VALUE ADDED, VALUES DRIVEN.℠

RFID: Customer Contracts, Privacy, and the Law

RFID Regulatory and Legal Issues

Ronald E. Quirk, Jr., Esq.

VENABLE LLP

RFID Packaging Technology

- Radio Frequency Identification (RFID) Automatic Identification and Data Collection (AIDC) Technology
  - "High-Powered, Wireless Barcode"
    - No line-of-sight required
    - Can hold detailed information about individual items; not just manufacturer and product

RFID Components

- **Tags: Passive or Active**
  - Semiconductor chips (both)
  - Antenna (both)
  - Battery (active tags only)
  - Active Tags
    - Read range up to 100 feet
    - $10-$40 each
  - Passive Tags (focus of this session)
    - Read range 10 to 30 feet
    - 13 cents – 30 cents each
- **Reader**
- **Host Computer System & Application Software**

RFID: Low Power Wireless Transmission

- Data is transferred via low power radio waves between tags and the reader
- Reader sends out signal, received by all tags within the radiofrequency (RF) field, and tuned to same frequency as reader
- Tag picks up the signal with its antenna, then transmits stored data (e.g., serial number, configuration, last location) to the reader: "backscattering"
- Reader receives the tag's signal, decodes it, and transfers data to host computer system

FCC: Little Regarded RFID Player

- All uses of radio frequency bands in the U.S. are regulated by the Federal Communications Commission (FCC), including RFID
  - Low power RFID systems do not require a license to operate, but are subject to other regulations:
    - Secondary spectrum use
    - Specific frequency bands
    - Power limits
    - Equipment certification

Importance of FCC Regulations

- FCC Regulations are Important to RFID Systems Manufacturers and Users Because:
  - They Limit the distance from which tags can be reliably read
  - FCC can force noncompliant systems to be shut down, and can issue substantial fines for regulatory violations

FCC Rules for RFID Systems

- RFID Operations are Regulated under Part 15 of the FCC's Rules for Low Power Devices
  - RFID systems are "secondary" spectrum users:
    - Must not cause harmful interference to other wireless operations
      - FCC lists RF emissions limits for unlicensed devices in Part 15, based on frequency band used
      - If RF emissions limits are exceeded, system must be shut down until problem is solved
    - No interference protection from other wireless operations

Selected U.S. RFID Frequency Bands

- **Low Frequency: 125 – 134 kHz**
  - Read range: to 18 inches
  - Typical uses: card key, access control
- **High Frequency: 13.110 – 14.010 MHz**
  - Read range: 3 – 10 feet
  - Typical uses: baggage handling, tracking equipment in hospitals
- **UHF: 902 – 928 MHz**
  - Read range: 8 – 30 feet
  - Typical uses: supply chain management, materials management
  - Most widely used RFID frequency: robustness & reading range

Restricted Frequencies

- RFID systems may not operate on unauthorized frequencies
  - FCC lists restricted frequencies in Part 15
    - Low power operations will be shut down if they operate on restricted frequencies

RFID Regulatory Classification

- Because RFID devices transmit low power radio waves, they are classified as “intentional radiators” by the FCC
  - UHF intentional radiators subject to additional operational restrictions under FCC Rule Section15.247
    - UHF reader transmitted power limit: 1 watt
    - FCC compliant RFID systems typically use frequency hopping spread spectrum modulation techniques to benefit from maximum reader transmitted power allowances
      - If a UHF reader “hops” across a minimum of 50 frequencies, and uses a directional antenna, it may operate at a transmitted power limit of 4 watts

RFID Equipment Certification

- **With Certain Specified Exceptions, FCC Rules Require that RFID Readers and Other Intentional Radiators Must Be Certified and Labeled as FCC Compliant Before They Can Be Marketed or Operated**
  - Certification is an equipment authorization issued by the FCC based on representations and test results submitted by the applicant
    - Main purpose of certification is to ensure that the device's RF emissions are within the FCC specs in order to prevent interference with other devices

RFID Equipment Certification

- **Certification Process**
  - Obtain an FCC “Grantee Code”
    - Application on FCC website
    - $50.00 fee
  - **File an FCC Form 731**
    - Technical report
      - Manufacturer name & address
      - Installation & operating instructions
      - Block diagram of device
      - Test results (use certified lab)
      - FCC identifier: grantee code & product code
      - Photos of device & components
      - $545 fee

RFID Equipment Certification

- **After Certification the Device Must be Labeled as FCC Compliant**
  - Label contents
    - FCC certifier
    - Notation on device:
      - This device complies with Part 15 of the FCC's Rules
      - This device may not cause harmful interference
      - This device must accept any interference received, including interference that may cause undesired operation

Responsible Party

- **Responsible Party for FCC Compliance**
  - Rules state that RP is whomever seeks grant of the certification: for practical purposes that is usually the manufacturer, importer, or vendor
  - The RP is also responsible for ensuring that the certified devices meet the FCC specs when operated
    - If another party modifies the device to increase power, change frequency, etc., that party becomes the RP, and the device must be recertified

Temporary Certification Exemptions

- **Sales Contracts**
  - Uncertified intentional radiators may be "marketed" by manufacturers and wholesalers when they have sales contracts with the retailer stating that delivery is contingent upon FCC certification
- **Trade Shows**
  - Uncertified intentional radiators may be advertised or displayed at trade shows, but a notice must be conspicuously placed in the ad or located nearby the device:
    - "This device has not been authorized as required by the rules of the FCC. This device is not, and may not be, offered for sale or sold or leased, until authorization is obtained"

Temporary Certification Exemptions

- **Business Sales**
  - A pre-certified intentional radiator may be offered for sale to a business or scientific user, as long as the prospective buyer is notified in writing at the time of the offer that the device is subject to FCC rules, and it will be certified prior to delivery

Temporary Certification Exemptions

- **Operations**
  - "Pre-authorized" intentional radiators may be operated (but not marketed) for the following purposes
    - FCC compliance testing
    - Trade show demonstrations (w/notice)
    - Exhibitions at commercial, scientific, and medical locations (w/notice)

FCC Sanctions for Noncompliance

- **Communications Act Section 302(b)**
  - Prohibits manufacturing, sale, importing, selling, offering for sale, or shipping, any electronic device or system that does not comply with FCC regulations
  - **Communications Act Section 501**
    - $10,000 base fine or two years imprisonment for willful violation of the Act
  - **Communications Act Section 502**
    - $500 per day for willful violation of FCC regulations
    - Each device sold is a separate violation
    - Each rule violated is separate violation

FCC Sanctions for Noncompliance

- **In Addition to Fines, FCC Will Order That Devices Must Not be Sold or Operated Until Problem is Fixed**
  - Responsible Party and sellers of devices are at risk for sanctions: "off the shelves" or "out of the ground"
  - Any new version of device must be certified before operation and marketing

FCC Cracking Down

- **Unlicensed Operations are Now on the "Front Burner" at FCC**
  - Former FCC Chairman Powell strongly advocated unlicensed communications due to spectrum scarcity, new services, etc.
    - Rulemakings to encourage use of unlicensed devices
    - More and more unlicensed devices are crowding the spectrum
    - Office of Engineering and Technology (OET) is getting very strict about rule violations involving unlicensed devices

Contract Issues & FCC Regulations

- **Responsible Party**
  - RP status generally cannot be “assigned” to another party
    - But, contract should state that no modifications to equipment may be done without RP’s written approval
      - Other party is on notice that RP status will change in the event of a major modification of RFID equipment

Contract Issues & FCC Regulations

- **Warranties & Disclaimers**
  - End-users would want vendor to warrant:
    - Equipment is FCC-compliant
    - Equipment in violation of FCC rules will be fixed or replaced at no charge
    - Compensation for downtime while equipment is being replaced in event of FCC violation

Contract Issues & FCC Regulations

- **Warranties & Disclaimers**
  - Vendors should specify pertinent FCC operational FCC regulations (power restrictions, etc.) and state that it will not warrant equipment if used in violation of FCC regulations
  - Vendors should disclaim consequential damages, such as lost revenue, for regulatory violations

Contract Issues & FCC Regulations

- **Indemnification**
  - Vendor should insist that end-user indemnify vendor in event of third party lawsuit if equipment is used in violation of FCC regulations
  - End-user should insist that vendor indemnify in event of third party lawsuit if equipment causes interference with no FCC violation by end-user
  - Mutual indemnification clauses are typical

Contract Issues & FCC Regulations

- **Contracts Involving a Manufacturer or Importer of RFID Equipment**
  - **Get assurances in writing:**
    - Equipment complies with all pertinent FCC regulations
    - Equipment is properly labeled
    - An Accredited Telecommunications Certification Body (TCB) performed the tests (or at least a reputable lab)
    - Be very wary of foreign labs performing tests
      - Even if FCC certifies equipment, if tests are done incorrectly, the RP could still be forced to modify or replace the equipment if FCC rules violated

Contract Issues & FCC Regulations

- **Frequencies**
  - Be sure RFID readers are designed to operate on authorized U.S. frequencies (e.g., UHF 902-928 MHz)
  - If planning for foreign operations, readers & tags should be functional over the full range of UHF frequencies: 860 - 960 MHz
    - Europe RFID UHF Frequencies: 865-868 MHz
    - Japan RFID UHF Frequencies: 952-954 MHz

RFID Privacy Issues

- **The Wal-Mart & Target Mandates Have Caused States to Rapidly Introduce RFID Privacy Bills**
  - In 2004, six states introduced RFID-specific privacy bills
  - In 2005, fifteen states introduced RFID-specific privacy bills
  - Many bills provide that retailers inform consumers if an item contains an RFID tag and/or destroy the tag at point of sale

RFID Privacy Issues

- **Main Fear is Collection & Dissemination of Consumer Data**
  - State lawmakers & privacy groups say that they are concerned that implanted tags will enable the merchant to track individuals by linking consumer's name and credit card information (at point of purchase) with a serial number from an RFID tag attached to a purchased item.
    - If tag is not destroyed, readers will pick up personal information from tags and ads will appear on screens targeted toward that consumer

RFID Privacy Issues

- **None of the RFID-Specific Privacy Bills Have Been Passed into Law**
  - Groups such as the Retail Industry Leaders Association (RILA) have successfully lobbied against them
- **But, states continue to introduce new bills monthly**

RFID Privacy Issues

- **Item-Level Tagging is Big Privacy Concern**
  - For now, privacy laws may not be too much of a concern for suppliers and packagers who do business with retailers:
    - Mainly case and pallet level tagging
    - Privacy concerns will arise when individual items are required to be tagged, as Wal-Mart and Target want to do eventually

RFID Privacy Issues

- **FTC: Database Security is Privacy Concern**
  - In March 2005, the Federal Trade Commission (FTC) issued a report advocating a “hands off” approach to RFID regulation
  - FTC stated that privacy is linked to database security
    - Companies using RFID to collect and augment personal data should implement measures to protect that data
    - FTC may revisit RFID regulation of companies do not secure their databases to adequately protect personal information

RFID Privacy Issues

- **Privacy Will be a More Serious Concern When FDA's Electronic Drug Pedigree is Implemented**
  - 2004 Report by Food and Drug Administration (FDA) Recommends RFID as Anti-Counterfeiting Measure
    - Sealing bottle at manufacturer, attaching tag w/unique EPC, using RFID readers to track unit every step of way to retailer would create "pedigree," a secure record showing that drug is safe & genuine
    - Pedigree "recommendation" for all pharmaceutical companies in effect by 2007

RFID Privacy Issues

- **FDA's Electronic Pedigree Will Likely Result in RFID Privacy Laws Specific to Pharmaceuticals**
  - As the drug pedigree deadline draws near, many states will likely be introducing bills that would require pharmacies to, at least, destroy RFID tags upon sale
    - Consumer advocates will push state legislators to pass privacy bills, with the idea that individuals' drug purchase information must be protected.
    - Placement of tags on packaging will likely be affected

RFID Privacy Issues

- **HIPAA May Influence RFID Drug Privacy Laws**
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA): federal law creating set of privacy requirements for medical records and patient health information
  - Dept. of Health & Human Services (HHS), FDA's parent agency, administers and enforces HIPAA provisions

RFID Privacy Issues

- **Major HIPAA Privacy Provisions:**
  - Mandatory notification of privacy practices informing patients about how their personal medical information will be used
  - Ban on marketing to patients with use of information contained in medical records
  - Right to demand that communications with medical personnel be kept confidential

RFID Privacy Issues

- **Privacy Advocates Concerned about RFID & Medical Records**
  - RFID could compromise security of medical information
  - HIPPA ban on marketing based on medical records could be violated if RFID tags are not destroyed after purchase of drugs
  - Insurance companies could use patient information to deny coverage

RFID Privacy Issues

- **Bottom Line on Privacy**
  - Privacy issues will become more pressing as retail and FDA RFID mandate deadlines approach
  - Stay abreast of current developments in privacy laws
  - Ensure that databases containing personal information are secure

Conclusion

- With RFID Poised for Rapid Growth, It is Critically Important to Know How to Navigate Within the Regulatory Environment
- Ignorance of the Law Could Impede Deployment of Even the Most Efficient and Well-Designed RFID Systems
- Stay Aware and Informed

Appreciation

THANK YOU