Tuesday, August 5, 2014

Expect more stringent regulations over 'big data' to emerge

Hsiao (Mark) C. Mao *is a partner and vice chair of the Financial Services Practice Group in the San Francisco office of Kaufman Dolowich & Voluck LLP. He may be reached at mmao@kdvlaw.com.*

Jonathan H. Yee *is an attorney in the Los Angeles office of Kaufman Dolowich & Voluck where he is a member of the Cyber Liability, Financial Services, and Professional Liability practice groups. He may be reached at jyee@kdvlaw.com.*

Like it or not, stricter regulations for Internet data tracking are imminent: The question is simply how sweeping such regulations will be. In conjunction with the Federal Trade Commission, legislators are already calling for stricter guidelines. Tighter regulations may also arise as a byproduct of efforts to increase cybersecurity across different sectors. Whether it is wise or not, the weight of the popular vote is in favor of stricter regulations on data brokering.

However, few truly understand how sophisticated Internet data "tracking" has become. Regulation would be impossible without unprecedented control on commerce.

The FTC's Call for Stricter Regulations

On May 27, the FTC released a report titled "Data Brokers: A Call for Transparency and Accountability." Chairwoman Edith Ramirez commented concurrently, "[y]ou may not know them, but data brokers know you." In the report, the FTC painted a picture of an industry that was opaque and unregulated, where consumers had little control over their personal data that is being collected, analyzed, aggregated, packaged, sold and indefinitely stored.

The FTC recommended legislation focused on the following: (1) giving consumers greater access to their personal information and related data, such as through an online database where brokers can readily identify themselves; (2) giving consumers the ability to opt-out with brokers and businesses that use the data; (3) mandating those dealing directly with consumers to inform them about their opt-out options and affirmatively obtain their consent before data is collected; and perhaps most importantly, (4) providing greater controls on how brokers and industry use personal information and personal information-related data in their businesses and transactions, particularly if data can be used to negatively affect whether consumers can participate in or complete transactions. In short, the FTC is recommending that data brokers and businesses be subject to the same type of regulations as many employed in mass-marketing and credit reporting.

The FTC's report was met with warm welcomes by many on Capitol Hill, including Sens. Jay Rockefeller of West Virginia and Ed Markey of Massachusetts, who had introduced a bill calling for greater controls on data collection.

The FCC's Cybersecurity Initiative

Even if legislation on data brokers continues to stall on Capitol Hill, data brokers might still be subject to stricter regulation due to greater efforts to enforce cybersecurity across industries. On June 12, Federal Communications Commission Chairman Tom Wheeler announced a new cybersecurity initiative, to create "a new paradigm for cyber readiness" before the American Enterprise Institute. Wheeler called for three central pillars: (1) informational sharing and situational awareness, (2) cyber-risk management and best practices, and (3) investment in innovation and professional development. Wheeler's comments placed greater emphasis on the need for "cross-sector coordination" in the private sector with governmental entities, and greater transparency on security efforts by all involved.

Although Wheeler stressed the importance of freedom of information on the Internet, he also commented that "[w]e believe that when done right, cybersecurity enables digital privacy - personal control of one's own data and networks." This comment echoes the FTC's concern that there is lack of sufficient control over the dissemination of personal information, even if the FCC is talking about data breaches as opposed to data brokering.

Advocates for tighter controls on data brokers will likely argue that the FCC's concerted efforts on greater control against cyberbreaches should come hand in hand with greater control on data brokers disseminating personal information and personal information-related data. Hackers looking to capitalize on their hacks will be looking for personal information, and advocates will argue that controls on data security will be best effectuated by more detailed regulation of data brokers and tracking of personal information-related information.

Are Unprecedented Controls Necessary?

Nonetheless, the controls envisioned by zealous consumers and legislators would have to be far more invasive than they think and understand. Data analytics have been in existence far longer than the current criticisms against them, and sophisticated techniques have long out-paced controls. For example, most consumers think of "tracking" as websites tracking who and what they purchase after they have logged in. Techniques today are generally far more sophisticated.

One increasingly popular technique - "canvas fingerprinting" - is very difficult to block, as first documented by Princeton University. Websites that use canvas fingerprinting instruct the computers of users to draw a hidden image upon visiting the page. Because every computer will draw this image slightly differently, with an acceptable degree of accuracy, data brokers may be able to identify your computers "fingerprints" and activities. When the information reported by numerous sites is aggregated, data brokers will have a very good idea of your e-commerce habits and patterns. Unlike the traditional "cookies," which are just a string of code stored in the temporary directories of your computer, canvas fingerprinting is much more difficult to block and therefore even more pervasive.

However, as evidenced within Wheeler's own statements before the American Enterprise Institute, authorities clearly recognize that there is something very American about a free and unfettered Internet. Furthermore, a lot of data aggregated about consumers are collected from information that consumers freely and voluntarily disseminate on the Internet. At its core, understanding consumer patterns can certainly facilitate market efficiency, in the same way as more traditional targeted marketing. Thus, it is understandable why the progress of greater controls on "big data" move so slowly in states and Capitol Hill.

Nonetheless, the FTC may be spearheading greater efforts to control "big data," as evidenced by its increasing willingness to exercise its powers pursuant to 15 U.S.C. Section 45 ("Section 5" of the Federal Trade Commission Act), against "deceptive" and "unfair" practices in e-commerce. Many of us are familiar with the FTC's enforcement actions against companies that are less than forthcoming about their privacy practices as "deceptive" practices. But less clear is the full breadth of FTC's authority to restrain "unfair" practices.

The FTC appears now to be testing its powers to curb "unfair" practices in the area of data security. In the 3rd U.S. Circuit Court of Appeals case *FTC v. Wyndham Worldwide Corp.*, 13-1887 (D.N.J. April 7, 2014), the FTC argued its powers to curb "unfair" data security practices of the hotel chain were broad, and the district court agreed despite Wyndham's motion to dismiss. The *Wyndam* court is amongst the first to apply the "unfairness" prong of Section 5 to the data world, and the order immediately caught the attention of the legal community. Just last week, the 3rd Circuit granted Wyndam's petition for interlocutory appeal. If the Court of Appeals affirms the district court's order, it would not be a surprise for the FTC to bring enforcement actions

against data brokers it finds engaged in "unfair" practices - especially given the FTC's efforts to lobby for direct legislation.

Tighter regulations on data brokers can come from a variety of sources as a result. Whether through direct regulation, the FCC's Cybersecurity Initiative, or broader exercise of its powers by the FTC, tighter controls appear inevitable. The question is the breadth of such controls, which can ultimately stifle a healthy and competitive Internet and mobile industry, or encourage it.

Hsiao (Mark) C. Mao *is a partner and vice chair of the Financial Services Practice Group in the San Francisco office of Kaufman Dolowich & Voluck LLP. He may be reached at mmao@kdvlaw.com.*

Jonathan H. Yee *is an attorney in the Los Angeles office of Kaufman Dolowich & Voluck where he is a member of the Cyber Liability, Financial Services, and Professional Liability practice groups. He may be reached at jyee@kdvlaw.com.*