and information across phone, chat, email, social media and SMS. And what's the best way to interact with consumers? Know who they are and what they like in order to better serve them. In 2016, thanks to text messaging, contact centers will have more valuable 360-degree insights into their customers than ever before. With this information, businesses can turn troves of data from disparate sources into actionable insights to provide customers with a highly-relevant and personalized experience, resulting in increased brand loyalty.

Consumers Will Demand Mobile Customer Service

When it comes to customer service, today's consumers – especially millennials – are more unforgiving than ever. **Eighty-six percent** of customers will quit doing business with a company if they have a bad customer service experience, and just a **1% drop in service is equivalent to a 15% drop in customer satisfaction**. When they do experience poor service, it's easier than ever to post a bad review via social media or review sites to damage the company's reputation. To avoid negative reviews and losing customers, it's important for companies to provide the type of service their customers want. For millennials – who will make up **75% of the workforce** by 2030 – that means receiving information quickly and via mobile.

Millennials hate being told they're a valued customer while having to wait to speak with a representative for an extended amount of time. In fact, they'd rather avoid speaking on the phone altogether. Today, **64%** of millennial consumers prefer texting a company for information versus calling

them, and **77%** of them have a more positive perception of a company they can reach via mobile messaging.

In addition to pleasing customers with quick and efficient communication, companies using mobile messaging-based customer service will be able to manage multiple inquiries at once, allowing them to resolve more inquiries and close customer service tickets at a higher rate. This means companies will have the opportunity to more cost-effectively improve customer retention rates, while creating long-term loyalty and revenue opportunities in the process.

Enterprises must adopt “New Age” communications as consumers look toward Emoji-based mobile messages, increasing their volume by 25% next year. Millennial consumers are ingrained to appreciate the ‘short and sweet’ and personalized – the essence of the emoji. In 2016, more customers will want to interact with enterprises in the same manner. While traditionally thought of as an unconventional business to consumer communication practice, today's consumer has become accustomed to communicating in such a fashion. In fact, while emojis used to be predominantly texted and tweeted by teens, today there are more 25-29-year-olds identifying as “frequent users” (75.9%) than under-25-year-olds (72.2%), according to **Emoji**.

Additionally, more than six out of 10 in the age 35+ crowd self-identify as frequent users. A great example of a business using emojis to engage with their customers is Domino's Pizza, who allows customers to order pizzas by simply texting a pizza emoji directly to the company. The signs are clear: enterprises that don't begin to adopt this practice will lose valuable mindshare with not just the largest generation today – millennials – but also the generation that precedes them. The bottom line in 2016 is that consumers will have a zero-tolerance policy for service that isn't prompt, customized and securely delivered via their mobile device.

To succeed with customers and meet their mobile needs, enterprises will need to focus on mobile web and SMS communication, leverage SMS to increase security, and dive into customer insights provided by using text messaging. By integrating SMS in new and unique ways in the coming year, enterprises have an untapped opportunity to enhance the customer experience and build long-term loyalty. For mobile network operators, there is a clear opportunity to improve their own customer experience and to partner with their enterprise customers to provide more mobility solutions.



THE BIG BET ON CONTENT

BY: TIM YOUNG

Behold: a look at the future, from the past. *“Mobile-phone companies are always trying to sell you the next big thing,”* wrote Rana Foroohar in [Newsweek](#). *“Phones that can stream football games, send you movie clips, download a new song or snap pictures are what beleaguered telecom operators hope will bring in the big bucks over the next few years.”*

She proceeds to discuss how western mobile carriers should look to Asia for profitable business models. The date of that piece? October 19, 2003.

Back to the Future

There are lots of other, fun little nuggets throughout the piece including a quote from Nomura analyst, Richard Windsor, stating that “text messaging is *the* data service at the moment,” a statement that was no doubt true at the time. And it’s interesting to note that even the publication which carried that story has gone, it experienced the effects of the digital business model, famously ceasing publication of its print edition before relaunching it a year later under new ownership.

I present this peek into the past to emphasize the depth of the roots of this fundamental question: how do mobile carriers remain profitable as customer expectations rise, external competition grows, and average revenue per user shrinks? On that last point, here’s a sobering statistic: according to the [CTIA’s semi-annual wireless industry survey](#), ARPU in 2014 for US-based carriers was \$46.64. Back in 2003 when that *Newsweek* piece was written, it was \$51.55. While revenues were close to an all-time high in 2014, CapEx was sky high.

So with all of this context well in mind, major US carriers are looking for the next big bet; and if the last few years are any indication, that means large-scale M&A with an appetite for content.

Big Numbers, Big Bets

AT&T’s acquisition of DirecTV is a good example. The \$49 billion deal was obviously good for AT&T for a number of reasons. It increases the carrier’s ability to offer bundled services, removes a significant competitor, and allows for greater synergy between mobile and fixed offerings. But as

Bloomberg Business pointed out during the merger, there was a major content angle. The National Football League (and that's American football, for our international readers) has had a content distribution deal with DirecTV for years, through which subscribers to the satellite service can get access to every Sunday afternoon game, regardless of where they live. It's been a lifesaver for, say, Buffalo Bills' fans living in Phoenix; but it's even more importantly an incredible source of content for AT&T. DirecTV's extension of the deal was a big consideration in AT&T's acquisition of the company. And the **recent initiatives** to further open up access to Sunday Ticket for streaming customers without DirecTV service is indicative of the merged company's thirst for new revenue streams.

It's not AT&T's only recent content play. In 2014, the **carrier announced an agreement** with the Chernin Group, a privately held media holding company, in which the companies would invest a combined \$500 million to acquire, invest in, and launch over-the-top video services. The joint venture, called Otter Media, has been active. It **recently invested \$22 million** in one of its brands, Ellation, the parent company of anime video service CrunchyRoll (which delivers Japanese programming like Naruto Shippuden and Sailor Moon to western fans and sports 20 million users, including 750,000 paying subscribers).

Meanwhile, AT&T's key adversary, Verizon, is hard at work placing its own huge bets on content. First, it made a series of acquisitions designed to better prepare itself to deliver content: content delivery network Edgecast, encoding company Uplyn, and perhaps most notably, interactive TV platform OnCue which it acquired from Intel. Then it made the big leap by picking up AOL in a \$4.4 billion deal last spring, a move most think was all about picking up AOL's advertising platform.

All of these pieces have gone into the pot, and the resulting stew is Verizon's Go90 service, an over-the-top play designed to reach customers well outside of Verizon's usual subscriber base. AOL's advertising platform—One—brought in a reported \$1.8 billion in revenue in 2014, and if those numbers persist (and Go90 can find an audience), Verizon could be well-positioned to pump up its overall income with the help of new revenue streams.

What's more, the carrier is working very hard to look at video streaming and the resulting ad revenue in very innovative ways. **Verizon hopes** to reach new levels of precision when it comes to customer targeting, and sees an opportunity to reinvent ads and the way that customers experience and interact with them. These are not new promises, but the

maturity of the tools at hand and the carrier's ownership of the value chain mean new possibilities to bring these promises to fruition.

Vertical Integration

Verizon is also demonstrating some long-range thinking for Go90 when it comes to geographical reach. **According to Variety**, AOL CEO Tim Armstrong told the audience at Recode's Code/Mobile conference in October that Verizon wants to become the largest mobile media technology company, which will involve reaching beyond its own network and possibly beyond the US border. He mentioned the possibility of developing partnerships with international carriers, or even white-labeling Go90 in other countries.

This push to operate OTT content distribution channels that distribute content independently from the carrier's other business is a new flavor of an older story. **As Bloomberg's Alex Sherman** pointed out in a piece last summer, cablecos were all about so-called "vertical integration" in the '80s and '90s. Time Warner owned TWC, Time, TBS, TNT, and lots more. Tele-Communications (aka TCI) owned interests in Starz, Discovery Channel, and others. Cablevision owned not only content networks, but also Madison Square Garden. They could theoretically host an event in one of the nation's most notable venues, broadcast that event, and own every part of the value chain.

That model failed, largely because U.S. cablecos (especially at that time) were regional rather than national. Furthermore, the ability to deliver content over-the-top didn't exist at the time, further limiting the value of those channels. But regions don't matter nearly as much in the OTT model, and providers are ready to take another shot.

Traditional partners are ready to come along for the ride. For example, Cisco picked up cloud-based OTT video platform 1 Mainstream late last year. **In a company blog post about the deal**, Cisco pointed out that global cloud traffic is set to quadruple by 2019, and 1 Mainstream will allow Cisco to better assist its customers in delivering new services faster.

With terrestrial competitors like Comcast (and its recently acquired NBC Universal assets) well positioned to deliver content that subscribers want, now is a great time for mobile carriers to leverage their networks—which meet customers where they want to be in an increasingly mobile society—to deliver and monetize content in a new way. These are big bets on content that don't show signs of slowing and we'll be watching in 2016 to see how they pan out.



The **DEATH** of Cellular Voice

BY: CHRIS PIEDMONTE

There are clear indications that we are beginning to see the slow, certain death of cellular network-based mobile voice services. Across the globe, customers are using their mobile devices to access data networks far more than they are to place mobile voice calls. When they do use their mobile devices for voice, many are turning to VOIP services such as [Skype](#), [Viber](#), and retro-POTS gone global upstart [Rebtel](#) rather than the cellular network. Why is this happening?

With the ready availability of IP connections, the improved voice and connection quality of VOIP and the option to augment calls with multimedia messaging, live two-way video and application sharing, mobile VOIP is becoming the communication paradigm of choice. Indeed, the major North American carriers are reporting almost no growth in the number of minutes consumed even while adding subscribers. They are also embracing WiFi calling as part

of their services and concentrating on other data-centric offerings to bolster revenue.

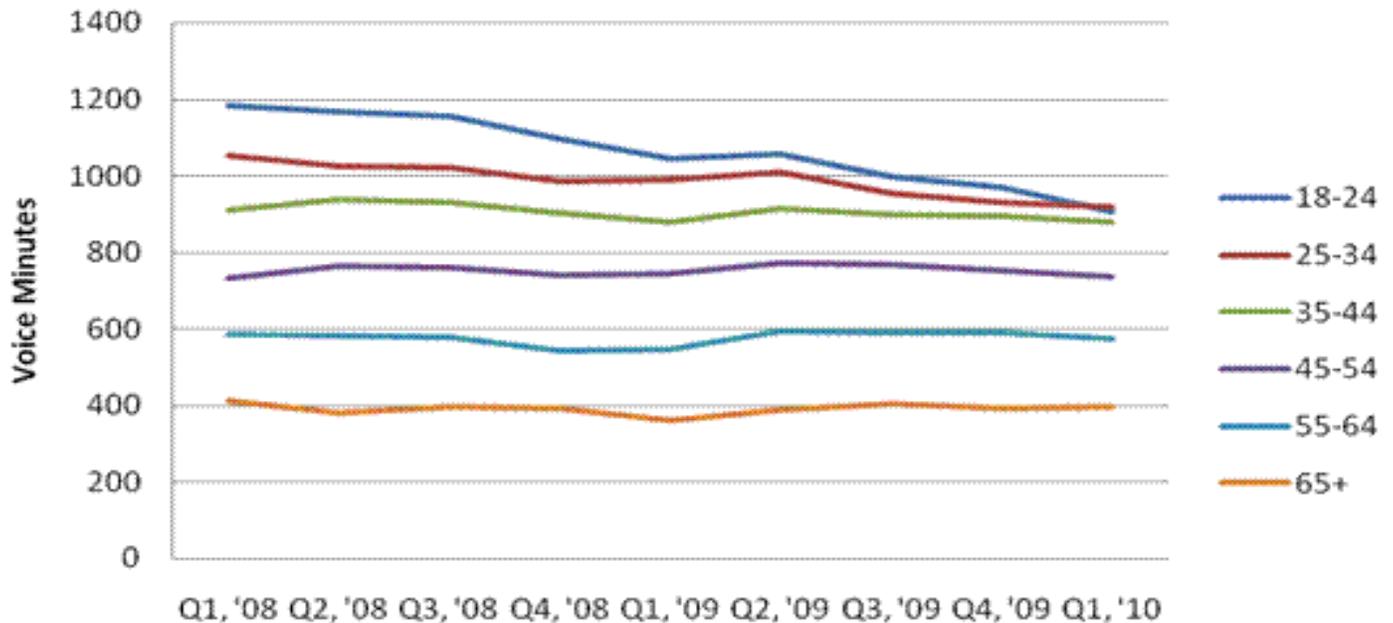
In this article we will explore the factors that are driving customers to abandon cellular voice in favor of VOIP solutions and how the telecommunications industry is and should be responding to this shift in consumer demand.

Declining Usage of Mobile Voice

Cultural changes are influencing the abandonment of mobile voice. As we become busier and spend less and less time interacting with our coworkers, friends and family, mobile voice has become less significant. We are becoming a texting and messaging society. A voice call requires that both parties be available and participate in the call simultaneously. Unlike a voice call, text messaging and other forms of non-verbal communication

Average Voice Minutes Used by Age

Nielsen Customer Value Metrics, Adult Postpaid Subscribers



Source: The Nielsen Company

are asynchronous and don't require the immediate and continuous participation of the communicating parties. The younger, Millennial generation has been quick to pick up on this fact and has been adapting their behaviors accordingly.

As far back as 2010, [The Washington Post](#) reported that only those over 50 years of age continue to place mobile voice calls as their primary means of communicating, while younger generations are shifting from racking up voice minutes to SMS message counts. The Post also reports that younger generations consider making an unscheduled voice call both rude and intrusive. A phone call is clearly no longer the preferred mode of communications for our busy and over-committed society.

There are even consumers who have abandoned their cellular network plans entirely and use their smartphones as WiFi-only devices. In 2013, a [CBS News](#) article extolled the virtues of dropping your voice subscription and going exclusively with VoIP over WiFi.

What's Wrong with Cellular Voice?

According to the 2014 [JD Power Wireless Network Quality Performance Study](#), the typical customer reported that

about one out of five calls placed through the mobile cellular network experienced some problem during the call. These problems included distortion and static, dropped or faded calls or dropping a call entirely. With about an 80% satisfaction rate, this gives the US cellular voice experience a shaky B minus. Having a bad personal call can be annoying and frustrating. Having a bad business call can have significant economic impact. With one out of five calls likely to go badly, why take the risk of conducting business over the cellular network with an unreliable mobile voice call?

From the MNO perspective, mobile voice usage and revenues as a percentage of overall revenue have been declining for many years now in North America. In Europe, Africa and Asia the tipping point occurred in a similar time frame from 2012 to 2014, with the larger portion of revenue shifting from mobile voice to data. Most other global regions are expected to follow as advanced 4G and 5G networks enter new markets and smartphone technology penetrates much of the third world.

A recent report entitled "[The Unbearable Lightness of Mobile Voice](#)," by TECHNECONOMYBLOG clearly shows this trend toward decreasing mobile voice usage. And although the report states that mobile voice is far from

With about an 80% satisfaction rate, the US mobile voice experience gets a shaky B minus.

providers to increase their data tariffs, slowing the adoption of broadband. Similar stories out of South Africa, Malaysia and other parts of the world indicate that this is a global trend.

Clearly, the combined issues of reported poor service quality and revenue shifting away from mobile voice to data and other services will continue to drive the telecom industry towards new means of monetizing data and application services. With no foreseeable increase in future revenue from mobile voice, investment in cellular networks to support mobile voice will decline in favor of investment in data infrastructures, paving the way for wide-spread adoption of mobile VOIP.

Faced with these changes in customer behavior and network usage, operators, carriers and major service providers are responding by offering WiFi calling services, adjusting their revenue models and planning for the eventual shift toward data-only networks as part of their 5G strategy.

Network Operator WiFi Calling

AT&T has responded by introducing automatic [WiFi Calling by AT&T](#). The service will automatically place a VOIP call if the cellular network is either weak or completely unavailable.

dead, it certainly doesn't seem to be moving in the right direction in terms of revenue and customer demand.

According to Cisco Systems, over half of voice traffic in North America will take place over WiFi connections by the end of this decade.

In India, a report by Credit Suisse forecasts that half of the revenue from voice and messaging could be eliminated by VoIP apps such as WhatsApp and Skype. This is a major threat to network operators in India where 80 per cent of their revenue still comes from voice. The Credit Suisse report goes on to say that the impact of VOIP will cause the

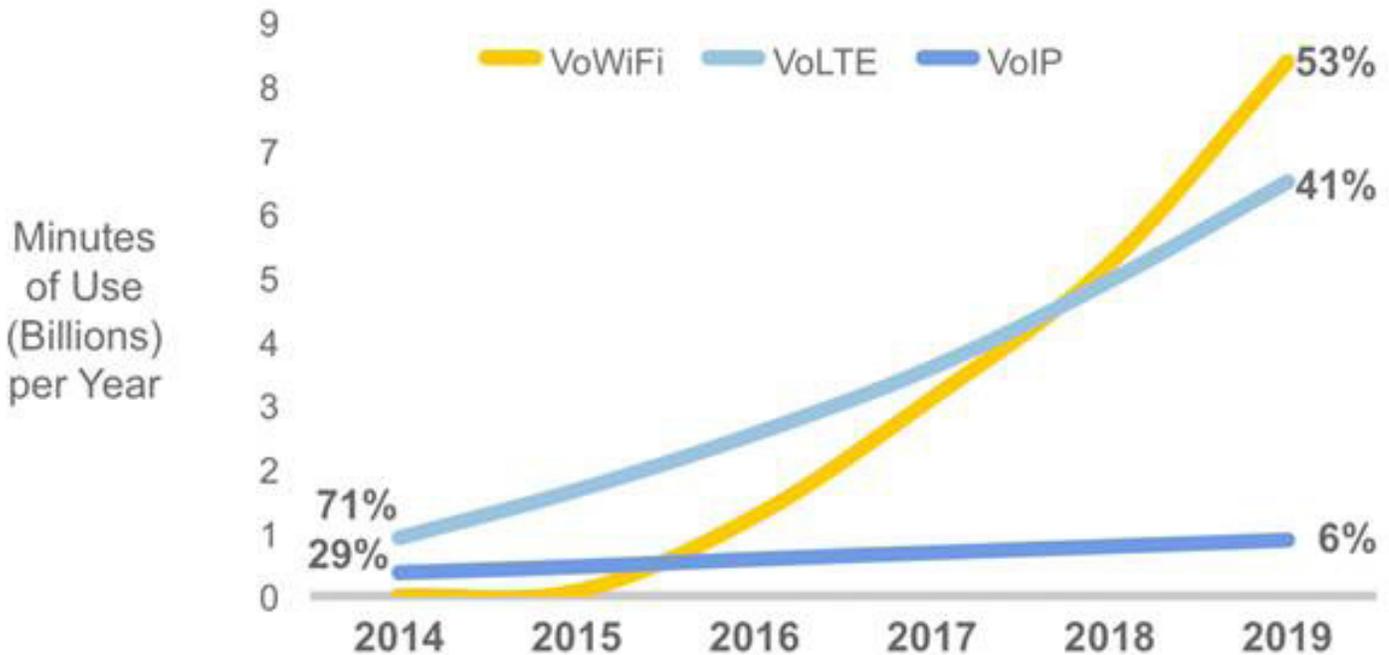


Figure 2. Over half of voice traffic in North America will take place over WiFi connections by the end of this decade. Source Cisco Systems.

So far, the service is only available within the United States, and U.S. territories of Puerto Rico and the Virgin Islands. It also only works if you use an iPhone 6.

Verizon has also announced the availability of [WiFi Calling by Verizon](#), but only for Android-based Samsung Galaxy S6 phones for now with other devices, including iPhones, sometime later in 2016.

Sprint has WiFi calling for both Android and iOS devices, but only the Android devices will support SMS when a cellular connection isn't available.

Of course if you've been following WiFi calling from the major U.S. carriers, you'd already be aware that CNET reported that [Sprint and T-Mobile](#) introduced their services years ago, with T-Mobile first introducing their Wifi calling service way back in 2007.

Google has also been dabbling in the WiFi-cellular voice integration space with Project Fi. A recent [article by Nicholas Armstrong](#) covers the pros and cons of Google's service. Although a good start, the unidirectional hand-off from Wifi to cellular and the delays encountered during transitions will likely not be acceptable to most customers.

Revenue Models

Two revenue models are emerging to support the future of a data-only network to support application IP traffic as well as VOIP. These are a flat-rate service with unlimited usage and a pay-as-you-go model. The best example of the flat-rate model is Swisscom. With a [customer-friendly web application](#) to recommend service levels, Swisscom offers unlimited calling, messaging and data access within Switzerland, as well as limited roaming in the EU and Western Europe. With unlimited data, moving to mobile VOIP becomes easier, allowing Swisscom to begin a phase-out of mobile voice as consumer demand shifts from voice to data.

An example of a pay-as-you-go model is PTel Mobile's PAYGO service. This model offers voice calls at 5 cents per minute, 2 cents per text message, and 10 cents per megabyte of data. Using their [web-based cost estimator](#), purchasing 300 voice minutes, 1,000 text messages and 50 megabytes of data results in a charge of 30 dollars. With this model, PTel revenue is directly based on customer usage, allowing consumers to choose between paying for mobile voice or VOIP on demand.

Two distinct revenue models are emerging to support the future of a data-only network.

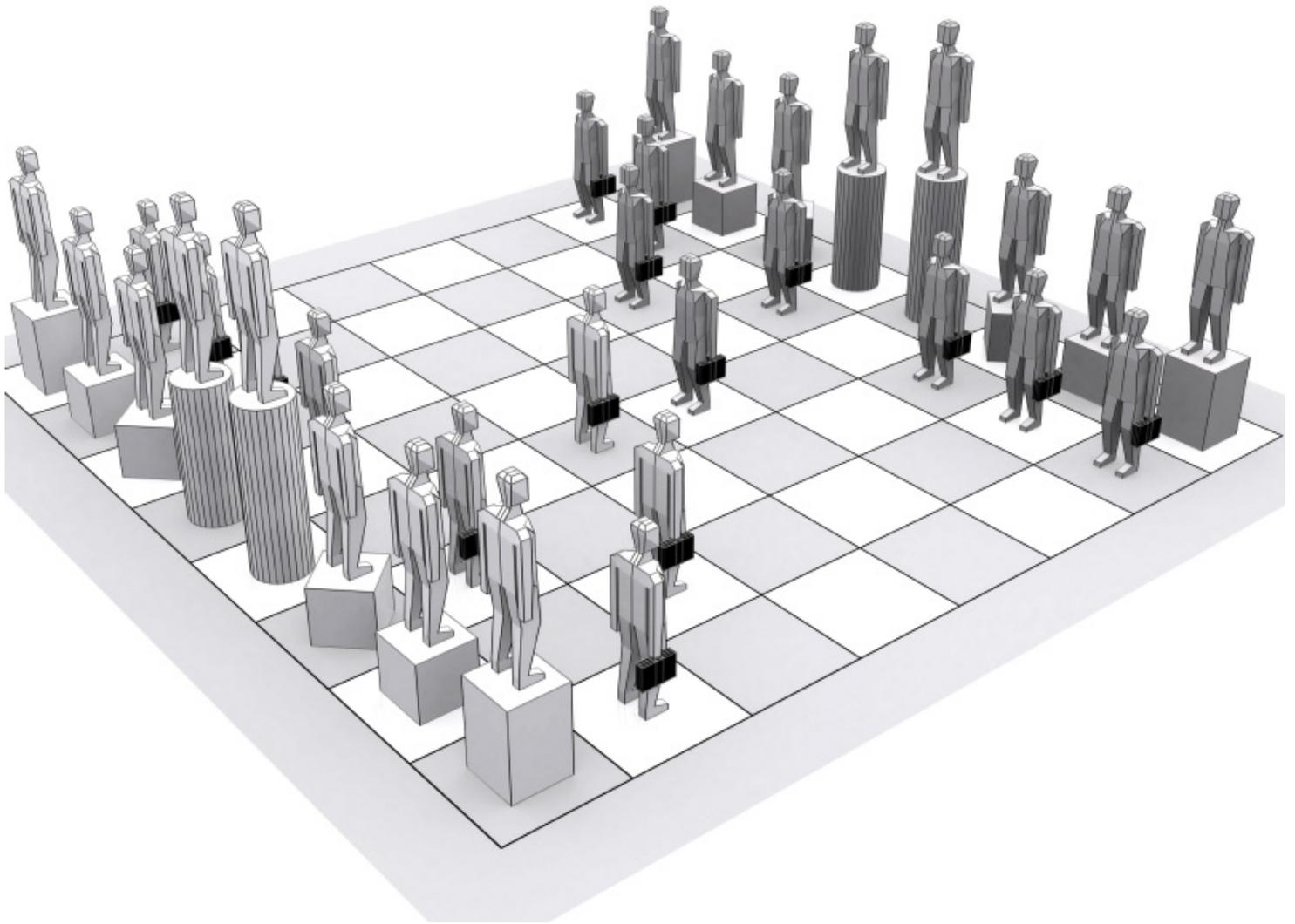
The appropriate model for each service provider is likely based on how they pay for their infrastructure usage, the target demographic of their customer base, how quickly their region is likely to move to a data-only network infrastructure and other factors.

Data-Only Networks

Finally, getting to data-only networks has a significant future advantage for network infrastructure operators. Unifying protocols will allow for better management of network traffic across cellular, small cell, WiFi and other emerging wireless network technologies, as well as backbone and long-haul services. It will also allow for better interoperability between providers of all three major delivery technologies: fiber, cable and wireless.

For this to occur, legacy infrastructure needs to be retired and upgraded in the US, Europe, Southeast Asia and other areas where cellular service was established primarily as a voice network.

The eventual roll-out of 5G technology in the early 2020s may see the first deployment of data-only networks. The deployment of such a network will certainly signal the accelerated death of cellular-based mobile voice.



MOBILE AND CLOUD GAMING

BY: WEDGE GREENE

The call is received in the payment inquiry center: “What is this two hundred dollar charge on my Visa?” Pay-to-Win games are monetized by user interaction with an in-game threshold: pay a little money and get a helper artifact or hint that enables the gamer to complete a level and advance.

Most of the time these games are free to start and then maintain a low purchase threshold to keep players involved. People start play as a way to kill time when they are bored. After all, a smart phone or mobile device is always at hand. Eventually, the player encounters a paywall, a requirement to pay a small fee before continuing the game.

The Paywall

The paywall is an obstacle in the game which can be overcome by paying a small fee. As their frustration increases, they agree to pay a little bit. Then in the future, making each small payment is easier at the next paywall. The game developer is selling a concept to move forward. On Candy Crush, the “pay to pass” threshold might be delayed until the late levels of the game, sometimes months into the habit, but it seldom is.

Candy Crush is a multi-billion dollar Over-the-Top enterprise that followed Facebook to mobile phones. From this, telecom providers just get data consumption fees; but it is estimated that it is played more than half a billion times a day on mobile phones. For the game publishers, there is high profit from in-app micro payments. Total expenditures on a game by a single addicted user can reach \$1,000. Profit is high. R&D and platform infrastructure costs for current phone games are relatively small, as are the transaction fees from the financial system.

King Games, the publisher, also developed an ingenious way to propagate users. Continued play can be “purchased” by inviting other new players to the game via the social network platform which is hosting the game. These player groups can “level up” with each other in their social networks. And players can pass lives to each other, if they have the patience.

The Gaming Market is Balkanized

People play this class of games addictively, but are not always happy with a game. Despite celebrity endorsements on talk shows, many users do not describe their experience as fun and pleasurable. Total time spent on a newly-introduced game is relatively short so there is no incentive to build games with depth or immersive “world view” construction. This market segment may also be future

**Games with depth or
immersive “world view”
construction are a potential
market opportunity.**

limited; social systems will eventually develop antibodies for this, just as it has for gambling. Big spenders will either request help or be forced to seek help. But these Pay-to-Win players are only a small segment of gamers. These are not what the gaming community itself considers as “serious lifestyle gamers.”

Pay-to-Win is not the darkest side of mobile gaming. Gambling is alive and well on the mobile platform. This morally-challenged activity is a natural fit to smartphones which can easily link to unregulated betting platforms. You can log in and place a bet outside of the standard economy and then watch the sporting event in real time on your media-enabled phone. It is not going away. Gambling has built cities in the wilderness and established out of the way places as destinations. Mobile phone gambling will at first compliment these locations, but later steal from the growth of these cities. Virtual bookies are just a fingertip touch on the phone screen. Social service networks will be hard pressed to keep up.

Still most phone gamers are mildly satisfied users. These customers want mobile gaming opportunities to expand but must split their gaming experience by platform availability. My wife plays a jigsaw game on her computer and solitaire on her phone. “You cannot see the jigsaw on the tiny phone screen and I prefer the mouse to move the pieces into place.” Nevertheless, for low resolution touch screen game technology, there is a wide variety of games for users to choose. Current classes of mobile games include ‘care for animals’, ‘shoot em up’ (SHMUP), collection games, and puzzle games. In tower-defense games a player holds a territory via collecting resources to combat a wave of enemies. Yet mobile strategy games are mostly not real time. Players take turns with the gaming platform and this limits the immersive experience. These types of mobile games are simple and lack depth of experience. Gamers expect each game introduction to be a fad market-driven by advertising.

Gaming content will push phone evolution.

Physical and Virtual Platforms

Mobile phone gaming platforms currently lag console-PC gaming in technology and depth of content. Historically the console-PC market is the sole supplier to the “lifestyle gamer.” Extracting value from mobile gaming is not a simple crossover of product name association. Fit must follow form in establishing immersive environments. Bad jobs by game publishers in trying to map console and server-based games to the mobile phone still makes lifestyle gamers wary of phones. This is a huge market if exploited successfully. Best seller console-PC games now gross billions and are rivaling film franchises as exploitable media content property.

But today, for this market, mobile phones are only being used in tandem with PC gaming. For example, two companies, Blizzard and Steam, introduced a mobile authentication system for games. The Steam Trading Card system is a meta-game system around other games. Steam controls purchase and user-to-user trading of in-game artifacts. Steam takes a small transaction fee for using their authentication tool allowing secured non-reputable trading transactions. Authenticated, mobile phone trades occur instantly; while out of system, direct player to player trades take days to complete.

Games with depth or immersive “world view” construction are a potential market opportunity. Tie-ins with turn-based Role Playing Games (RPG) work with existing technical limitations on the phone to provide some immersion in the gaming experience. Accommodating to the technical limitations of phones as a delivery platform, one approach is nostalgia. Final Fantasy 9, a popular console game of years past, is imminently forthcoming for Android, iOS and Windows. Final Fantasy fans might appreciate that the game on a modern mobile phone doesn’t look a whole lot different from the original. The phone is extending the lifespan of an otherwise potentially obsolete game.

Also smaller scope phone game tie-ins extend the virtual world’s immersive experience to simple individual play; for example, the multi-player interactive, real-time First Person Shooter console game Halo. Set in the Halo world, but a separate game, in Halo for mobile platforms, the user drives an armed vehicle and runs around shooting aliens. This provides the illusion of depth and context by keying on emotions and loyalty developed elsewhere in the large environment console game. It extends the phone market to the console crowd.

By simple extension, a way to add depth might be to tie mobile games to Massively Multiplayer Online Role-Playing Games (MMORPGs). MMORPGs are a combination of role-playing game and online game in which a large number of players interact with one another within a virtual world. The depth of these games is greater even than platform-bound games on PCs and consoles. But the network data usage, memory requirements, storage requirements, control systems and graphic demands of these games are greater than current mobile phone technology.

A major obstacle publishers generally need to overcome is that the game can’t take up too much space on the phone. Users prefer not to sacrifice too much limited phone storage to mobile games. It may be that MMORPGs will not transition to the mobile phone. Instead brand new uses of the phone for games will be needed.

Natural Fit

My daughter was going through security at the airport wearing a Pokémon hat – a rather obvious orange critter. “Is that a Charizard on your head?” My daughter responded with a small laugh of relief, “Why yes, my friend made it for me.” The guard pulls out his wallet and opens it up. There within is an original print holographic trading card of a Charizard. “It’s my favorite character. I’ve carried around this card for 16 years.” Cartoon drawing style fits with mobile screen graphic drivers. Millions of kids were raised on classic Pokémon: the anime, the trading card game, and the hand held console games. That is a huge potential of locked-up emotion that an ICT business can leverage.

Gamers expect the next winner of the mobile gaming market to be the forthcoming Nintendo Pokémon GO. It will put Pokémon on phones where the phone becomes a PokéBall, a device used to capture and collect the Pokémon monsters. This is a natural use for the phone that is consistent with the game mythology. It makes use of the mobility of the phone to allow the finding of characters in different places. I expect it will overflow with marketing tie-

in as brick and mortar stores perhaps buy rights to offer Pokémon characters that the players come to capture. The millions of past Pokémon collector/player kids are a dedicated marketplace. Other similar anime platforms likely will follow this lead to market.

Expanding on the notion of fit follows form, Pokémon comes with a history of direct player-to-player interaction. Past Pokémon gaming platforms allowed players to trade Pokémon or have live Pokémon battles between co-located users. This natural interaction is more socially engaging than contacting Facebook friends in Candy Crush. Currently it is not known if mobile phone Pokémon GO will interwork with non-phone traditional platforms such as the Nintendo 3DS. However, Nintendo has a history of letting users transfer game progress and characters forward (but not backward) as platforms evolve. This might allow games to drive replacement of phone generations interlinked with Pokémon generations. Always connected mobile phone platforms also open up cloud storage to these players. Pokémon will be stored in the cloud so a player can collect an indefinite number of characters without storage limitations. And this allows rich customization and individuality in these stored characters so the Pokémon become individual virtual pets of their owner player.

Control Issues

Touch screens are difficult for interacting in the environment of games. Small touch screens are not precise enough for dedicated gamers. Obscuring the screen with a finger in real-time play is disastrous. This is limiting what can be done with games and maintains the tech segmented market of console-PC vs. mobile phone. Breaking this barrier should be a goal of mobile device makers. This is happening with cars. At a recent trade show, BMW showed a gesture control system for the car dashboard, eliminating the need to touch anything. Equipment supplier Visteon previewed their practical gesture system in this BMW concept car. Could similar technology be used with mobile phones? Why not.

Evolution of the control interface is already in development as the next big technical improvement to the phone. Gesture systems could overcome touch screen limitations. Eye tracking can improve control without obscuring real-time play on the screen. Motion and orientation sensors could allow the phone to act similar to a Wii motion controller allowing the phone to mimic artifact used in real space by the player. Automatic transactions to cloud storage replace limited phone storage. Working in tandem, Bluetooth listening devices could allow a concurrent audio

narrative to occur. Use of conference calling between players interacting in the same virtual game environment might transfer the successful gamer interaction experience of MMORPG.

Pokémon GO will include a Bluetooth bracelet that unlocks phone game interactions. For other games I expect the IoT market will provide Bluetooth devices that interact as controllers or in-world play artifacts via links to the phone. It is completely reasonable to expect the use of the camera in phones to enhance reality in future mobile games. Already the GPS in phones is used in the game Ingress which was released in 2015 for Android and IOS. Ingress is an augmented-reality massively multiplayer online location-based game. Players travel to specific real-world locations and then interact with the real-world locations of other players.

The Co-Evolution of Phone and Gaming

Gaming content will push phone evolution. Microsoft demos of HoloLens involved a Minecraft experience that appeared to be happening in the real world. Google Glasses will interact with mobile phones in new successful generations of the technology. Virtual Reality (VR) attachments to mobile phones will become a standard product owned by dedicated gamers.

Software in phones will also evolve to push the gaming experience into new realms. A forthcoming example of this is Google's Tango technology. Tango works by combining inputs from a range of phone-based sensors and processes them into usable information, exploiting phone interlinks with fast Cloud platforms. New phone tech sensors include an infrared emitter and infrared camera which picks up the reflected light. A wide-angle camera adds visual features combining device location to the composite mapping of the local environment. The Tango system also includes enhanced accelerometers, gyroscopes and barometers.

Tango enables a mobile device to map indoor spaces. A Tango enabled phone can determine its location and orientation in relation to a virtually mapped environment of floors, walls, ceilings and furniture. Tango is a platform that can turn a smartphone into a controller with Kinect-like environment mapping and a Wii-like gesture mapping. This turns a mobile phone into an artifact mimic able to interact with other artifacts in indoor spaces. Nexus, Lenovo, Qualcomm, Intel, Nvidia and LG are all signed on to include Tango in their devices. Google offers APIs for game developers. You can be sure this is in concept exploration phase at major game publishers.

Kiko-Lyn's *Great* Mobile Adventure



BY: WEDGE GREENE

As post-millennials live and work, they will expect everything to be networked, connectivity to be integrated, access to information immediate, and monitoring of activities real time and continuous. International cultures amalgamate in the Internet-driven society. The IoT evolves from artifacts accompanying life to the artifacts of life.¹

Academy

When Kiko-Lyn was just a little girl she was sent from her secure and timelessly Japanese urban apartment to the local shogakkou academy. Kiko-Lyn was told by her parents that this would be a great adventure. She packed up her beloved Fire Tablet, the newest in a string of annual birthday tablets sent by her Aunt Rachael in distant America. She could not leave alone her pet foxes that come and go in the

virtual house, always needing to be fed and leaving puzzles and presents for her to click on. Kiko-Lyn dressed herself in the brand new school girl uniform, a pretty red plaid skirt over white tights and a crisp white blouse with puff sleeves. Around her neck went the school kerchief. Her dad speaking in his warm American accent, relaxed in his Air Force dress uniform, told her to pay attention to the kids around her and mimic their actions before speaking or jumping in. Her mom in proud aristocratic tones said for Kiko-Lyn to remember that hers was a revered and ancient Japanese family, “always beloved of the mountain spirits.”

Her mother walked with her to school that first day, past the newly opened cherry blossoms, leaving her at the school gate. Kiko-Lyn was directed to enter past the wall and follow the other girls across the play yard to the main doors where

a matron waited on the collection of first form girls. Kiko-Lyn was apprehensive, but charged with excitement. Just like in Anime, like her Radiata posters, she was about to become the emotional hero of a new story. She joined the other girls walking toward the school entrance. Proud and hopeful, she put a welcoming smile on her face. *Would they share their bento boxes at lunch?*

But as the day wore on, the whispers of “hafu,” “Konketsuji,” and “ainoko” turned to cat calls from the other girls. She did not get to share her lunch as none of the girls would sit with the “impure.” No one offered to play with her at the after class Go Club. Kiko-Lyn turned inward and silent.

As the year wore on, Kiko-Lyn’s silence at school crept into her life at home. She stopped talking and never raised her eyes. She did as she was told, but her only friends were in the mobile games of her tablet and its anonymous social networks. Eventually her dad and mother called her to the table for a family conference. Kiko-Lyn dreaded a lecture on how she could act to resolve things, because she didn’t believe there was an answer. Her dad spoke, “Kiko, I know you are not happy here. Your mom and I believe we have a solution for this. I’ve spoken with my sister, your aunt Rachael in San Francisco, and she wants you to come stay with her and go to school in America.”

“We love you so much Kiko,” says her mom, “and we will Skype every day to see how you are doing.” Kiko-Lyn loved the video calls and technology presents from her aunt. But she had little hope. School was a place of evil spirits masquerading as kids. She was packed and bundled off to her aunt in America. But what Kiko-Lyn did would not expect this to be a great adventure. She was being sent into hiding.

San Francisco

Rachael met the little girl at the terminal gate, taking her hand from the stewardess. She was on line with her sister-in-law, who was watching from the go camera on Rachael’s lapel. Rachael had agreed to wear the body camera and send real-time encrypted video surveillance to her brother and sister-in-law. As Rachael went to meet their little lost child, her sister-in-law coached Rachael on what to say and do over a Bluetooth ear plug. Rachael was thankful for this support and managed a smooth entry for Kiko-Lyn into her household.

Over time Kiko-Lyn opened up to Rachael. She liked the big American condo with its pool. Her room was three times as big as in Japan and all her special things had arrived by container and been set up in her space. But Kiko-Lyn only

answered when directly queried by her teachers. She did not make friends with the coarse kids. They were not mean, but their lives were so different. The Anime they watched was years old, the translations were wrong. And no one followed the popular Manga from home. When she did translate for the few who asked her, they still did not get it. Everything was too foreign.

Rachael, in concert with Kiko-Lyn’s parents, tried a new approach. They enrolled Kiko-Lyn for after school classes in the unique San Francisco Flow Academy. Koko-Lyn had been delighted by Flow videos on YouTube. Their hope was that the low-key Flow Arts mixture of Aikido, Gymnastics, Juggling, and slight-of-hand would engage the isolated young girl. And it did. As Kiko-Lyn began to master the Poi, the Duo, the staff and the wands, her self-confidence blossomed. When she went to her first Flow Festival with Rachael, she began to laugh and spin about the festival bonfire with the other kids. Kiko-Lyn had found herself in the Flow and re-entered the world with the goal of becoming a Flow Warrior.

Her parents came to stay in San Francisco so Kiko-Lyn could continue after-school and weekends at the Flow Academy. After six years, they all returned to Japan. Rachael was moving east with her new company. Kiko-Lyn’s mother was called back to DoCoMo labs and her father, retired from the Air Force, had a new marketing job at NEC robotics. Kiko-Lyn was not worried. She could help spread Flow to Japan.

Five years pass.

Tokyo Days

Kiko is much in the style. Her day persona is occupied with her early morning college classes. She blends in with her fellow “species dysphoria” students, most of who are older than she, by adopting a fox persona. Her cosplay costume is trimmed in fake red fur with black tips. Their Googles™ are enhanced reality overlays packaged into a pair of environmental eye protection goggles and nose filters. Each of them has customized their Googles™ with favorite characters from Anime, Manga, and myth. Kiko-Lyn has enhanced her Googles™ with twitching fake fox ears and a black button nose. The fox nose includes a solid state gas chromatograph tracking the purity of air – a regrettable necessity in 21st century life. The ears appear as simple costume artifacts, but she has embedded remote pickup mikes in each ear and they track nearby conversations and flick toward any loud noise. Just like with a wary, real fox. She says hello to fellow cosplayers: several bird friends and a pride of tigers. They all lunch on “swish swish” at the Yoshi’s

Shabu Shabu restaurant. She thinks *secret muggle identities can be fun too*.

Most weekends she and her friends engage in city spanning computer games across the background of Tokyo - lost in an augmented world of virtual images and metadata projected over views of the real streets and buildings by their Googles™. The gaming quests and tasks are sent by her aunt's friend, Jorge. Jorge refers to them as "his Irregulars" and they respond with his call sign "Sherlock." Last Saturday, Jorge remotely coached them through a full parkour run into a Blade Runner-ish overlay of the Tokyo business district, fighting virtual mutants in Atago, Seisho-ji and out to Kaneiji. Afterwards, Jorge said they were nearly ready to enter the Japanese National Metagames.

On the afternoons she is not training, Kiko-Lyn works her unpaid internship at her father's offices in the old NEC headquarters. This is a multi-story office building with a deep hollow core and offices on the outside walls. Open walkways surround the multi-story core with floor after floor of waste high white rails. A perfect place to develop and test urban drones.

Kiko works in swarm robotics. As she enters the building, she whistles out to her flock which has hidden in plain sight, camouflaged against the flat panel rails of the balconies. Her swarm is twenty hand-sized dragonfly analogs. Their skeleton is printed from diamond-fiber infused magnesium zinc alloy and wings of high temperature printed ceramics. They are coated with a novel use of flexible liquid crystal - micro screens arranged over the whole surface in an array. The result is a skin of synthetic chromophores of her invention. The swarm turns off their white speckled camouflage and suddenly appears, launching into the central open space.

They flock in circles about her, lit up in neon glow colors. She has keyed their color to her moods and today she is happy and expectant. As she climbs in the glass elevator her flock follows her upwards circling in the updrafts of the central shaft. Spectators in the open walkways stop to watch and laugh as these sparkling dragonflies circle up floor to floor, forming briefly displayed patterns of Catfish Kanji. Kiko-Lyn is a local celebrity and the corporate office pet.

A worker says, "Wow, that's new. Are we seeing Kanji display in the murmuration?"

"Yes," Kilo-Lyn answers. "Because of the small flock size and rapid movement in the base swarming pattern these images are very transitory. But as the swarm moves and repeats the configuration, successive bugs each flash a static segment

of the pattern. Many bugs, moving through the same spot and flashing in sequence, create the vertical shape of the Kanji. The flickering ghostly image occurs as different parts of the Kanji pop in and out of existence. Glad you like, it's a serendipitous visual effect blurred into the eye. On a time lapse video the Kanji is clear." Then she stops; I must not say too much.

On her Googles™ she reviews the video footage she programmed the swarm to capture while she was at school. Each bug is a node in a broadcast mesh and they auto upload to the their controller; an innocuous "toy" handle for a "retracted" lightsaber staff that is attached to her belt. Rather than have them link up on her handle, forming their resting configuration as a staff, she sends the flock to feed at any charger plates they can find. Today's surveillance target is her father and his lab assistants. Software stitches together the faceted views of the different flyers into a smooth movie. She watches her father for any open display of concern and finds none. A normal day with some packing as the trade exhibit is readied for airfreight shipment to their upcoming trade show, the Mobile World Congress. Her father is taking her mother on the trip to Mobile World Congress. Tomorrow she will wish her parents off for a happy working European vacation and nothing should cause them to rethink leaving her on her own.

Meiji Nights

Nexteday² night, with her parents off in the plane to the conference, Kiko was going Jedi. Time to live her hidden alter persona.

The flash mob arrives in ones and twos at the Meiji Shrine (Meiji Jingu) Treasure House. To relieve the crowds at the Kanda Myojin Shrine, it now remains open at night. The videography team releases its camera drones to track the other arrivals and eventually position in a 360 grid around the courtyard. Combined in software with detail shots from each cosplayer's personal camera drone, Kiko-Lyn will be able to edit a 3D playback. But the gathering must be obscured at its start and the players quick to disperse, as many would take exception to this street performance at the shrine.

The pageant starts with music flowing from the camera droids. A traditional wedding procession marches through the courtyard. Spectators are used to this; it happens every day. The bride is in a white kimono and hood and the groom in a formal black robe, walking together under evening light. But what is this! Shinto priests are not leading this couple; Jedi cosplayers lead the way.

Spectators from the crowd suddenly join the procession. The rest of the wedding party trailing behind the couple is now made up as x-wing pilots. Suddenly, a group in the watching crowd throws off their coats and appears as Ronin demons.

The mock battle dance is on. Everyone is Flow Parkour. The central Jedi is wielding Kiko-Lyn's staff which bursts into glow as a double lightsaber. She twirls and cartwheels in tumbling runs up and over the wooden shrine walls and buildings. The staff spins in mesmerizing patterns around her arms, her shoulders, her legs, and head. Her companion Jedi flings out a glowing short light saber that seems to spin away and "called by the force" return to his hand. He is clearly an expert at the illusion "flow wand."

The blaster bolts of the Ronin and the x-wing pilots are simulated by LED illuminated string darts, juggling clubs, and spinning rope poi that flash out and back like blaster fire. Suddenly a dart connects with Kiko-Lyn's staff and it fractures into a flock of glowing, flying dragonflies. They swirl and flash about her and climb to flock over her head. From her robe, Kiko-Lyn pulls and pops open two large fans which she uses to deflect the dart bolts. Each time a dart and fan connect, Kiko-Lyn triggers a fireworks display on the fan. Each fan is an array of flexible liquid crystal video screens. She spin tosses the fans and they reach out as if to strike at the Ronin leader, flash image an explosion and return, and again. The demon collapses. Quickly the x-fighter pilots finish off the lessor Ronin. Everyone leaps up and bows and off they quickly scatter through the park.

In the later video editing, they will time blur the flashing of the chromophores above Kiko-Lyn as she dances about the courtyard. The Kanji will spell out the story and emotions of the players across the top of the treasure house ending with, "May the Flow be with You." *PFM*³. This is Kiko-Lyn's ninth production but the first ensemble with the help of her Flow Parkour friends. Through YouTube subscriptions and sponsorships she has amassed a respectable, independent source of underground funds and this production should help her set up manufacturing of her new Chromophore Fan flow toy.

Red Pill

The next day Kiko-Lyn is sleeping in when she is awoken by an urgent Call Notification by her panicking parents. She is told that her Aunt Rachael was attacked via the web overnight and has been injured. She should send a get well message. Also, they are worried that video bloggers or business rivals of Rachael may seek to get at her through Kiko-Lyn. They want Kiko-Lyn to go to a retreat hotel in the mountains near

Nikko for the week that they are away. Kiko-Lyn agrees in order to calm her parents and thinking the colorful Shinto shrine would make a good backdrop for her next daytime video.

Kiko-Lyn keeps much closer tabs on her aunt than either her parents or Rachael realize. Rachael was no pet parent, but she never went anywhere without her dog Toby. Toby entered Rachael's life just after Kiko-Lyn went back to Japan; so Kiko-Lyn affectionately thought of Toby as her replacement. Kiko-Lyn had presented Rachael with a prototype robotic harness of her own design for Rachael's Toby. When the dog slept, segments of the harness detached from its web and worked at grooming the dog. When Toby stirred, the segments scampered back to link up on neck and shoulders. Kiko-Lyn hoped her Aunt would manufacture and release this harness, if its alpha trials with Toby were successful. So far her aunt resisted; saying normal dogs would not be as patient as Toby with the mechanicals. While not okay with this, Kiko-Lyn accepted a continuing alpha trial, as she had surreptitiously added video cameras and network uplink to the harness segments. She queried her cloud for yesterday's video and was appalled at the first person views of Toby taking down the household bots. Then Rachael flashed into view with a huge head gash and blood everywhere. "Nobody does that to my aunt!" she exclaims.

Jorge will not help her. "I've been called off and specifically excluded from involvement by Rachael per ICE restraining orders for her. Stay out of this; it is too dangerous. I'll engage the Irregulars to help keep watch on any approach to your apartment. Do as your parents say, but ask a friend from the team to go with you to the shrine." Kiko routinely blogs her life to these friends, sharing her daily life and feelings in an ongoing private blog; as they also do for her. But she knows in this case these friends will be more loyal to Jorge, their gaming master, than to her. *So it's a solo underground job* thinks Kiko-Lyn. She revokes all shared access keys to her cloud life-log and tweets a "on private retreat" message. She shutsters at going dark. So she repeats to herself, *I'm not a kid anymore*.

Kiko-Lyn applies skin dye makeup and prosthetics to make her legs and spine appear only partially healed from a traumatic injury. Above her pelvis she adds an electronic switchable nerve block from the apartment's first aid station. Then she bolts on an exoskeleton of silicon carbide nanoparticle-infused magnesium zinc alloy. She prints some fake attached webbing to make the exoskeleton look like cybernetic leg braces that allow a paraplegic to walk. In reality this exoskeleton allows her to move very fast and bounce high during her Flow Warrior shows. She loads false

data to her medical data insert. The program is accurate except it exaggerates an injury received doing parkour. The accident is in the public data record, and caused her a temporary need for a medical exoskeleton. But the temp part is not public, so her exoskeleton travel license is real, and a fake paraplegic disability should be credible. She needs to look vulnerable but be super parkour.

Kiko-Lyn sends out info agent spiders to trail the web for information on Jonathon and *International Widget*. Most of his data is not publicly available. Jonathon keeps a scrubbed information footprint on the public web. Nevertheless, a few hours later a cloud-based text and video analytics program flags a citizen advocate blogger with axes to grind on exploitative businesses. This blogger has captured frequent comings and goings of Jonathon Xavier Blake, General Manager *International Widget*, in Hong Kong for meetings with factory representatives of mainland businesses suspected of using child labor. A cross check of publicly available flight manifests and seminar registrations show many more Hong Kong trips, and longer stays than these surreptitiously documented meetings. *Could this be a location for Jonathon's mistress or an unofficial residence?* Jonathon's main residence of record in the Cayman Islands is unassailable. Turning up nothing better, Kiko-Lyn is off to Hong Kong. She buys a ticket with her underground funds. This bank account is in her name and not hidden; it is just that none of the adults in her life ever thought to look for it.

Traveling to Honk Kong, Kiko-Lyn has texted back and forth with the citizen blogger Dongjing "Dawn" and come to see her as trill⁴. Dawn sets up a meeting for lunch. Each appears in public as their obscured YouTube identity and dressed for the meeting as their online persona. Kiko-Lyn is happy to make a new media sister and everything she learns of *International Widget* just amps up her desire to Skunk them. Kiko-Lyn reviews pictures Dawn took that show Jonathon's employees traveling to and from Tsuen Wan New Town via private car, always using the same town car company.

The MTR train ride is over some beautiful mountain passes through parkland. Kiko-Lyn downloads the car company app and requests passage to "the offices of *International Widget*." Expecting as a regular stop, it will be in their database. It's a long shot, and also flagging someone's attention is her goal. Picked up at Tsuen Wan Station, she is delivered to a nondescript office building in the warehouse district.

Capture

Kiko-Lyn enters the building, sees no English signage, and uses translation software to scan for a directory showing

for *International Widget*. A big security guard grabs at her. She has her staff in "glass rod configuration" and the chromophores swirl in pastel blues and greens. It is a distraction. As a hood encloses her head, Kiko-Lyn keys her staff to "Scatter, Hide, Follow, Record." She has pre-selected Jorge's net address for the flock's media outbound queue. She drops her staff which seems to shatter on the floor. In reality, the staff disassembles into the dragonflies of her swarm, releasing their hold to the staff shape by rapidly unbraiding diamond-hard legs.

Behind her she hears, "Poor snowflake, broke your expensive toy" and a dark chuckle. Kiko could twist away and throw her mugger using Aikido, but her objective is to seem helpless and get caught. This should gain her entry to Jonathon's lair. Self-justifying allowing herself to be captured, *How else could she locate incriminating evidence on Jonathon? Plus video of this capture should motivate Jorge to get involved.* She fakes a struggle to draw attention from her dropped staff handle. It is deploying legs and climbing up her calf where it will configure to mimic a controller of her fake leg braces. In the hood, the Googles™ gas alarm triggers and her filter is ripped from her nose. Thinking I'm gonna be #rekt⁵, Kiko-Lyn falls unconscious. As Kiko-Lyn is carried away, her swarm deploys camouflage and follows the homing beacon in her staff handle.

Later, when he gets the video mails of Kiko-Lyn's capture, Jorge's invectives startle even his hardcore staff. As video fragments from the swarm trickle in, they allow Jorge to follow her transport during the kidnap, and provide coordinates of her eventual location. He knows that despite Rachael's earlier restrictions, he must act.

Kiko-Lyn wakes up starfish⁶ in a room furnished as a 19th century cabinet of curiosities. She is strapped into an ancient dental chair, but her "paralyzed legs" are not latched to the chairs stirrups. Her exoskeleton is off to the side of the room, being prepped for an empty display shelf. Displayed around the room in wooden and glass trophy cases are mounted specimen skeleton bones which all show breaks from bullets, blades and trauma. Many are displayed with the weapon that made the injury, newspaper clippings and exhibit description cards. Two walls are historical oddities, but one wall is contemporary. *This is necrophobia⁷ disturbing.* Adjoining the historical collection are modern cases with 3D relief prints and looping animated GIFs. Many are of the same man bearing guns, crossbows, swords and axes. Not all the mounted injuries are of game animals. Human tibia with bullet holes, femurs sliced in two, knife in ribs, and several crushed skulls are given prominent display. *Drakeface⁸*, she thinks, *This guy is sick sick sick. I'm going to make a mint in*

*selfiecida*⁹ residuals. Change of plan; best not to wait for Jonathon, who looks to enact these predatory interests on her. She triggers the video recorders built into her Googles™ and exoskeleton. Game on. She quotes Jorge, “Release, reconnoiter, evade, sabotage, escape.”

Fur-sure, she imaginary gesture quotes. *My next generation swarm will include cutting tools. But for now, it's illusion time.* She whistles her flock; momentarily panicked with nomophobia¹⁰ when nothing flies toward her. Then from several displays she sees a flash tailored to the directionality of her eyes. Six, she counts, made it here. Others will be holding station on the path to the outside and completing a mesh network link out to the public net. The dragonflies crawl over and attach to her wrists. She activates a stored program, from her video stunts, for the chromophores to display large bruises and raw wounds. When the attendant comes, it will seem she needs treatment from a self-damaging struggle. She keys the spinal neural blocker off, feels her legs tingle with returning feeling, and starts yelling as if in panic and pain.

She is hoarse before anyone bothers to show up. *Clear view, a facial image and kinesthetic walking pattern off to the analytics cloud for identification. One down*, she thinks. The swarm throbs and shows fresh hemorrhaging. The attendant rushes to release her arms speaking in what Kiko-Lyn’s translator program just flags as swearing. As soon as the arm buckles are released, Kiko-Lyn swings her legs up into a scissor-hold and then flips herself to the floor. She lands the attendant’s head first. She clamps the nose and mouth and waits for her medical sensor to flag him as unconscious.

These minions have noticed her escape. Using clues from the video eyes of her dispersed swarm, Kiko-Lyn is directed out of the way of pursuers as they appear in dragonfly eyes. Eventually, this puts her off the outbound path and into areas of the building the flock has not surveyed. But she has picked up three more dragonflies. But her rapid action advantage is lost; time to hide and reconnoiter. Hiding must be possible in this old facility that would be retrofitted, not built with integrated sensors. Now it’s time to move in stealth and map for hiding spots.

She runs a Tango 3D model reconstruction of all the rooms and passages mapped by her dragonflies and starts modeling a virtual avatar seeking refuge. Hunkering down and switching her view to virtual reality, her avatar walks the 3D halls projected in her Googles™. She is searching for sensor dead spots to hide. She finds a potential spot where her avatar turns invisible. She physically moves there to wait it out. She pulls up her hood and keys the chromophores in

her clothing to simulate background and shadows. Her main worry now is making any noise that audio sensors could detect. She is hungry but only uncomfortably so. She notes that it’s been 34 hours since her capture video went out to Jorge. Worrying, *Is he Trust fail? How soon will he respond?*

To be continued...

Footnotes

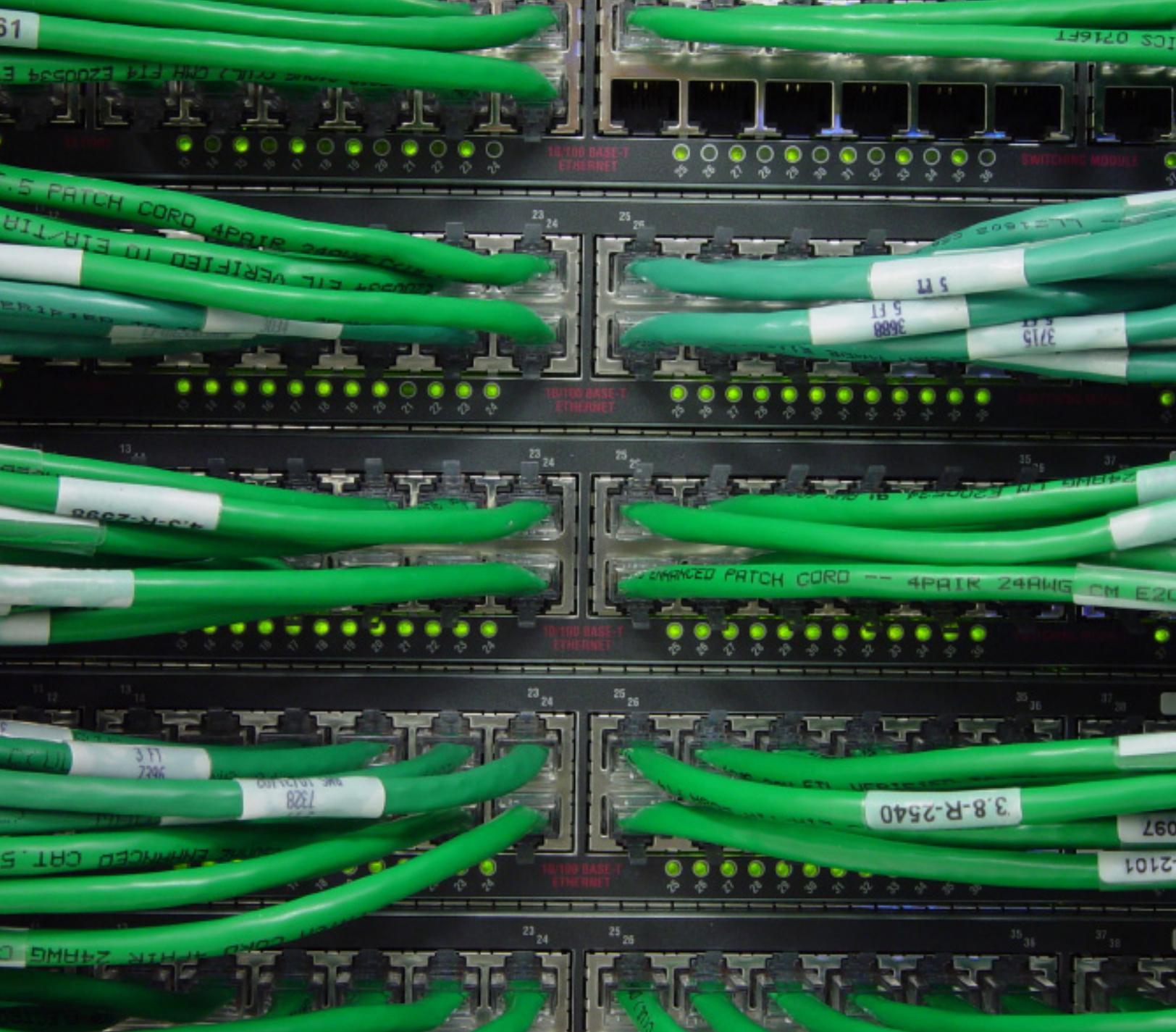
1. Kiko-Lyn uses contemporary urban slang as if it has become everyday speech with her generation. These are language drift, not misspellings.
2. Nexterday: the day after tomorrow
3. PFM: Pure F***ing Magic
4. Trill: Well respected, a combination of “true” and “real”
5. #rekt: When one gets completely strung out with hangover.
6. Starfish: Spread out and stuck like a starfish
7. Necophobia: Abnormal, persistent fear of dying or being dead
8. Drakeface: More than just sad.
9. Selficide: Taking selfies in dangerous situations or circumstances
10. Nomophobia: Fear of being away from a mobile phone.
11. This is an ongoing fictional series portraying the use of technology in the future. Any past or present resemblance is completely coincidental. Any trademarks are the property of their owner.

Pipeline
MARKET RESEARCH

**CUSTOM RESEARCH
REPORTS & SURVEYS**

**LEVERAGE THE
COLLECTIVE KNOWLEDGE
OF THE GLOBAL MARKET**

GET PRICING & DETAILS



AUTOMATED INFRASTRUCTURE MANAGEMENT

Automated Infrastructure Management (AIM) automates discovery and documentation of network cabling infrastructure in the data center, central office or commercial building.

By adopting an AIM solution, network administrators can streamline provisioning and monitoring of network connectivity, gain an accurate view of what is connected where in the network, reduce downtime by real-time notification of unplanned changes and produce up-to-date reports on the state of the infrastructure.

In this article, we'll look at the definition of AIM, discuss its applications, and consider some features to look for when choosing an AIM system.

The problem with manually documenting the network

Today, about 90 percent of IT networks are documented using manual tools like spreadsheets, which are laborious and prone to human error - which can be costly.

Network technicians often spend as much time updating and maintaining this manual documentation as they do connecting things and resolving issues. The risks associated with inaccurate documentation can make troubleshooting and change management time-consuming and potentially expensive.

For example, suppose a company hires a new employee and needs to provide a work space for that employee. The request is sent to the help desk and a ticket is created. Then a work order is sent to the technician who is dispatched to find out if an outlet is available in the desired location.

Even if documentation exists, the technician needs to go there to see if there is an available outlet to double-check and verify if existing documentation is accurate.

Next, the technician has to contact the network team and ask it to provide or assign a port, and the network team then has to determine what ports are available. The help desk enters the information into the work order and hands it to the technician.

Finally, the technician has to figure out where to make the connection. The technician goes to the wiring closet and

finds that all 48 ports on the switch are already connected, although it's not clear if all of the ports are actually in use.

The next step is either to start the procurement process for a new switch or else manually determine if some of the connected ports are no longer in use and can be re-used.

From start to finish, this process can often take a long time.

What is AIM?

Automated Infrastructure Management (AIM) systems are an intelligent approach to physical layer management that gives network managers unprecedented control over their networks. An AIM system can reduce the time it takes to deploy new assets, which in turn saves on operational costs. Cost savings over the lifespan of the infrastructure can outweigh the initial capital investment of the AIM system.

AIM systems have been around for years; but in the latter half of 2016, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) are expected to ratify standard ISO/IEC 18598, which describes the functional requirements and operations along with the data framework and API for AIM systems.

An AIM system consists of intelligent hardware and software components that are designed to detect the insertion and removal of patch cords. The software collects and stores the resulting connection information, relates that connection information to cabling connectivity information, and relates the cabling connectivity information to information from other sources (i.e., Layer 2-7 network management systems) through application program interfaces (APIs).

AIM systems can also provide the capability to discover networked devices and to pinpoint their physical location within facilities.

With an AIM system in place, the network administrator knows exactly what is connected where. He or she has a real-time view of the physical network connectivity and the ability to generate alerts when an unplanned connection or disconnection occurs.

The system also provides a work order management system that generates trouble tickets and directs a technician to

With AIM systems in place, network administrators know exactly what and where devices are connected.

the exact location of the problem. Finally, the AIM system generates reports that show what is connected where.

Applications for AIM Systems

AIM systems improve several aspects of data center or central office operations, such as:

Change management – You can't manage what you can't see; and without an AIM system, the network manager can't see the physical layer of the network. By capturing information about every physical connection and relaying it, through an API, to higher-level network management systems, the AIM system provides an accurate, real-time view of the physical network connectivity and can issue alarms when an unplanned or unauthorized change occurs.

Asset management – If the network administrator has no visibility into which switch ports are actually in use, he or she may opt to buy a new switch when an old one appears fully utilized.

AIM systems provide an accurate view of which switch ports are in use (and what they are connected to), so IT managers can optimize asset management and reduce Capex. AIM systems can also track distribution, usage, and management of power over Ethernet (PoE) systems within a commercial building.

Troubleshooting – AIM systems document the precise location of a connectivity problem. In fact, some AIM systems can cause the port LEDs on problem connections to blink so the technician has a visual guide to the problem. This approach greatly speeds troubleshooting because the technician doesn't have to spend time verifying manual documentation or hunting for the location of a problem.

Security – AIM systems enhance network security because they can report when a port is disconnected, or connected in an unauthorized location. Without AIM for example, a malicious user might unplug a server and move it to an office so he or she could access the server through its management port, bypassing logical security measures. The network manager would see that the server went down for a few minutes and then came back online, and such an anomaly might be ignored rather than identified as a problem. With an AIM system in place, the manager would know that the server was moved to a different location, and this could trigger an alarm.

Reporting and Compliance – Organizations operating under regulations like Sarbanes-Oxley need to provide accurate documentation of change management in their networks for audits and compliance. AIM systems produce up-to-date reports on the state of the network to facilitate compliance.

Disaster Recovery – Without up-to-date documentation, an IT manager is reduced to guesswork when trying to rebuild a data center or central office in the event of a disaster (for example a power outage, fire, flood or earthquake). Having real-time documentation with an AIM system makes it possible to know exactly what was installed where and how everything was connected so the data center or central office can be rebuilt quickly and cost-effectively. Accurate documentation also makes insurance reporting much easier.

Choosing an AIM Solution

There are many AIM solutions on the market. In this section, we'll look at some features to consider when selecting a product.

Quality of information provided – Different AIM systems provide different levels of information. While all will report that a patch cord is connected or disconnected, for example, some will allow you to store information about the length, type, and even color of the cord being monitored. This additional information can be a big help when troubleshooting or recovering from a disaster.

Work order management – Work order management systems vary in their feature sets. Trouble ticket generation and management should be as automated as possible, and some AIM systems will produce trouble tickets with step-by-step instructions for fixing a problem and then automatically close out the ticket

when the problem has been remedied. In addition, some AIM systems support mobile devices so a technician can use a tablet or smartphone to view and process a work order.

Device Discovery – AIM systems capable of communicating with LAN switches, SAN switches and other IP-enabled devices allow for the determination of the precise location of all active devices connected to the network. Location information is absolutely critical when security issues arise and need to be addressed immediately. With device discovery, accurate, real time information regarding port utilization is also readily available. This allows for optimization of existing equipment and expensive purchases can often be postponed or even avoided.

APIs – The ISO/IEC standard specifies that all AIM systems should have either SOAP or RESTful web services APIs so they can share physical-layer connectivity and device information with other network management systems. Choosing an AIM solution with RESTful APIs (which have superseded SOAP-based technology) will greatly simplify the integration process.

AIM systems improve overall management of data centers, central offices or commercial buildings by monitoring all physical connections and reporting what is connected where.

They significantly shorten troubleshooting times, improve work order management, tighten security, and improve change and asset management for IT managers.

With a new AIM ISO/IEC standard set for ratification in late 2016, this technology can become a key contributor to efficient data center and central office management.

PIPELINE MEMBERSHIPS

Join Now

MEMBERSHIP BENEFITS

- **Bundle *Pipeline's* marketing services**
- **Receive up to 50% discount**
- **Finance your marketing investment with lower monthly payments**
- **Build your own package**



[CLICK HERE](#)

The first month of 2016 was an active one for a variety of telecom issues, including Wi-Fi, security, and corporate acquisitions. It's no surprise that network technology continues to evolve and the FCC was busy addressing a number of issues regarding infrastructure and service. Let's start with Wi-Fi.

Wi-Fi changes for the better – and maybe worse

Cisco got its day in court and won after Texas-based Commil USA had brought suit against the network communications technology giant, claiming it infringed upon a Commil USA patent that enabled wireless signals to be spread over a large area where multiple access points are needed. A federal court decided that [Cisco did not infringe upon the patent](#) and reversed a near \$64 million judgment against Cisco after a long-running patent dispute between the two companies.

While Cisco was found not liable for patent infringement, there is some concern that broadband operators may be infringing upon the privacy of home Wi-Fi router users. A new study from Juniper Research predicts that at least [one in three home routers will be used as public Wi-Fi hotspots](#) by 2017 as a low-cost way of rapidly expanding domestic Wi-Fi coverage. However, the study indicated that service providers may not be making router owners aware that they are running public traffic through their private equipment.

Speaking of alternative ways to provide public Wi-Fi access, LinkNYC has begun rolling out [free gigabit Wi-Fi service in New York City](#), beta-testing a program to turn 7500 NYC phone booths into Wi-Fi hotspots with encrypted secure connectivity through mobile devices. Almost immediately, IT security experts expressed concern that the new program's lightning-fast, [converted Wi-Fi hotspots will attract hackers](#).

The dark side of telecom service: security and fraud

Most people applaud the freedom and convenience of modern telecommunications service; but issues concerning security and fraud for both consumer and service provider are always lurking in the background (also see: [The Signaling Security Problem](#) in this issue of *Pipeline*).

A [new report](#) by international trade organization Mobile Ecosystem Forum (MEF) identifies a number of mobile security threats and reveals that over one third of consumers are avoiding downloading and using more mobile apps because of privacy and security concerns.

But consumers aren't the only ones with concerns. Another report, this one from Neural Technologies, reveals that telecommunications providers worldwide this year face [\\$300 billion in losses](#) from uncollected revenue as well as internal and external fraud.

There is good news on the fraud and security front, though. In a related survey by the Communications Fraud Control Association, global [telecom external fraud losses have actually dropped 18 percent](#) since 2013, totaling just over \$38 billion in 2015. The survey cites as a main reason for the decrease in external fraud the increase in collaboration among carriers in more effectively identifying and stopping fraudulent activity.

A new technology announcement by global information services provider Experian may [help in the effort to reduce fraud](#). The company has introduced a batch phone verification product that supports compliance with the Telephone Consumer Protection Act (TCPA), distinguishes phone type, and validates phone information in real time with over 4500 carriers.

Apparently fraud cuts both ways. Canadian mobile services provider [Telus was found guilty of making false or misleading representations](#) about premium text charges it was assessing its subscribers. The company agreed to provide its customers with CAD \$7.34 million in rebates as part of a consent agreement the service provider reached with the Competition Bureau, the independent law enforcement agency that ensures Canadian businesses operate in a competitive manner.

An industry in motion: companies bought and sold

It was also a busy month for mergers and acquisitions, and for good reason. New analysis by Bloomberg reveals that [wireless competition is fierce and growing](#), putting a premium on spectrum space. The new report offers a global outlook for 2016 and indicates that wireless carrier competition is heating up in North America. As a result, spectrum auctions are getting more attention than ever. In fact, the value of spectrum in the FCC's latest auction rose significantly above prior auctions and the secondary market, underscoring the need for more of this resource.

One of the most notable acquisitions was [Nokia's takeover of Alcatel-Lucent](#), which will now officially disappear, replaced by a single networking giant doing business under the Nokia brand

and offering complete mobile and fixed network solutions to take on competitors such as Ericsson and Huawei. The deal has turned Nokia into the number two largest global telecom networking company in the world, second only to Ericsson.

And that wasn't the only major buyout to make headlines this month. In the U.K., communications service provider **BT sealed the deal with EE**, the country's largest mobile operator. The Competition and Markets Authority (CMA) cleared the way for the sale of the joint Orange and Deutsche Telekom mobile unit to BT, saying the acquisition will not significantly harm competition or customers.

Now that EE is safely tucked into BT's pocket, the newly-expanded service provider is looking at **developing joint ventures with Deutsche Telekom** - now BT's largest shareholder after the EE acquisition. Analysts hint at a move to all IP networks for the two major European carriers as DT takes a 12 percent stake in BT and, in an ironic turn of efforts, may be looking to now acquire the primarily-fixed-line U.K. telecom as BT expands into TV, mobile (with its takeover of EE), and ultra-fast broadband.

Closer to home, Ericsson announced it was **acquiring U.S. entertainment content provider FYI Television** in a move to expand the Swedish communication technology and service provider's content discovery business from Europe to the rest of the world. Ericsson claims to be the largest provider of content discovery services in Europe and intends to make its business global with the addition of FYI.

Just to the north, Canada's Zayo Group Holdings Inc. completed its **acquisition of Manitoba Telecom Services Inc. subsidiary Allstream** for CAD \$465 million. The move adds trans-Canada routes and dense metro networks to Zayo's portfolio and makes the company the only pan US/Canada network provider.

No rest for the FCC

The Federal Communications Commission was busy all month with a number of telecommunications issues, ranging from what to do with legacy systems to where and how fast telecom services should be.

AT&T spent a lot of face time with the FCC, arguing points about dumping outdated services and getting rid of copper. The carrier giant has petitioned the FCC to **discontinue what it considers obsolete services** such as collect-calling and



other operator-assisted offers that have declined sharply over the past decade. In a separate filing, **the company sided with competitor Verizon** to oppose TelePacific's proposal to the FCC asking for a delay in the retirement of copper infrastructure. TelePacific cited possible diminished services to customers who may not have access to IP networks. However, AT&T asserts that providers - including TelePacific -- already have sufficient time to inform their business customers that they might be switching away from copper.

Speaking of AT&T and the FCC, all of this activity has made the FCC realize it needs to modernize its communications - so it turned to AT&T for some help. The carrier has **signed a five-year agreement with the FCC** to provide it with a cost-effective IT solution supporting secure mobile and cloud-based applications. The service will link a number of offices and data centers and let the FCC change network and Internet needs on demand. Using AT&T's services, the FCC can connect to diverse cloud service providers.

In its effort to modernize, **the FCC may have become too aggressive**, says six senators. According to a letter written to the commission, Senators Daines (R-MT), Wicker (R-MS), Blunt (R-MO), Fisher (R-NE), Johnson (R-WI) and Gardner (R-CO) expressed their concern that the commission has set an overly ambitious benchmark for broadband internet speeds. The senators called the speed requirement, which last year changed broadband download speeds from 4 mbps to a minimum of 25 mbps, "arbitrary" and said it "fails to accurately capture what most Americans consider broadband."

INDUSTRY NEWS DIGEST

In other FCC news, the commission has wrapped up the special-access data-collection proceedings it had undertaken to better understand competition in the special-access market, where services are provided to carriers enabling voice and data traffic to be transported from cell phone towers and buildings. Sprint took the deadline to submit comments as an opportunity to complain about the [high wireless backhaul fees](#) charged by incumbent local exchange carriers (ILECS), claiming they are unreasonable and will only drive up wireless costs for consumers.

FCC chairman Tom Wheeler just announced a proposal to [unlock set-top boxes](#) from cable and satellite subscriptions to enable consumers to use their preferred devices for accessing programming, saying it would open up the industry to more choice and innovation. In response, MVPD advocacy group The Future of TV Coalition released a “fact sheet” [rebutting the FCC’s assertions](#), saying the commission’s proposal is based on “myth,” not “reality.”

Finally, with the warming up of US relations with Cuba, the FCC has announced that the [last remaining country on its exclusion list is now officially open for US companies](#) to provide telecommunications services without separate commission approval. The commission went on to say that removing Cuba from its exclusion list benefits the public interest as it will likely alleviate administrative and cost burdens on both telecom companies and the FCC and fuel more competition among carriers interested in the new market.

To read more news stories, be sure to check our *Pipeline’s* real-time [news center](#) and [subscribe to Pipeline’s weekly and month newsletters](#).

To have your company’s news included in our coverage, send your press releases to pressreleases@pipelinepub.com for consideration.



2016 INNOVATION AWARDS

**NOMINATE YOUR COMPANY
TO VALIDATE YOUR INNOVATION**

**SPONSOR THE AWARDS
TO COMPETE FOR FREE**

CLICK HERE >



Apptium is an innovative technology partner to leading service providers in Telecom, Media, Entertainment and Health Care. Our solutions provide customer-centric digital experiences to enhance and improve every step of The Customer Journey.

For more information, visit www.apptium.com



BARCELONA 22-25 FEB 2016

The GSMA Mobile World Congress is the place where mobile leaders to gather, collaborate and conduct business. In 2015, Mobile World Congress hosted more than 93,000 mobile professionals from 200 countries in our largest-ever event. Make your plans now to be part of the excitement at Mobile World Congress 2016, in the Mobile World Capital, Barcelona.

For more information visit www.mobileworldcongress.com



gen-E offers network and systems solutions to better manage a broad spectrum of service industry infrastructures, employing their own custom solutions (gen-E Ops Center), as well as the top-ranked IBM Middleware for Network and IT Service Management suite, among others, to provide a singular view into the health and performance of a customer's entire IT and business infrastructure, integrating and consolidating tools and events across business, data center and network operations.

For more information, visit www.gen-etech.com



Founded in 1993, NetCracker Technology is the proven, strategic partner delivering mission-critical solutions to communications service providers around the world. With our global reach, leading-edge technology and unbroken track record of successful implementations, we eliminate operational and business silos and deliver real-time experience in an on-demand world.

For more information, visit www.netcracker.com



gen-E offers network and systems solutions to Ontology Systems is revolutionising how telecommunication network operators get to know their networks. We replace expensive and fragmented views of your network with affordable, comprehensive and dynamic panoramas so you can truly know your network. Ontology Systems is proud to count some of the world's largest telecommunications companies amongst its customers, including a number of Vodafone Group companies, Telenor, Telkom South Africa and Level 3 Communications.

For more information, visit www.ontology.com



Markitexture is a marketing consultancy that specializes in helping companies build awareness and increase revenues through tailored marketing programs, processes, and support systems. Markitexture combines creativity, marketing expertise, and technology to form highly effective marketing programs. This unique perspective enables us to understand, analyze, and optimize our clients marketing programs to ensure they maximize the return on every marketing dollar spent.

For more information visit www.markitexture.com

A PUBLICATION BY

Pipeline

Pipeline Publishing, L.L.C
2723 South Main Street, Suite 150
Ann Arbor, MI 48104
Phone: +1 (734) 707-4988
Fax: +1 (734) 794-4701
www.pipelinepub.com



© 2016, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as copying, modifying, or reprinting, will be prosecuted under the fullest extent under the governing law.