THE NATIONAL LAW JOURNAL
DECEMBER 3, 2012
An ALM Publication

# When discovery clashes with privacy law

Allowing too much business information to accumulate can cause problems. Defendants prefer them, while patent owners seek compensation for willful future infringement.

BY MICHAEL COLLYARD
AND MICHAEL GEIBELSON

No matter the industry or market sector, increasingly robust data-analytic platforms offer business decision-makers new, quantifiable insights into the factors that motivate customers and consumers. At the same time, however, concerns about data misuse have led to a complex set of laws and regulations that impose limits on how businesses treat certain kinds of personal information, known as personally identifiable information (PII).

Businesses that want to use data analytics and comply with those privacy rules have an additional burden when the data in question become or could become part of discoverable information in litigation. Then, businesses must make choices about how to handle PII data, which of it to produce and the justifications to support those decisions. Balancing these data-driven issues requires an understanding of the ever evolving landscape of each competing concern.

Data analytics allow businesses to harness captured data, statistics, algorithms and other mathematical tools to improve decision-making. The more specific the data, the greater the insights they produce, particularly for marketing initiatives. Conversely, every time structured information is filtered, the analytic value diminishes. As a result, a strong business reason exists to maintain and use as much structured information as possible to increase the reliability of the predictive conclusion.

Yet ethical and privacy considerations call into question the full extent of analytics' reach. Governments and regulatory agencies have drafted a wide range of data-privacy rules and regulations to address fair information practices and the concerns data use creates. In the European Union, the E.U. Data Protection Directive (1995) and the Organisation for Economic Co-operation and Development Guidelines (1980) create one set of requirements to protect information that qualifies as PII. The Asia-Pacific Economic Cooperation crafted the APEC Framework, a less well-defined set of guidelines for the protection and use of PII. The United States is a member of APEC and has signed the APEC Framework.

Within the United States, federal and state laws and regulations often are tied to a particular sector or industry. For example, the Video Privacy Protection Act (VPPA) of 1988—enacted in response to disclosure of U.S. Supreme Court nominee Robert Bork's video rental records—prevents disclosure of personally identifiable rental records of "pre-recorded video cassettes or similar audio visual material." Restrictions within the VPPA have motivated online entertainment providers like Netflix Inc. to seek an amendment that would allow consumers to consent to disclosure of rental information as part of their agreements. The Cable Television Consumer Protection and Competition Act of 1992, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act and the Health Insurance Portability and Accountability Act (HIPAA) further illustrate the myriad kinds of industry-specific data-privacy issues addressed by federal legislation.

In addition, the Stored Communications Act of 1986 defines privacy rights in data stored by third parties such as cellphone companies and social-media sites like Facebook and Twitter. There also are recently introduced but nonbinding Federal Trade Commission recommendations on data privacy, pending federal data-privacy legislation and individual state data-privacy laws in all but four states. Each has sometimes differing rules and recommendations regarding the protection and disclosure of PII. At the same

time, standards for internal analytics use of PII continue to evolve.

### AND THEN THERE'S E-DISCOVERY

As electronic discovery practice has moved from infancy to adolescence, businesses seeking to gain control of their ever increasing store of potentially discoverable electronically stored information have begun to implement a recognized set of best practices. More and more, general counsel's offices have helped their organizations recognize the need to design and implement data retention policies that provide for the regular review and elimination of non-necessary data. Policies that allow too much data to accumulate may increase the cost of future, but now unanticipated, litigation. Policies that don't retain enough data may lead to accusations of spoliation and all its attendant consequences.

How data needed for analytics fit into data retention policies can become further complicated once data-privacy considerations come into play. Data-privacy laws may impose retention limitations at odds with data holds and litigation needs. For example, the VPPA and similar state laws limit the amount of time data regarding video rentals may be retained. (Note, however, that the U.S. Court of Appeals for the Seventh Circuit rejected the notion that a private cause of action exists for violation of the retention limits set forth in the act in *Sterk v. Redbox Automated Retail LLC*, 672 F. 3d 535 (7th Cir. 2012). Other privacy laws explicitly limit the disclosure of PII that may otherwise qualify as relevant, discoverable electronically stored information. Employee records containing privileged HIPAA information serve as an easy, but not singular, example.

Adding data analytics into the mix requires a further risk-benefit assessment. Do businesses keep data containing PII allowed by privacy laws even if its retention pushes the limits of best practices for electronic discovery? What modalities exist to protect PII from disclosure for legitimately retained data? It turns out wisdom gained in the electronic-discovery trenches can help companies navigate the complicated intersection of privacy, PII and ongoing data-analytic needs.

### A HYPOTHETICAL

Imagine that a national branded product—say toilet paper—uses its own analytics and discovers that its sales have disproportionately declined in a particular retail outlet. A little additional research shows that the decline began when the retail outlet introduced its own store brand of toilet paper with a logo that the brand holder believes infringes its trademark. The brand holder brings suit and serves discovery requesting sales data and records for a period both before and after the introduction of the store brand.

Imagine also that the retail outlet has a large, robust data-analytics platform to track consumer purchases. The data maintained include purchase dates, individual product stock-keeping unit codes and PII including purchaser name and credit card number. The database has allowed the retail outlet to anticipate purchasing trends and has provided important insights for marketing, inventory, equipment investments and long-term budgeting. The information's value has led to the maintenance of the data over a number of years, and their regular use means they have not been subject to reduction as part of data-maintenance practices. Arguably, all the information in every sales record involving the competing brands of toilet paper is relevant and discoverable, but production of the information risks the disclosure of protected consumer PII.

One would hope the retail outlet would have already recognized the competing electronic discovery and privacy concerns its analytics data present and crafted data-privacy policies that comply with the standards of all potentially affected markets—including international ones. Then, carefully conducted custodian interviews and electronic-discovery tools can help identify the data sources where they exist. That data-privacy policy would help begin to demonstrate the sensitivity the business uses when handling PII in its normal course of business. Once the business purpose and protections have been established, outside counsel can work to protect PII from disclosure in the litigation and defend any discovery efforts to produce it.

Electronic discovery's framework of devices to protect disclosure of privileged information runs the gamut from restricted data pulls agreed to during Rule 26(f) meet-and-confers and judicial protective orders to line-by-line redactions. The retail store, defending its brand analytics, could make its case that its ability to pull sales data separate from PII will provide sufficient information to the national brand, with counsel in an agreed-upon protective order that specifically contemplates protection of PII. Protection of the PII in the litigation format is essential because, although disclosure of PII actually introduced in court enjoys judicial privilege, prohibited disclosures made along the way do not.

Data proliferation offers businesses both opportunities and challenges. Better technologies and increased data-capture contacts have created new opportunities to mine records for insights into critical business decisions and directions. At the same time, companies have learned that keeping unnecessary data can create unanticipated problems in litigation and that PII data require particular sensitivity given the complexity of laws governing data privacy. Good planning and recognition of the multiple and competing issues involved is the best way for businesses to stay ahead of the data curve.

*Michael Collyard (macollyard@rkmc.com) is a business litigator and head of Robins, Kaplan, Miller & Ciresi's L.L.P. electronic discovery practice group. Partner Michael Geibelson (mageibelson@rkmc.com) is a business litigator serving clients in the retail and food and beverage industries.*