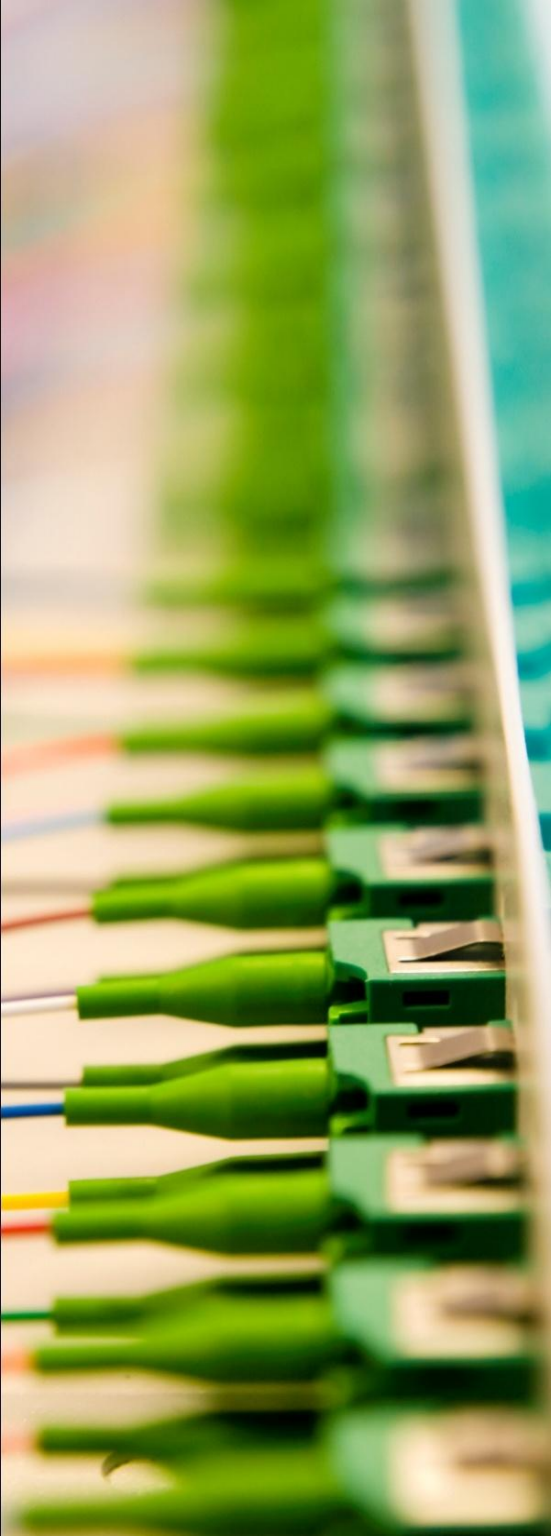


Mobile Roadmap: Navigating Around the Coming Collision in the Mobile Ecosystem

Kevin DiLallo
kdilallo@lb3law.com

Joe Schmidt
jschmidt@techcaliber.com

April 24, 2012

Agenda

- Conflicting Forces
- Technology
  - Services
  - Equipment
- Industry Structure
- Pricing and Deal Structure
- Consumerization
- Security
- Mobile Device Management

Conflicting Forces

Conflicting Forces

- Faster data services and more feature-rich content *versus* smaller, costlier data plans
- Exploding employee demand for mobility *versus* shrinking enterprise telecom budgets
- Employers' desire to offload costs to employees *versus* their need to protect their networks
- Individuals' expectation of privacy *versus* increasing demands for personal information and ways to collect that information

Technology

Technology: Services

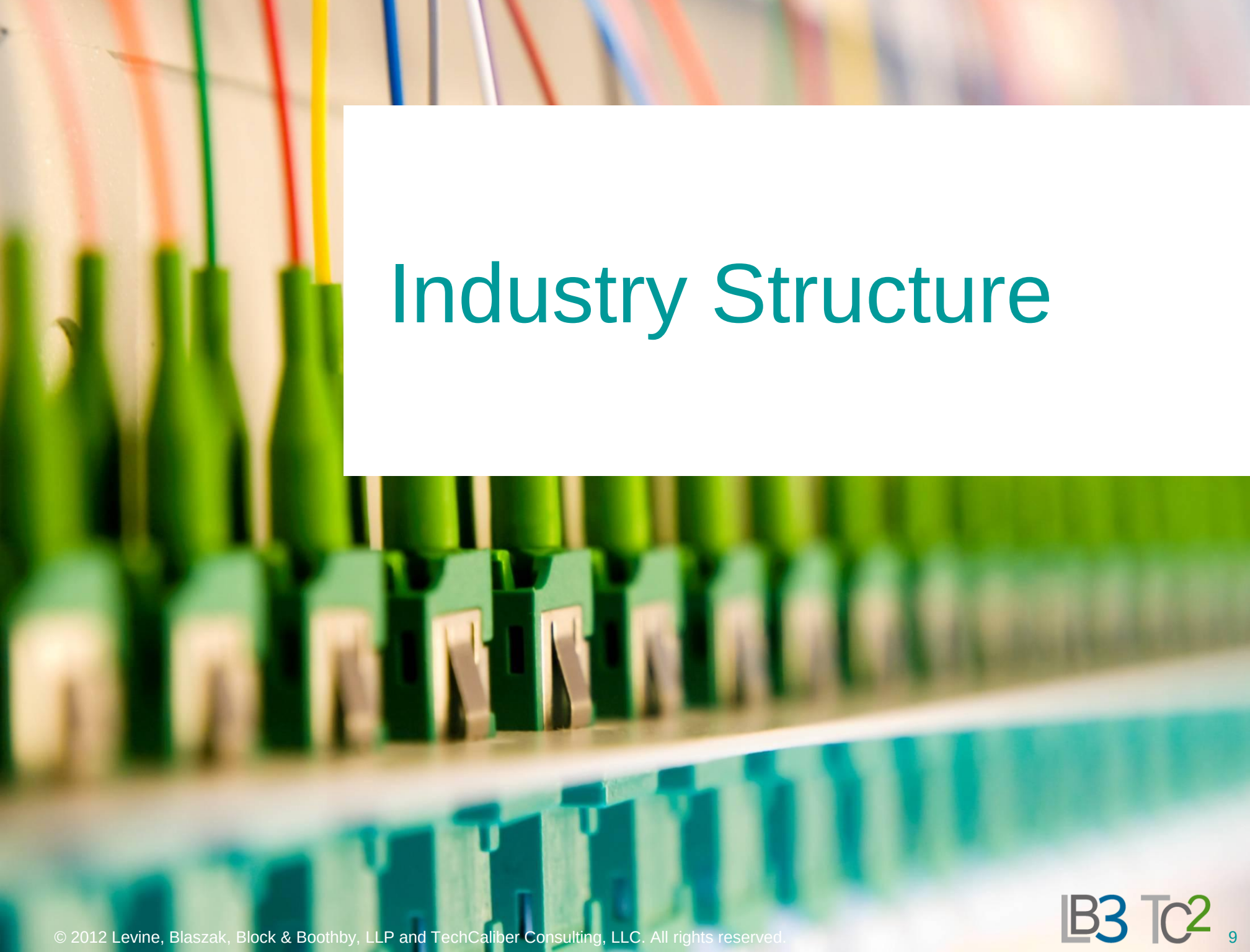
- LTE will be the dominant US standard by 2013 and the global standard three years thereafter
  - Greater opportunity to port your device between carriers
  - But differences in frequency bands used in different countries will mean that only multi-band phones can roam globally
  - Because Sprint and T-Mobile are so far behind AT&T (40 markets) and VzW (200 markets), their market share will continue to erode
    - Sprint says it will deploy in six markets by middle of this year
    - T-Mobile plans to deploy in at least a few markets by year-end
  - Analysts question whether Sprint will be able to afford to build a nationwide LTE network
    - Although Clearwire, in which Sprint holds majority interest, is building LTE its choice of technology (TD-LTE) is different than Sprint's (FDD-LTE), which will make it difficult to find compatible devices

Technology: Services

- Next enhancement is LTE Advanced, expected in 2013
- Data rates and low latency for LTE, and especially LTE Advanced, will make wireless an attractive option for enterprise data networks (probably as back-up)
  - Pricing may be an obstacle, however
- Voice over LTE is still evolving
- Skyrocketing demand for data and multimedia content, fueled by iPhone and Android devices, are driving carriers to greater and greater reliance on Wi-Fi offload
  - Moreover, FCC predicts 275 MHz “spectrum deficit” by 2014
- All carriers will expand their hotspot networks through acquisitions and partnerships to ease pressure on their 4G networks

Technology: Equipment

- Enterprises are trending away from aircards and toward tethering and MiFi hotspots
  - Pricing differentials and human nature* favor tethering
    - Bluetooth and Wi-Fi enable easier wireless tethering
    - * Individuals are never without their smart phones but often forget to bring their air cards
- Tablets will soon overtake laptops as mobile computing option
- In-building systems are becoming smaller and cheaper: femtocells on steroids
- Ubiquitous indoor coverage will hasten adoption of FMC and “cutting the cord” in the enterprise
- Moore’s law will continue to make smart phones faster and cheaper



Industry Structure

Industry Structure

- Verizon Wireless will emerge as hands-down frontrunner
  - Head start in LTE + AWS spectrum licenses purchased from cable co's (if approved) + superior network = more converts
  - Cross-marketing and resale deals with 4 cable companies will further extend its reach as well as direct and indirect subs
    - But pressure from competitors, Congress, FCC, and unions casts shadow over ultimate consummation of deals
  - Ability to re-invest earnings without having to pay dividends has allowed VzW to gild the lily
- AT&T will continue struggling to satisfy both its shareholders and its customers
  - As a result, it will never be able to keep pace with VzW

Which Leaves Sprint Where?

- As a takeover target
- Sprint's days appear numbered
  - Has $15B take-or-pay commitment to Apple
  - Has huge liabilities coming due in 2013, 2015, 2016 and 2017 and too weak a balance sheet to refinance
  - Unclear whether Sprint will have cash and spectrum to build-out nationwide LTE network
  - In the meantime, subscribers may defect to AT&T or VzW, who have major LTE lead

Industry Structure

- What will T-Mobile do?
  - Perhaps be acquired
  - Continue to be in the lower tier of the Big 4
  - Its network is surprisingly robust
  - Its problem is cash; it has a stingy parent
- What about Dish's plan to use its spectrum to build an LTE network?
  - Two words: "Good luck;" has very little spectrum
- And how about Century Link?
  - If anyone would/should/could acquire Sprint, it's them
- Other smaller players will remain small

Pricing and Deal Structure

Pricing and Deal Structure

- Economics is going to force major carriers to overhaul their pricing structures, which are unsustainable in the long term
  - SMS and MMS are propping-up profits while data costs, network upgrades and smart phone subsidies are draining them
- Expect more tiered data plans similar to voice buckets of minutes
- Expect pooled data plans for families and individuals with multiple data devices
- SMS and MMS are cash cows and will stay that way
- Voice may be a cheap add-on to data plans rather than vice versa
- Good chance the FCC or a court will invalidate exclusive handset marketing deals as anti-competitive
- Increased carrier acceptance of BYOD

Consumerization

Mobile “Consumerization”

- Enterprises are trending toward BYOD
- For years, IT standardized on RIM platform
- iPhone and Android OS have overtaken BlackBerry as smart phone of choice
  - Greater functionality, wider choice of apps
  - But less efficient data algorithms, battery life than RIM devices
  - Marked cost differential between iPhone/Android devices and RIM
    - Hardware prices
    - Mobile service pricing
    - Better graphics, apps & access to content = more temptation for non-work-related use
  - Will RIM’s new BBX operating system turn the tide?
- 4G Data Services and Tablets are fueling the trend . . .
- . . . and multiplying enterprises’ security risks and legal exposure

Mobile “Consumerization”

- Cutting Costs and Accommodating Employee Preferences
  - Pendulum is swinging back to individually-liable workplaces
    - In our view, the vacillation between corporate-liable and individually-liable models will continue, as neither is perfect
    - Individually-liable models are more expensive, disfavored by employees
    - But management feels better not having commitments to carriers
  - The BYOD trend is unstoppable
    - MDM solutions allow employers to secure personally-owned devices they know about
    - The big security concern is unknown, rogue devices
      - Yet few companies take measures to deny rogue devices access to corporate servers
  - Enterprise customer pressure will force carriers to allow more personally-owned devices, not sourced from the carrier, to use their services without any ETF

What is BYOD?

- BYOD was originally about enabling users to use their personal devices to connect to corporate applications
- Also driven by the "you can use what you want, but you pay for it" IT department approach
- Allowing employees to connect their non-reimbursed personal devices to corporate applications (e.g., email and calendars), using personally-liable plans
- Allowing/requiring employees to pay for their preferred device (e.g., if they want an iPhone instead of a cheaper BlackBerry), but using corporate liable plans
- Giving employees varying stipends/allowances to cover personal wireless expenditures and allowing connectivity to corporate applications

Can BYOD be a path to cost savings?

- In some quarters, BYOD is seen as the path to cost savings
- If the wireless bill goes to zero then the business case writes itself – “The company doesn’t pay for your briefcase, so it will no longer pay for your smartphone”
- In reality, companies will rarely take the “briefcase” approach
  - Companies tend to look at providing an expense allowance or stipend for users’ personal wireless service
  - BYOD business cases are getting more complex

Can BYOD be a path to cost savings?

- Un-optimized wireless services and miscellaneous costs can provide a BYOD business case mirage
- BYOD is unlikely to save money unless you move the cost burden from the company to the individual
- BYOD can be a very good way of providing a wider range of users access to corporate applications via a wider range of devices
- Mobile Device Management is key to enabling BYOD

Security

Smart Device Security Risks

- Like laptop computers, but worse
- Small and portable, so more susceptible to loss and theft
- Numerous wireless interfaces make them more vulnerable to electronic interception, location tracking
  - More “attack surfaces” mean more potential ways in – Wi-Fi, Bluetooth, Internet access, email, IM, MMS, SMS
- Greater memory, processing power = more opportunity for complex malware
- Downloading insufficiently vetted apps can introduce malware
- Use of mobile devices for payment creates financial incentives for hijacking
- Rigid IT policies may lead to rogue devices and unauthorized workarounds
- Resistance to surrendering combined business/personal device to IT control
- Lack of IT visibility into rogue devices interconnecting with corporate servers without authorization
- Interconnected mobile devices can be platform to penetrate networks, servers

Designing a Comprehensive Employee Mobile Device Policy

- Any policy should address three areas
  - (i) prohibiting employee behavior that could create liability for both employee and employer
  - (ii) implementing company data security and privacy policies;
  - (iii) minimizing employer's operational costs
- Any policy should be the product of collaboration by Law, HR, Compliance, Finance, Risk Management, Operations, and Technical/IT – need senior management support
- Update annually as technology and company's plans evolve
- Policy should be signed be each employee
- Policy should cover both company-issued and employee-provided devices and service plans

The Policy Should Address Mobile Security Risks

- User-oriented measures: training and awareness of security procedures and precautions
  - Maintain physical control of device; never lend it out
  - Comply with organizational policies and procedures re: PINs and passwords, backing up data, and limiting sensitive data stored on device
  - Never open suspicious email or attachments
  - Do not attach storage cards or other removable media that might contain malware
  - Do not download apps that have not been approved by IT organization
  - Turn off Bluetooth, Wi-Fi, infrared and other wireless interfaces when not needed

Legal Risks the Policy Should Address

- Employer (vicarious) liability for employee negligence, misuse
  - Automobile accidents top the list
    - Device does not have to be company-issued, as long as employee was conducting business
    - Use of mobile device while operating vehicle prohibited
    - Employee to pull over if must talk, email, or text
  - Copyright Infringement (unauthorized downloads of protected content)
  - Harassment, stalking, sending spam
  - Violating other users' privacy rights
  - Inadvertently breaching customers', vendors' confidentiality

Legal and Financial Issues the Policy Should Address

- Using Internet or wireless network in violation of AUP
- Unauthorized charges, contributions billed to company
- High volumes of personal and distracting non-business use
- Unauthorized ordering of devices and service on company account for resale to third parties
- Direct employer negligence for expecting use of mobile device for business without adequate training re: risks and risk-management procedures
- Violation of employee privacy through tracking, data collection
- Acknowledgment by employee of employer's right to content stored on device

Mobile Device Management

Mobile Device Management (MDM) is increasingly important

- MDM solutions used to manage “smart(er)” devices are offered by many vendors, including Sybase, Good Technology and MobileIron
- Initially used for managing devices and as a response to security concerns
  - The growth of alternatives to the RIM ecosystem has been a key catalyst for the growth in MDM, which typically supports multiple device platforms (iOS, Android, RIM and Windows Mobile) via a single application
  - MDM provides important security capabilities such as remote wipe, pushing out patches and applications, and security policy enforcement (e.g., strong password requirements)

MDM gives companies policy enforcement capabilities

- In addition to enforcing security policies, MDM solutions can be used to monitor and enforce usage policies
  - Barring and monitoring different usage types
  - Usage reporting
  - Managing users' ability to consume different usage types (e.g., international calls)
- Capabilities can be significantly more sophisticated than the limited options offered by carriers, and can be administered quickly and easily on a self-service basis
- In sum, MDM can be an important enabler of BYOD and can be used to enforce wireless policies

What to look for in a Mobile Device Management Solution

- Multi-platform, device diversity
- Cloud-based
- Functionalities:
  - Policy Enforcement
  - Security and Compliance implementation
  - Containerization
  - Inventory Management
  - OTA Software Distribution, patching, updating
  - Administration and Reporting
  - IT Service Management (e.g., permissions)
  - Network Service Management (e.g., contract management, cost control)
- Procure solution through competitive bid process