Technology Brief...

January, 2018

J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategy, Insight

INSIDE THIS ISSUE

2018 will be the year of "Smart" in Mobile

Mobile remains a very competitive business with major smartphone vendors continuously trying to outdo each other, and consumers often left doubtful that the latest gadget is really something they need to buy. Previous mobile competition was all about having the best displays or the fastest processing. Early on-board assistants, like Siri and Google Assistant, raised the bar and gave us a taste of what was coming. However, these features have become much less differentiated by brand these days. It's time for the next wave.

The next generation will be about "smart", and is now making its way into our every day mobile devices. It's not just about voice interfaces to a search engine or calendar entry as we've had in the past or rudimentary AR/VR. We're seeing truly smart assistants, learning about us and altering the functioning of our device as they go. They have the potential to both dramatically alter how we interact with our devices, and how they interact with us. And we've just scratched the surface with new visual interactions.

This new strategy is emerging as more vendors deploy an AI cloud behind and closely linked to their devices. Services like Samsung Bixby, which started as a way to help users navigate functions on their device, is now being extended to include interactions beyond the device and into the real world. Clearly Amazon Alexa and Google Assistant are not just popular because they are a way to interact with your devices using your voice. Rather, they are increasingly popular because they are tying our devices to other things around us (e.g., home automation), and making it much easier to perform complex tasks.

"…the next 2-3 years will see a large impact from "smart" mobile devices, as service providers like Apple, Amazon and Google make their systems available universally, and vendors with the needed high level of resources, like Apple, Samsung, Huawei, LG, add increasingly sophisticated tech into their devices – sometimes as a hardware, and sometimes as cloud services (e.g., Samsung Bixby)....."

But Smart doesn't stop there. With the advent of more capable mobile engines, including enhanced graphics and AI capability from the likes of Qualcomm, Samsung, Huawei, etc., we're now in a position to see "Assisted Reality" become part of our mobile devices. This will be even more compelling once we move to 5G networks with higher speeds and importantly much lower latency. But even with current 4G/LTE advanced networks, the ability of the device to guide us in the real world by providing visual cues and superimposed images often based on internal 3D visual sensors is enabling a smart ecosystem to emerge to offer many more intelligent ways to interact with our world. This will definitely be a major battleground in the next 2-3 years as vendors try to outdo each other in providing Assisted Reality capability, and generally without the addition of a head worn display that is unappealing to many consumers.

Voice interfaces and AR are not the only smart features coming. Apple's visual log in capability demonstrated on the iPhone X may indeed be revolutionary, even though visual log ins have been done before. But more importantly it's a first step towards something potentially much more profound. It will ultimately allow apps to understand our moods and/or our emotions, much like people do when they speak to one another and read facial expressions. This not only provides emotional feedback, but can potentially be used in many important ways – from reading facial expressions from people who may not be able to communicate in normal ways, to monitoring a patient's health, to creating a new way to secure data/passwords/logins through unique facial expressions. In the next 2-3 years. I

expect to see a plethora of new and innovative uses for advanced facial recognition technology. I expect most vendors to make the capability an inherent part of their offerings.

While I expect the typical players to be dominant in this emerging market (e.g., Amazon, Google, Apple), its unclear yet how well Microsoft will do. Cortana is a good assistant and Microsoft clearly has high levels of expertise in all aspects of assisted reality and AI. But without its own ecosystem to play on, it's reliant on enticing vendors to support their offerings. This may be a hard sell to mobile phone vendors bound to the Android ecosystem, but I do expect Microsoft to be successful with their smart technology in most enterprise uses of smart mobile.

All of this "smart" coming in the next few years will start out in consumer devices, but it is destined to become an important part of enterprise use as well. Things like assisted reality, emotional monitoring/visual cues, smart virtual assistants, etc., will become an important part of logging in, safety monitoring of users, just in time training and on the job assistance, among many other purposes. They will ultimately make enterprise users more productive and allow enterprise apps to be much more intuitive and easier to use, while also making the work environment safer. Enterprise deployments generally lag consumer tech by 2-3 years, but I expect this time around they will be implemented fairly quickly since many of the services associated with this new tech will be tied to the cloud, which enterprises are already adopting in a big way.

Bottom Line: the next 2-3 years will see a large impact from "smart" mobile devices, as service providers like Apple, Amazon and Google make their systems available universally, and vendors with the needed high level of resources, like Apple, Samsung, Huawei, LG, add increasingly sophisticated tech into their devices – sometimes as a hardware enhancement, and sometimes as their own implementations of cloud services (e.g., Samsung Bixby). Although companies like Baidu will be content to play in their home market for the short term – they definitely have visions of being a major international player and rival of the big guys. I expect with their massive scale and considerable resources, Baidu, Alibaba and other Chinese players will eventually achieve broad market penetration, although that likely will take 3-5 years. Nevertheless, you will see "smart" coming to your device very soon.

Will the next great AI breakthroughs be coming from outside the US?

While still in its infancy, Artificial Intelligence (AI) is advancing quickly and more services are now making their way to the marketplace. To date, most of the work that's well known to consumers has come from the labs and R&D centers of big US companies (e.g., IBM, Google, Microsoft, Intel). There is still a lot of work being done at university research labs and in many spinoffs, but generally these startups are not currently major players in the market, although many have interesting technology. They do not pose any real threats to the dominance of the big players, as most will invent and ultimately be acquired for their potentially promising technology and be integrated into an existing ecosystem.

"…It's very likely that in the next 3-5 years, we'll see a very different AI market than exists today. Many Asia companies will challenge the current leaders, even as newer startups find compelling ways to advance AI (and often get acquired by the bigger players in the process)…..

We currently see very few foreign competitors in the North American market. But I believe real change is coming to the AI market from multiple big international players, who currently may be less visible, but who nevertheless are making major investments. As a result, the AI marketplace will change in the coming 2-3 years, with new players, and new breadth of services being offered to both consumers and business users.

Many Chinese companies are investing heavily in AI technology, albeit with a purpose. They see autonomous driving, drones, smarter appliances, healthcare and general Internet of Things as a major focus where they can have significant impact based on their predominant role in consumer electronics and emerging "gadgets". While cloud providers (e.g., Baidu, Alibaba, Tencent) look to improve their operations through AI and sell services often based on ecommerce enablement, many of the more traditional product vendors (e.g., Huawei, Xiaomi) are looking at ways to embed AI in mobile and consumer appliances to give them an advantage in the marketplace.

That's not to say that China is alone in the race. Major companies in South Korea (e.g., Samsung, LG, Hyundai) are also investing big-time in AI technology to power products and services for their customers. As these companies are already well established internationally, working from their base of mobile devices and appliances will allow them to rapidly have an impact on services, particularly as their brands are already recognized in most of the world. A big question mark in emerging markets outside of China is India and what it may bring to the table. I expect India, with its vast engineering resources and expanding base of home-grown competitive companies, to become a key player in AI in the next 3-5 years and potentially even sooner.

Although to date most of their efforts have been concentrated on their home markets, all of the above players are now looking to break out and propel themselves into direct competition with the major international players like Google, Microsoft, Amazon, etc., not only in the US and other mature markets, but around the world. Fueled by a large domestic market where they can often dominate and develop compelling, large scale products (sometimes due to political preference for home based systems) they can relatively quickly leverage their current developments and installations for the expanding overseas markets. And once deployed at scale locally, it's becoming increasingly easy to expand globally through already established cloud based geographically dispersed and localized data service centers. The hardest part of the expansion will be marketing the services, rather than technical challenges, but we've seen many international players quickly overcome lack of market presence through social and word of mouth endorsements. It's very likely this will follow a similar path.

Bottom Line: It's very likely that in the next 3-5 years, we'll see a very different AI market than exists today. Many Asia companies will challenge the current leaders, even as newer startups find compelling ways to advance AI (and often get acquired by the bigger players in the process). The current leaders ignore these up and coming competitors at their own peril. And consumers of services should get ready to find some less familiar names serving them in the not too distant future. With a greater variety of service offerings, the world of AI will become much more attractive and adaptable, and that's good for both consumers and business users.

Security in the age of EoT

The Enterprise of Things brings a unique requirement to enterprise security that is distinct from normal end points and data centers. Indeed, with a greatly expanding number of units that will be deployed over the next 2-3 years (I estimate there will be more "things" in enterprise than PC and mobile phone clients combined within 3-4 years), it is imperative that companies address the growing security requirements for these devices in order to avoid the potential for catastrophic events (e.g., hacking of automated tools, disruption of processes, autonomous vehicles losing control, drones crashing, GPS systems redirected, etc.). While some may be costly in terms of data or production loss, others may be downright deadly!

"…Many older EoT installations exist and new ones are rapidly coming online. EoT should not follow the consumer model where anything is fair game and lowest cost often outweighs required secure implementations. … it's imperative to try and come up with some standard security practices that can at least limit the type and scope of security breaches....."

There are many issues involving EoT security, which should be seen as an integrated component of overall enterprise security, but for this brief discussion I'd like to focus on 3 key points that can easily make or break an EoT installation. These three areas are:

Hardening of the devices

It's imperative that companies deploy EoT devices that are built on secure and verifiable architectures for both hardware and software. Technology such as ARM's TrustZone or Intel's Trusted Execution Technology provides a secured area of the chip that can be used to store critical data that can securely identify and/or run kernel level code to prevent malicious activity. Root of trust systems now prevalent in many of the newer generation of chips and proven in the mobile device world also provides a way to verify the OS on booting and/or before running so as to prevent

hijacking of the device. Unfortunately, many older, and even some current EoT devices, are built on lower level, less functional chips that do not provide such technology. I believe it to be imperative that companies identify and quickly replace any such devices as the ease with which they can be hacked is appalling, and the damage potential is great.

Securing the code running these devices
Code security requires both a hardware and software approach working in unison. As indicated above, modern chips have built in security functions to protect against errant code that can be used to hijack a device. In conjunction with a hardened operating system, like BlackBerry QNX which has been used in mission critical applications for many years, and newer versions of Android and Windows for IoT, a combined front against malicious activity can be established. But that's not enough. It's also imperative that companies test their apps for any potential avenues of attack. Many test tools exist for apps running on virtually any OS, but many EoT products still contain custom built low level code that has never been adequately screened. Along with the imperative to check the hardware technology stated above, it is equally important to assure that the software is fully secured.

Monitoring of network traffic on/from these devices.
Finally, to assure that no hostile takeover of large numbers of devices takes place, as has been shown to occur in many consumer devices where DDOS attacks where delivered from wireless cameras, WiFi access points, etc., an effective way to prevent such activity can be enabled by monitoring traffic to and from the EoT endpoints. Many network monitoring tools already exist (e.g., RSA NetWitness, Citrix Netscaler) and these can prove valuable in finding any suspicious network activity that could point to malicious behavior. While I believe all organizations should be deploying network traffic monitoring as a security measure on all transactions, it's doubly important for EoT devices that could affect safety and/or operations of the organization.

Bottom Line: Many older EoT installations exist and new ones are rapidly coming online. EoT should not follow the consumer model where anything is fair game and lowest cost often outweighs required secure implementations. While no EoT installation is quite the same, it's still imperative to try and come up with some standard security practices that can at least limit the type and scope of security breaches. Without a concerted effort, EoT can actually do more harm than good.

About J.Gold Associates, LLC.

J.Gold Associates provides advisory services, syndicated research, strategic consulting and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies. We work with our clients to produce successful new product strategies and deployments through workshops and reviews, business and strategic plan coaching and reviews, assistance in product selection and vendor evaluations, needs analysis, competitive analysis, and ongoing expertise transfer.

J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends in the computer and technology industries. We have acquired a broad based knowledge of the technology landscape and business deployment requirements, and bring that expertise to bear in our work. We cover the needs of business users in enterprise and SMB markets, plus focus on emerging consumer technologies that will quickly be re-purposed to business use.

We can provide your company with a trusted and expert resource to maximize your investments and minimize your risk. Please contact us to see how we can help you.

Recent Research

Contact us to request the following research reports:

Market Studies
- **The State of Enterprise Mobile Management (EMM)**
- **Mobile E-Commerce: Friend or Foe?**

Emerging Technology Trends
- Highlights our key emerging trends for the next 3-4 years

Commentary and Analysis
- Apple and IBM in Enterprise: Joined at the Apps

Research Reports
- Android in the Business Environment: Is it Safe?
- Your PC has an Identity Crisis: Saving the cost of hacks and other benefits of enhanced identity
- Replacing Enterprise PCs: The Fallacy of the 3-4 Year Upgrade Cycle
- Keeping Notebooks Past Their Prime: A Study of Failures and Costs

Whitepapers
- A Heuristic Approach to Mobile Security
- MDM- Where Do We Go From Here?

J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Research, Analysis, Strategy, Insight