Proskauer

French DPA Issues Guidance Surrounding Practice of Web Scraping

Proskauer on Privacy Blog on **May 13, 2020**

On April 30, 2020, the French data protection authority, the CNIL, published a guidance surrounding considerations behind what it calls “commercial prospecting,” meaning scraping publicly available website data to obtain individuals’ contact info for purposes of selling such data to third parties for direct marketing purposes. The guidance is significant in two respects. First, it speaks to the CNIL’s view of this activity in the context of the GDPR and privacy concerns. Second, beyond the context of direct marketing related privacy issues, the guidance lays out some guiding principles for companies that conduct screen scraping activities or hire outside vendors to collect and package such data.

Privacy Concerns

Based on its investigation into commercial prospecting, the CNIL guidance noted that some entities are scraping individuals’ phone contact information posted on online directories or listings, even though such individuals may not have given consent for such collection and subsequent reuse for marketing solicitations. The guidance states that although such contact information is from publicly accessible websites, the individuals who posted the information did not reasonably expect to have it scraped for “prospecting,” and as such, the contact information is still “personal data” under the GDPR and cannot be re-used for marketing without the consent of the data subject.

The guidance notes that such consent should be obtained prior to any reuse of the data for marketing purposes and must be freely given, specific, informed and unambiguous. The CNIL states that the acceptance of the terms of general conditions mentioning that the individual accepts to receive marketing communications is insufficient, as it not specific. In addition, the CNIL notes, the individuals' rights under the GDPR must also be complied with, such as the right for an individual to oppose to the processing of their data and the need to provide appropriate information to the individual as to the processing of their data (the business reusing the data should in principle make a privacy policy available to the concerned individuals).

With the release of this guidance, the French data protection agency (a "DPA") has quietly confirmed that web scraping involving the collection of personal data, even from publicly available websites, implicates the need to conform with the GDPR and requires that companies (and their vendors) perform needed compliance. This is not the first time that a European DPA has investigated data scraping activities. In March 2020, the Polish DPA issued its first fine under the GDPR against Bisnode, a Swedish-headquartered company that specializes in business intelligence and data analytics. Apparently, Bisnode had scraped data from publicly available government databases about individuals' prior registrations as sole proprietors and other related corporate activities and produced certain reports for its clients. To fulfill certain requirements under the GDPR, Bisnode had sent emails to affected individuals with known addresses (and posted notices on its website), but it failed to send postal notification to millions of other individuals or entities due to the administrative cost and burden of doing so. The Polish DPA issued a fine for such a violation. Instead of complying with mailing millions of notices, Bisnode reportedly stated it would delete the data at issue, and appeal the Polish DPA's order. Regardless of the outcome, data scraping is something that EU regulators are beginning to keep an eye on.

General Concerns About Scraping

As we've stated on multiple occasions, it is important for downstream recipients of anonymized web or user data or analytic reports breaking down such data to understand how such data is collected and processed and whether such data collection is done according to applicable law or contractual requirements. Putting aside the GDPR issues, the CNIL guidance is a timely reminder to those entities engaged in web scraping about the importance of due diligence with respect to the data collection. The guidance also laid out some guiding principles for companies that conduct screen scraping activities or hire outside vendors to collect and package such data:

- Understand the duration of the web scraping and data processing activities
- Know the origin of the scraped data and whether the website from which the data is collected restricts its collection and commercial reuse
- Minimize the collection of personal data, and refrain from collecting any data that is irrelevant for the expected purpose of the data extraction
- Inform individuals affected by the collection of any personal data
- Carefully oversee vendor relationships concerning the nature of the data processing and any privacy and data security obligations. The CNIL suggests that service contracts should comply with certain GDPR requirements and, among other things, should specifically outline the nature of the data collection activities, including the purpose of the processing and the types of personal data collected (if any).
- Conduct a data protection impact assessment (DPIA), if appropriate

View Original

Related Professionals

- **Jeffrey D. Neuburger**
  Partner
- **Stéphanie Martinier**
  Partner