Hashed & Salted | A Privacy and Data Security Update
September 2022

Commercial Surveillance: Technology, Government and Civil Rights Implications

As brick-and-mortar stores struggle to compete with online retailers' data access, physical surveillance technologies have become increasingly sophisticated, enabling the creation, monitoring and analysis of customer data in real time. Artificial intelligence (AI)-powered cameras equipped with facial recognition technology (FRT) and object detection have been implemented alongside thermal-sensing people-counters and tailored marketing messages. Companies considering adding these technologies must carefully assess their benefits and risks in order to boost their bottom line while protecting against liability and reputational harm.

COVID-19 catalyzed the digitization of physical security protocols, as technologically advanced heat sensors, cameras and algorithms began to analyze customers' temperature, social distancing and mask wearing. While passive security cameras—closed-circuit TVs, for example—have long protected physical stores and venues, new technologies allow these same cameras to actively process and analyze data, make predictions about future consumer behavior, and contact the police. The Department of Labor, citing a projected 9.5% increase in global demand for sensors from 2019 to 2025, expects employment in security systems services companies to grow 13.6% from 2019 to 2029. Companies seeking to protect their physical locations from crime, personalize their marketing and build revenue should consider these technologies alongside appropriate risk frameworks and responsible AI values to ensure their successful—and ethical and legal—implementation.

The Benefits of Commercial Surveillance

Companies leading the market in physical security and surveillance have begun to implement technologies enabling the creation and collection of in-store data to improve consumer experiences and store security. Some security systems focus on crime prevention; replacing the human reviewers of dozens of screens, automated systems now can listen for gunshots, detect unusual behavior, initiate alerts and lock doors at the signs of danger. Moreover, video surveillance equipped with FRT can secure venues against threats such as riots and arson, as demonstrated by the use of FRT in stadiums abroad. Beyond general safety and security concerns, the digitization of physical retail has enabled companies to engage in predictive analytics, consumer marketing and inventory management.

Implementing smart surveillance can increase your company's bottom line, boost consumer satisfaction and retention, ensure compliance with state laws, and help physical retailers compete with online retailers. Smart surveillance that previously undergirded many approaches to COVID-19 compliance—from fever monitoring through heat sensors to social distancing monitoring by location—now may be turned into business intelligence systems. Security systems equipped with object detection can automatically alert employees to gaps in stock, ensuring customers always have what they

Attorney Advertising

need in-store. Object detection also can serve to avoid waste—for example, by monitoring the ripeness of fruits and vegetables. Implementing these smart technologies further improves the company's bottom line by increasing in-store dwell time, limiting waiting times at checkout counters, and fueling growing basket and ticket sales. Some companies have gone as far as automating the entire shopping process, building systems to allow consumers' phones to serve as greeter, cashier and marketer all in one.

While online retailers use advertising technologies, cookies and more to build customizable solutions for consumer behavior, physical stores lack access to these data. Effectively competing in the retail marketplace requires systems for tracking, understanding and improving the in-store consumer experience. Some companies provide consumers with radio frequency identification (RFID) wearables to collect and process this data, while others implement in-store smart technologies to create this experience without requiring consumer involvement. Collected data—about time spent making a decision at a shelf, time between visits to the store, favorite repeat purchases and more—can be used to drive business solutions and consumer happiness. The personalization of marketing, coupons and reward programs can increase company growth rates by 6% to 10%. Many consumers then can receive personalized marketing for the items they buy, the items they need and the items they want; often, offering coupons and rewards based on this data can increase customer loyalty and retention.

When choosing the best smart solution for your company, determine your desired level of automation, concurrently existing streams of data and optimal results. Deciding the extent to which automated technologies will play a role in your business requires careful consideration of implementation, monitoring and upgrading costs. Furthermore, building a framework that allows for the implementation and integration of smart hardware and software in your physical stores (from existing online stores) may fill performance gaps between online and offline retail. Defining successful implementation of these technologies, periodically assessing their effectiveness and adjusting their usage accordingly can mitigate risks while increasing revenue, aiding with compliance and creating a competitive advantage.

The Risks of Commercial Surveillance

While technology and AI-integrated surveillance systems have great potential to add value, companies also must carefully consider the risks inherent in adopting these approaches. Cybersecurity, consent and civil rights are just some of these concerns, alongside how to handle law enforcement requests for data. Adequately protecting your business necessitates carefully accounting for these risks during contracting as well as during initial implementation and subsequent monitoring.

Cybersecurity Risks

The data collected from the digitization of retail stores and venues—through applications, point-of-sale information or sensors throughout the store—are often sent to a cloud system, expanding the potential attack surface for cybercriminals. Fortinet, a cybersecurity solutions and services provider, reports that cybersecurity intrusions in retail have long-lasting impacts; 42% of companies that are victims of cybersecurity attacks experienced a degradation in brand awareness, while 40% experienced an operational outage that impacted revenue, and 33% had an operational outage that put physical safety at risk. The risk of infiltration to your data can further implicate consumer concerns about sensitive data shared with third parties. Of course, the interaction between data breaches and liability will be based largely on your industrial sector; sensitive health, child or financial data may raise concerns with regard to the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA) or the Fair Credit Reporting Act (FCRA). Large cybersecurity risks always are looming in the background of retail surveillance, and actively monitoring the systems' protection is key to protecting company reputation and revenue. Contracts between security providers and retailers also should be structured to require immediate notice of data breaches—with failure to do so considered material breach—as a built-in check.

Civil Rights Risks

When implementing advanced AI-powered surveillance technologies, be cautious about the systems and models that make decisions for your company, particularly with regard to predictive technologies; the risks of biased data sets, training models or algorithmic outputs can be quite great.

Predictive technologies use data about the consumer—from gender to shopping history to ZIP code—to generate prognoses regarding best marketing techniques, likelihood to purchase certain objects and more. If your company's security surveillance system uses AI to process data and make predictions, internal controls should be included that pinpoint exactly what data is being used to draw these conclusions and how the AI has been trained to reach conclusions.

FRT, for example, must be equally effective for everyone, not just white males. Unfortunately, many technologies—even those used by law enforcement agencies—have been shown to struggle on this front. Members of marginalized communities—who also are consumers of your brand—may be subjected to greater intrusion as a result of the technology you choose to implement.

While many algorithms will be protected in court by trade secret designation, dealing with accusations of discrimination under Title VII can be harmful to your brand, legal team and C-suite. Further, the Federal Trade Commission (FTC) has announced that using or selling discriminatory algorithms violates Section 5 of the FTC Act, and it threatens that companies must "[h]old yourself accountable—or be ready for the FTC to do it for you."

One approach to allocating and mitigating the risk of bias between technology providers and corporate entities seeking to use these technologies is purposeful contracting. Clearly allocating the risks at an early contracting stage can mitigate liability. The risk of biased outputs is not often borne entirely by one side; rather, systems and internal controls are set up to require security providers to run systematic tests on the biases of their systems and course-correct when issues are identified. For every use case, consider where the greatest risk of bias lies—collection, processing or using the data—and strategically allocate risk accordingly. Moreover, even if your current contracts don't permit audits and testing, when you update those terms, those updates should address future requirements for testing, auditing and transparency. Finally, it is important to note the reputational risks associated with civil rights violations. Loyal customers may find new retailers if they are uncomfortable with the implementation of surveillance technologies, particularly if they identify as a member of a protected class. It is imperative to carefully tailor your surveillance AI systems—and the contracts undergirding their operations—based on the applicable use case, ethical standards and company values. Below, we'll talk more about some best practices for the use of commercial surveillance technologies.

Governmental Risks

The capture and storage of data related to physical commercial surveillance bring up the additional risk of governmental request, or purchase, of collected data. Governmental requests for data—with noncompliance presenting an omnipresent risk of a broader subpoena—can present particular challenges for companies processing sensitive data, particularly in the light of the U.S. Supreme Court's decision *Dobbs v. Jackson Women's Health Organization.* For example, if your AI-powered surveillance system connects to shoppers' phones to determine how far they traveled to reach your store, the storage and processing of this location data may later be requested by governmental actors (such as an attorney general seeking to prosecute a shopper). Although some companies abide by almost all governmental requests for data, many others have internal proceedings with various balancing factors, legal requirements and contractual obligations to abide by before any information is shared.

Concepts of data minimization and data retention policies may assist with establishing internal policies that minimize the risks of intrusive governmental requests—or later subpoenas—which can have drastic reputational effects. Consumer reactions to governmental cooperation varies; ensuring that each decision considers the applicable laws, compliance requirements and use cases can help with outward-facing explanations of your decisions to engage—or deny—governmental actors. These explanations of decision-making further increase the transparency and accountability of your "privacy by design" framework.

The Balancing Act

While security surveillance technologies may greatly increase your company's bottom line, they must be installed with careful contractual language and risk assessments, particularly regarding governmental requests for data and civil rights implications. Carefully building internal policies with regard to these requests, engaging in collaborative contracting in anticipation of these risks, identifying areas of concern

in the cybersecurity space and creating an actionable framework for responsible AI can be imperative to becoming a leader in this space. A recent Accenture report found that although 69% of companies investigated have started implementing responsible AI practices, only 6% have operationalized their capabilities to be responsible by design. Improving customer experience, increasing your bottom line and utilizing cutting-edge technology can be integrated with actionable responsible AI in a solution that adapts to the technology while staying true to your company values, brand and mission.

Client alert prepared by Toby Irenshtain.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com

7049 REV1 09-09-2022