Security and Privacy in the New Retail Ecosystem

Eric Rosedale and Françoise Gilbert, New York Law Journal

June 26, 2017

Mobile phones, mobile applications, sensors, beacons, connected objects, and analytics are transforming not only the way in which consumers shop but also how manufacturers and retailers determine what to sell, and when, where, or how to sell it. The use of these technologies, which is rocking the retail sector, raises important legal issues for developers, owners, and operators of retail projects. This article focuses on legal and compliance issues raised by this paradigm shift.

New Shopping Experience

The stores that win today's race to attract customers tend to be those that have invested resources in merging the online, mobile, and physical store experiences to develop a new ecosystem that connects physical and digital worlds. This multichannel strategy seeks to provide consumers with a seamless shopping experience, both online and in a brick and mortar store.

In a digital world, effective retailing combines the use of physical, Web, or mobile app stores. In brick and mortar stores, retailers increasingly rely on digital capabilities that could, for example, recognize a returning visitor and serve up data about that visitor's purchase history to help sales associates deliver high-touch service. New forms of telemarketing may involve artificial intelligence, for example through the use of intelligent sales assistants.

Other examples of new technologies employed by retailers are:

- Personalized digital coupons delivered to a mobile device upon entering the store;
- Ability to call for assistance or check inventory via mobile device;
- Shopping carts equipped with tablets able to assist a customer in navigating the store, based on the customers' digital shopping list;
- Interaction with the customer's wearable devices to suggest products based on desired activity levels tracked; or
- Smart mirrors to "try on" different garments virtually.

These methods of interacting with consumers rely extensively on the collection of data about individuals. When this data is associated with the consumer's email address or smartphone ID, it is

likely to be deemed "personal data" and trigger a wide range of privacy and cybersecurity laws and the related compliance requirements.

Legal Framework

The U.S. federal and state privacy and cybersecurity legal framework restricts the way in which personal data may be collected, used, and shared; grants individuals privacy rights; and requires businesses to ensure the security of the personal data collected.

In particular, businesses are expected to provide detailed disclosures of their collection, use, or sharing of personal data, and limit that use and sharing to the purposes so disclosed. The collection of some categories of personal data, such as precise location data, may be restricted and may require the individual's prior affirmative consent. Direct marketing, in the form of commercial email, text messages, and telemarketing, is also restricted.

Adequate security measures may be required to protect personal data. Further, almost all U.S. states require businesses that suffer a breach of security to promptly notify the affected consumers and/or the relevant regulatory authority of the existence of the breach under certain circumstances.

Enforcement actions by regulators and class action lawsuits filed on behalf of consumers regarding personal data issues arise frequently. Fines and damages may be assessed, and some businesses may find themselves under the direct supervision of their governing agencies for significant periods of time.

The Minefield

The technologies used to create today's new shopper experience present potential areas of liability for developers, owners, and operators of retail projects under the existing U.S. privacy and cybersecurity framework. Consider, for example, beacons, sensors, and geo-fencing technologies. They are intended to allow interaction with consumers as they enter the store, and delivery of personalized messages to those who have downloaded the brand's app. They may allow tracking consumers' paths through a store to help improve store layout and merchandise placement strategies. However, in both cases, the collection of precise location-based information may require the consumer's prior consent.

Similarly, fingerprint recognition, facial recognition, iris scanning, and voice identification can be used to improve targeted marketing efforts, boost security, and expedite payment. However, biometrics information laws may require prior notice and consent and the use of appropriate security measures.

Artificial Intelligence can help create a new "expert personal shopper" experience by allowing interaction with potential customers to identify their needs, suggest an appropriate product, and direct them to the aisle where the product is located. However, in addition to the general rules addressing the collection of personal data, there may be restrictions on the massive collection of personal data necessary for the robot to act intelligently and interact with the consumer. There may also be other liability implications, for example, if the robot becomes aggressive.

"Magic" mirror technologies will enable consumers to try on virtual outfits in different colors and styles. However, this entails the collection of personal data, such as measurements, which, when combined with the consumer's contact data, would trigger the application of privacy laws. Visual product search technologies can be used by shoppers to take photos of a product and find similar items in a store. However, any re-use of this data for interest-based advertising is likely to trigger the application of the laws on interest-based advertising and profiling.

Virtual showrooms using augmented reality or virtual reality technologies for the furniture market allows consumers to try before they buy. What happens if the store fails to use appropriate security measures to protect the photos of the consumer's home and possessions, and the database is hacked, triggering a series of burglaries of these homes?

Self-checkouts and enhanced point of sales systems help expedite payment transactions and build loyalty. However, the secondary use of the payment data, such as sharing with analytics companies for marketing, consumer profiling, interest-based advertising, and other purposes raises significant privacy issues. Further, the use of self-checkouts and enhanced point of sale is likely to rely on Wi-Fi or Bluetooth technologies, which might expose businesses to potential security breaches.

Risk Management

The sophisticated uses of personal data to gain market distinction or drive operational efficiency exposes the retail ecosystem to the risk of being caught in the complex net of data privacy and cybersecurity laws, regulations, guidelines, and jurisprudence. When counting the many ways in which new technologies and tools could be used to extract more knowledge about potential customers, businesses should also count the many ways in which they might be intruding into personal lives, drawing conclusions that should be ignored, making assumptions based on inaccurate data, or exposing individuals to risks of identity theft.

When contemplating or evaluating a new project that includes the use of personal data, consider:

- Assessing what data is to be collected, the purposes for which it will be used, how it will be stored, transmitted, or destroyed, and for how long it will be kept.

- Evaluating the legal and regulatory landscape affecting the proposed practices, and their implications for your business.

- Building a data collection and use plan that incorporates privacy and cybersecurity concerns from the beginning, so that the practices, tools, and technologies proposed to be used offer the safeguards necessary to protect consumers and prospects, and their respective data.

- Developing and documenting a detailed data protection program that takes into account the privacy and security compliance obligations of the business and the numerous risks to the personal data and the privacy rights of individuals.

- Ensuring that service providers, subcontractors, tenants, or subtenants do the same. It is important to record these obligations in contracts, and pay attention to liability and indemnities for third-party claims arising from a third-party tenants' data fraud and security breaches.

- Ensuring that all employees are sufficiently trained to understand and address these risks.

- Reviewing, improving, or expanding the insurance coverage as necessary. General liability insurance policies typically do not cover the costs associated with cybersecurity risks, such as a security breach. Landlords and tenants should discuss cyber insurance or other appropriate coverage with risk managers or insurance brokers.

- Reviewing lease documentation to confirm compliance with insurance requirements and assess potential exposure if a breach of security or other cybersecurity incident occurs.

- Revisiting these steps and measures periodically. Technologies change, risks change, laws change.

Conclusion

The convergence of new shopping trends, data collection, and analytics technologies is reshaping the traditional retail store business model while creating a new array of opportunities for physical brick and mortar retail developments. Businesses should take steps to increase their awareness and understanding of the numerous legal, compliance, and risk pitfalls associated with the use of new technologies that rely on the connection of personal data of consumers to better serve their customers. The obstacles should be addressed with method, structure, and precision and with due appreciation for the importance, and fragility and sensitivity of the personal data being collected and processed and the applicable legal and compliance requirements.

Eric Rosedale, head of international real estate practice development at Greenberg Traurig, is a shareholder in the firm's New York and Amsterdam offices. Françoise Gilbert is a shareholder in the firm's Silicon Valley office.
