Managing supply chains effectively is becoming increasingly challenging as outsourcing and offshoring increases, and globalization makes marketplaces more competitive. Supply chain management has emerged as one of the key areas for firms to gain a competitive advantage (9). For over two decades, information technology (IT) has provided the impetus for more effective supply chain management. In the 1980s, electronic data interchange initiatives enabled firms to deal more effectively with suppliers. In the 1990s, supply chain innovations such as vendor-managed and co-managed inventory and configure-to-order supply chains would have been impossible without IT. Today, it is widely believed that the use of radio frequency identification (RFID) technology will enable substantive supply chain transformations.2, 3, 5

Much of the recent RFID discourse has centered on its potential to improve supply chain management.2, 3 RFID can benefit retailers and upstream supply chain members. It can help reduce counterfeiting, theft and the bullwhip effect; it can improve on-shelf availability, customer service, inventory management, downstream forecasting, warehouse and back room operations.

Preliminary results suggest that Wal-Mart is benefiting from its RFID initiatives1 and many retailers around the world have begun RFID trials. If RFID investments are to pay off through better supply chain management, firms will have to modify many of their processes to take advantage of the real-time individual item information that will be available. It is through these RFID-enabled process innovations that firms can gain competitive advantages. Consequently, supply chain processes and data can be among the most confidential information for firms. To date, supply chain process innovations have been protected from competitors by U.S. laws. However, with RFID deployment, current laws may no longer offer protection.

Corporate intelligence (legal information-gathering about competitors) and espionage are common across all sizes of firms.6, 8 Until now, gathering intelligence about a competitor’s supply chain has been limited by both cost and legal constraints. The time, effort and visual or physical actions necessary to gather useful information about a competitor’s supply chain make it costly. In addition, it can also be illegal, because current laws against burglary, theft of trade secrets, copyright infringement and unfair competition limit corporate intelligence. However, because RFID data is passed wirelessly between the tag and the tag reader, and because tag data may be created by many different firms in a supply chain, RFID deployment will make it easier for competitors to gather intelligence at a low cost.12

Striking a balance between supporting innovation and facilitating competition is at the heart of capitalism as well as the production and use of knowledge. On one hand, scientific and technological innovations expand the frontiers of knowledge and contribute to the technological progress that affects how people live and work. On the other, competition in the marketplace enhances economic welfare; it is through competition that some of the benefits of innovation are passed on to consumers. Estimates suggest that ap-
proximately 70 percent of the market value of U.S. firms lies in trade secrets and intellectual properties. In the U.S., there are laws that seek to reward innovation (e.g., patent, copyright, and trade secret laws), and other laws that seek to promote fair competition (e.g., the general tort of unfair competition). When RFID is deployed, existing laws could legally allow competitors to quickly and inexpensively learn a great deal about the functioning of a firm’s supply chain and changes to supply chain processes, reducing the benefits that firms gain from supply chain process innovations. The laws aimed at rewarding innovation and promoting competition may fail to prevent such intelligence gathering.

RFID vs. Barcode Use

RFID technology could eventually replace most barcode-based systems currently used to identify and track products in a supply chain (e.g., UPC™, ISBN™). RFID is an electronic replacement for barcode-based identification. An RFID tag is a small object that can be attached to or incorporated into any object. RFID tags contain silicon chips and antennas that enable them to receive and respond to radio-frequency queries from an RFID reader (transceiver). The simplest RFID tags include an electronic ID that can be read by a tag reader. The Electronic Product Code™, or EPC, is a current standard for RFID identification. The EPC was developed by EPCGlobal, Inc., a standard setting organization for the implementation of RFID worldwide. A key difference between RFID-based systems and the identification systems they will replace is that with RFID it is not necessary to have a physical or visual (i.e., line-of-sight) connection between the tag and the tag reader. Moreover, RFID tags can contain much more information than the barcode tags they replace. At the simplest level, an RFID tag’s EPC can identify the manufacturer, the product type and even a serial number for the tag, allowing individual items to be identified. More advanced tags can store additional data as an item moves through the supply chain (e.g., time, location, temperature).

Two types of RFID tags are relevant to this discussion: write-once tags and re-writable tags. Typically, write-once tags are written by the manufacturer and identify the product item. This is similar to what happens today with barcode systems. Manufacturers place barcodes on products. The data on re-writable tags can be written by different firms as a product travels through the supply chain.

Consider the simple supply chain depicted in Figure 1. Firms M1 & M2 are product manufacturers who ship their products through T1, a transportation firm. These products are delivered by T1 to wholesalers D1 & D2. Transportation firm T2 moves products from D1 & D2 to retailers R1 & R2, from where they are sold to consumers. If re-writable tags are used, manufacturers M1 & M2 can write the product item identifier. The time when the product is picked up from the manufacturer and delivered to the distributor (e.g., D1) can be written to the tag while it is in the possession of firm T1. The time when the product is picked up from D1 and delivered to retailer R2 can be written to the tag while it is in the possession of firm T2. Essentially, data can be written to a tag while the product is in the possession of different firms in the chain.

When products are identified by barcodes, firms are prevented from acquiring useful information about a competitor’s supply chain for two reasons: (1) because human actions are necessary to acquire the data; the barcode must be scanned as the product moves through the chain, and (2) much of the information useful to competitors is embedded in the proprietary computer systems of individual firms in the supply chain (e.g., firms T1 & T2 in the example). As a result, practical considerations and current laws protect this information from competitors. It should be noted, however, that competitors are free to use supply chain data that is in the public domain, such as catalogue or part numbers, or even a product’s UPC or ISBN, even when the data is created and controlled by a firm. Such data is neither copyrightable nor secret, and thus not owned by the firm.

As noted earlier, the use of RFID may allow competitors easy access to data that could prove harmful to a firm. For example, a firm could purchase a competitor’s products from several locations and monitor the locations’ replenishment dynamics. Tag data could be read in a store or as merchandise is unloaded; an agent could walk down an aisle with a tag reader or place a reader next to a supply route. Unique product item identification can be valuable to firms, but may also prove to be extremely valuable to competitors. Individual item identification could allow competitors to learn a great deal more about the firm’s supply chain and processing and delivery systems than they currently can. When re-writable tags include processing data, it could be easier for competitors to obtain valuable information about a firm’s supply chain processes. It should be noted that although the effective read-range of the cheapest tags is only a few feet today, technological improvements continue to increase read ranges.

U.S. Laws Governing Data Protection

Legal protection for data under U.S. law falls into three primary categories: trade secret law, copyright law, and contract law. Table 1 provides a synopsis of these laws in the context of RFID tags. The key issue is whether current
laws provide firms with proprietary rights to the data.

In a supply chain context, there are two types of data that firms may need to protect from competitors: product identification data, and product processing data.

**Protection of product identification data on a tag.** In general, under U.S. law, individual product identification data, such as the EPC™, cannot be protected by trade secret or copyright law. First, tag identification data is the one piece of information a tag freely broadcasts when queried by a tag reader, and is therefore unlikely to be protected under trade secret law.

Second, although each EPC is unique, the courts have consistently held that information such as individual product codes is not copyrightable. A product code is generally held to be a single piece of factual information, lacking sufficient originality to be protected by copyright.

Protection of processing data on a tag. Information on tags that include processing data could be of great value to a competitor. Such tags may contain data obtained from attached sensors or data based on communications with readers. These compilations of processing data could provide valuable insights to competitors about a firm’s operation and distribution systems.

Determining trade secret protection for processing data is the same as for the identification code. The first question is whether or not the firm has taken reasonable steps to maintain secrecy of the data. Unlike the identification code, however, the need to transmit processing data is likely more limited. If the tag freely transmits all data when queried by a reader, this would not be considered a reasonable effort to maintain secrecy. However, if access to the processing data were restricted through the use of a challenge-response protocol, it could make unauthorized access illegal. Clearly, encrypting processing data would be the best way to ensure that unauthorized access is illegal. In essence, the protocols employed for processing data will determine whether or not access by competitors is illegal.

Firms may also claim protection for processing data as a copyrightable compilation of data. Copyright law protects factual compilations of data as an original work if the method of selecting, arranging or coordinating the data is unique and original. However, such protection would not extend to compilations of processing data. First, the law does not protect works that present information in a fashion that is commonplace (e.g., the alphabetical list of names in a telephone directory) because there is no original selection or arrangement of the information. For example, compiling a list of dates when a tag was accessed by a reader as it moves through the supply chain would likely not be protected. Second, compilations that are generated automatically based upon pre-determined criteria are not protected since there is no original selection or arrangement of the data. Even if the system that is used is original, no person is exercising judgment to select and arrange the individual pieces of data; the software does it automatically. Therefore, this data will not be protected by copyright.

Even if compiled data were protected by copyright law, another problem arises in determining who owns the copyright. In the example, manufacturers would install the tags with the item ID, while pickup and delivery times would be recorded on the tags while they are in the possession of firms T1 & T2. Thus, each firm in possession of the tag could be the author of the data generated while they possess the tag. This raises the question of whether the data thus compiled consists of several separate works, or a single work co-authored by the different parties creating the database.

Firms could circumvent these problems with their supply contracts. They can agree to limit access to tag data,
RFID Tag Decisions

One of the advantages of RFID over barcodes is that individual items can be identified. The value of individual item identification to a firm will vary by product. For example, individual item identification is likely to be more valuable if the product is perishable than it would be for non-perishable products. Another advantage of RFID is the ease with which misplaced products can be located and tracked in a store or warehouse. This information could be more valuable for high-cost, small-size items than it is for low-cost, large-size items. Essentially, product characteristics will determine what type of information (ID only, or ID and processing data) is most beneficial for different products. As a result, firms and industries are likely to consider different types of RFID tags for different products.

Supply chain visibility is very important to effective supply chain management and can be improved with RFID. Visibility can be achieved in different ways, with the choices affecting intelligence gathering. For example, information about a product item as it moves through the supply chain can either be stored in a tag or in the computer systems of each firm in the supply chain. In the example used earlier, trucking companies T1 and T2 can store the information about pickup and delivery time in their own computer systems. These trucking companies could allow supply chain partners access to this information to increase visibility. If tags only include individual item product IDs, with processing data being stored in the computer systems of firms in the chain, tag costs will be low, while the costs of sharing information across supply chain partners will be high. In this case, access to processing data will be protected from competitors, as it is with current barcode-based systems. If, instead, the data is stored in a tag, tag costs will be higher (re-writable tags are more expensive), but the costs of sharing information across supply chain partners will be lower. In this case, competitors could legally access processing data quite easily. The more information that is stored in a tag, the easier it will be for competitors to gather useful information about a firm’s supply chain, notwithstanding any legal restrictions against accessing or using the data.

Conclusion

The potential for RFID to make supply chains more effective and to improve productivity is widely acknowledged. There is a caveat; competitors could have much easier access to supply chain data and could learn of a firm’s supply chain innovations far more quickly than in the past. Until now, a major target of corporate intelligence and espionage has been product innovation [6, 8]. Firms gather information on products under development by competitors. It has been difficult for firms to learn about a competitor’s supply chain process innovations. However, implementation of RFID could change that. Tagged objects in the supply chain will make it much easier for firms to gather valuable supply chain information about their competitors.

For firms introducing supply chain innovations based on RFID tags, trade secret and copyright law provide only limited proprietary rights to the data in these tags. Moreover, there is no clear answer as to which firm has what rights regarding tag data. Also, any contracts addressing these issues would only bind the parties to such contracts. As a result, firms will have little or no legal recourse when competitors access this information.

Firms and industries have some options available to limit a competitor’s legal access to tag data:

- Technology-based approaches can be used to restrict access to tag data (e.g., encryption, passwords, pseudonyms, or blocker tags) [7]. The use of such mechanisms to protect the data will often make it illegal for competitors to access the data. However, technology-based solutions pose other problems. For example, using passwords to protect tag data requires that the tag reader know the identity of the tag in order to send the appropriate password. Encrypting tag data imposes another requirement – a third-party (e.g., EP-CGlobal, Inc.) must typically manage and distribute the keys necessary to encrypt and decrypt the data.7 Technological solutions will increase costs and may require third-party involvement, which could affect deployment.

- In the short run, contracts between trading partners can be used to require partners to protect the data from competitors and to forego data ownership rights. However, the contracting approach only binds the firms signing the contract.

- Firms can push for the enactment of new laws to protect RFID data. This will take time and it is unclear what form new laws will take. Law makers seeking to promote economic growth must carefully weigh innovation rewards against the need to promote competition. An often-discussed change would provide specific protection for databases, apart from copyright or other law.

Finally, the answers to a number of RFID-related questions that many firms must address in the near future are affected by the issues raised here. For example, how should the fact that competitors may have easy access to supply chain data affect:

- the benefits of RFID-engendered process innovations?

- a firm’s decision to support RFID deployment?

- RFID tag design decisions that a firm supports? or,

- a firm’s support for technology-based solutions to the problem?

RFID, like many technological innovations, presents new challenges to our legal and economic systems. Until the law catches up, managers face many RFID-related decisions in a unique and uncertain environment.

References


Brian L. Dos Santos (briandossantos@iitbombay.org) holds the Frazier Family Chair in Computer Information Systems at University of Louisville’s College of Business.

Lars S. Smith (lars.smith@louisville.edu) holds the Samuel J. Stallings Chair at the University of Louisville’s Louis D. Brandeis School of Law.

© 2008 ACM 0001-0782/08/1000 55.00