

Nelson Mullins

Attorneys and Counselors at Law

“Staying in the Game: What Your Business Must Do to Survive in the Digital Age”

ACC Special Event CLE

August 1, 2007

Sponsored by: Nelson Mullins Riley & Scarborough LLP

Donna K. Lewis

I. Introduction

A. Digital-Enabled Business Opportunities

- Communications
- Website
- Broadband
- E-Commerce
- Mobile
- Game consoles

B. Traditional Business Models and Revenues

- Media (industry convergence)
- Healthcare (electronic records)
- Financial Services (industry consolidation, process improvements)
- Retail (supplement customer service and commerce)
- Other industries
 - E-billing
 - Customer service (e.g., CRM)
 - Product extensions
 - Branding
 - Advertising
 - Sales

C. Striking the Balance

- Industry convergence/increased competition
- New opportunities
 - New markets (geographic, demographic)
 - New distribution methodologies and platforms
 - Enhance customer/vendor relationships (communications and interaction)
 - New products and services
- Consumer behavior shifting
- Established business models and relationships
 - How to expand without jeopardizing existing models
 - Change management issues
 - Potential conflict with corporate culture
 - Sufficiency of corporate resources

D. Requirements/Resources

- Content
- Technology

II. Content - Complex Rights Issues

A. Technology-enabled business opportunities

- Communications
- Website
 - Promotional/branding
 - Product offerings (i.e., e-commerce)
 - Service offerings (i.e., e-billing/payment)
 - Community
- Broadband
 - Multimedia opportunities (video, audio, gaming)
 - Enhance existing website
 - Facilitate interaction/community
 - Provide premium/subscription offering

- Mobile platforms
 - Extend relationship to new locations
 - Opportunity for targeted marketing efforts
 - M-commerce opportunities
- Gaming consoles
 - Brand fit
 - Demographic fit
 - Targeted messaging
- Advertising
 - Reach in new locations
 - Interactive capabilities
 - Targeting opportunities
 - Linking capabilities for purchase
 - Sales lead generation
- Data Collection

B. Type of Use/Rights Needed

- Commercial (advertising, endorsements)
- Marketing (promotional of primary licensed rights)
- Licensing/merchandising
- Media (radio, television, print, Internet)
- Platforms (television, computer, mobile device, game console)
- Creation of derivative works
- Internal business use
- Decision to license or develop

C. Type of Content

- Sports (players, teams, league)
- News (source, producer)
- Entertainment (talent, producer, direct, guilds)
- Music (artist, writer, label)

D. Stakeholders

- Varies by type (see II. C above)
- Owner(s)
- Talent
- Unions/guilds
- Third party licensees

E. Legal Issues

- Copyright
 - Rights of owner
 - ◇ Reproduction
 - ◇ Adaptation
 - ◇ Distribution
 - ◇ Public performance
 - ◇ Public display
 - Use under existing licenses
 - ◇ Review of rights granted
 - Express rights for use
 - Sufficiently broad rights
 - Ancillary rights (e.g., marketing rights)
 - ◇ If granted, review possible limitations
 - Broad reservation of rights by owner
 - Quality control/approval rights of owner
 - Territorial limitations
 - Potential distribution or display on yet-to-be developed platforms
 - Other requirements that are not practical on the intended platform
 - Restrictions on assignments or sublicensing
 - Acquisition of necessary rights
 - ◇ Availability of rights (or subject to pre-existing third party license)

- ◇ Identification of all ownership stakeholders (e.g., text, photographs, music, video, trademarks)
 - ◇ Defining immediate rights necessary
 - ◇ Contemplating logical extensions
- Other IP Rights
 - Trademark
 - Moral rights
- Rights of Privacy/Publicity
 - Traditional Rights
 - ◇ Right to prevent intrusion upon personal solitude
 - ◇ Right to prevent publications that place one in a false light and would be offensive to a reasonable person
 - ◇ Right to prevent public disclosure of embarrassing private facts
 - ◇ Right to prevent unauthorized commercial exploitation of a name or likeness (i.e., right of publicity)
 - Rights of talent (publicity)
 - ◇ Applicable contractual restrictions on the scope of use
 - ◇ Expansive judicial protection for the scope of the right of publicity
 - ◇ Product placement, commercial endorsement
 - ◇ Licensing/merchandising rights (e.g., games)
 - Royalty rights
 - Approval rights
 - ◇ Guilds (DGA, SAG, WGA)

III. Internet/Technology Issues

A. Commercial Websites

- Website Privacy Policies
 - What data is collected
 - How the data is used
 - General explanations

- Website Terms of Use (General)
 - Contract terms
 - Ownership
 - Prohibited uses/activities
 - Disclaimers
 - User consent as to postings/submissions
 - Limitation of liability
- Website Terms of Use (Special)
 - Age limitations
 - Commerce-related

B. Electronic Records - General Operational Concerns

- Consider type of data
 - Employee
 - Vendor
 - Customer
- Understand all relevant systems
 - Networks
 - Computers
 - Mobile devices
- Understand data flow
 - Collection
 - Use
 - Access (internal and external)
 - Storage
 - Disposal
- Privacy concerns (classification)
 - Sensitivity of data
 - Country of origin
 - Purpose of collection (other legal restrictions)

- Security concerns (access)
 - Administrative security
 - Technical security
 - Physical security

- Information security
 - Prevention of loss, unauthorized access and misuse
 - Assessment of internal and external threats and risks to administrative (employee access), technical (systems access) and physical (facilities access) information
 - Need for procedures and controls to preserve
 - Confidentiality (privacy, authorization)
 - Integrity (authentic and complete)
 - Availability (assessable as needed by those authorized)

- Security control elements
 - Preventive
 - Detective
 - Responsive
 - Administrative
 - Technical
 - Physical

- Threats extend to corporate confidential information/trade secrets
- SOX internal control issues (integrity of data)
- E-discovery rules
- Related corporate policies
 - Technical security compliance requirements (vendors); audit rights
 - Business continuity/disaster recovery
 - Hiring practices/background checks (employees, vendors)
 - Data collection (employees, vendors, and customers)
 - Document retention (employees, vendors, and customers)
 - Records disposal (employees, vendors, and customers)
 - Commercial website terms of use and privacy policy
 - Breach notification policy/procedures

- Outsourcers and service providers
 - Understand additional security risks
 - Global transfers of data/content with offshoring (additional security and privacy concerns)
 - Vendor access into IT systems
 - Compliance with service levels; user/customer satisfaction
 - Control v. cost

- Patent issues
 - Patent trolls
 - Litigation for business processes
 - E-payment patents

- Insurance risk management
 - Assess coverage

- New challenges to privacy enabled by technology
 - Outsourcing (must understand vendor data flows)
 - DRM
 - RFID
 - GPS-based services

C. Electronic Data Privacy/Security

- Ability to manage and collect valuable data
- Multiple points of regulation
- Specific US laws applicable to certain types of data (i.e., market approach):
 - Fair Credit Reporting Act (“FCRA”) – applicable to entities in the business of sharing and selling information about consumers (i.e., information brokers) and users of such consumer reports (FACTA amendment)
 - Gramm-Leach Bliley Act – applicable to domestic financial institutions and entities that significantly engage in financial activities; regulates internal and external use of “nonpublic personal financial information” data collected; not preemptive of state law

- HIPAA – applicable to certain types of record holders, such as health care companies, health plans, health care clearinghouses and health care providers, and “business associates” and others who use and handle personal health information (i.e., not all databases containing health information); not preemptive of state law
- COPPA – applicable to commercial website operators and covers the collection and use of information on children under the age of 13; verifiable parental consent required
- Specific US laws applicable to government agencies and national security
 - Privacy Act of 1974 and Matching Amendments (federal agency records)
 - ECPA (government wiretap)
 - Patriot Act (compels disclosure)
- FTC – Unfair or deception trade practices
 - Cannot violate posted TOS or privacy policy; potential liability
- EU Directive
 - Focuses on an individual’s right of privacy rather than US market approach
 - Protects personal information maintained by a broad range of companies across different industries and restricts the flow of personal data outside the EU
- Data breach/identity theft statutes
 - FACTA (“FCRA”)
 - Data breach notification laws
 - ◇ No federal law
 - ◇ California S.B. 138
 - ◇ Inconsistent state laws
 - Criminal identity theft statutes
- Other relevant laws and proposed legislation
 - CAN-SPAM Act (commercial e-mail; preemptive)
 - Anti-Phishing Act of 2005
 - Spyware (state level prohibition or regulation)

D. Piracy

- Perception or reality of increased risk associated with electronic format
- P2P models (precedent and opportunity)
- Digital Rights Management (“DRM”)
 - DRM focus is traditionally on the rights of copyright holder
 - Control file access (e.g., number of views, length of views)
 - Control use (e.g., ability to alter, share, copy, print and save)
 - DRM approaches to secure content:
 - ◇ Containment – encrypt content to limit access to authorized users
 - ◇ Marking – place watermark, flag or XrML tag on content to signal to a device that the media is copy protected (distribution approach)
 - ◇ Authentication (by content, device, users)
 - ◇ Secure execution environment
 - DRM may be a threat to:
 - ◇ Privacy concerns – to the extent that methodology requires identification and authentication data; a user must reveal his or her identity and rights in order to access content; ability to profile; lack of anonymity
 - ◇ Open source software development/innovation – if the copy protection is embedded into the devices, this may endanger development of open source software; e.g., many DRM systems work with Windows OS to the exclusion of Linux and Mac users
 - DMCA challenges (e.g., reverse engineering)
 - Fair use of copyrighted content – need to be able to transfer to a portable device and operate seamlessly in a manner that is consistent with current law and related consumer expectations.

IV. Regulatory Issues & Challenges

- Industry specific
- Merging industries and conflicts between
- State v. federal law

V. Summary – Role of Digital Opportunities in Allowing Businesses to “Stay in the Game” and Challenges

- Opportunities
 - Ability to monetize existing assets and create new revenue shares
 - Provide support for and evolve traditional business models and objectives
 - Formulate a strategic and forward-looking approach to licensing and development of IP
 - Afford additional opportunities in the form of global reach, remote access, multiple devices, technology-enabled distribution and other process-driven efficiencies, targeting (e.g., Wi-Fi or WiMax allowing expansive use)
 - Integrated approach to consideration of various issues and the impact on business objectives and flexibility
 - Enable and leverage new demographic and geographic reach

- Challenges
 - Likelihood of adoption (i.e., relevance, ease of use)
 - Time frame for adoption (i.e., timing of adoption, ROI expectations)
 - Coexistence with traditional business models
 - Privacy, security and piracy
 - Managing and negotiating with multiple stakeholders
 - Complex ownership rights