Hughes Hubbard & Reed

Discovery of Privacy Breaches on Facebook Puts New Emphasis on Debate Over Personal Data Protection

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

The recent Wall Street Journal report revealing that some of Facebook's most popular applications have been leaking user information has brought attention to a little-known corner of the Web advertising business. And that attention may ultimately lead to substantial changes in the way companies do business both with Facebook and throughout the wider Web. The Facebook disclosures were the result of a common Web standard called a referer. As web users navigate from site to site, the referer tells the new site which page the user is coming from. Most of the time, this is an innocuous tool used to help websites track the source of their traffic flow and customize user experience. However, when user IDs are included in web addresses, as is the case with Facebook and other social networking sites, this practice could potentially expose the browser's identity. The user IDs can be used to look up public information on the user's Facebook profile, which, depending on the selected privacy settings, could include anything from the user's name to his age, hometown, or even photos. Sharing any user information with advertising and data companies is a violation of Facebook's privacy policy. However Facebook has stated that it does not consider the sharing of IDs with application developers to be a privacy breach and that the disclosures by the applications to advertising companies were, for the most part, inadvertent and a "byproduct of how internet browsers work". Facebook has announced a proposed solution that would encrypt user IDs in referer headers to prevent inadvertent disclosure to third parties. The encryption will be mandatory starting January 1, 2011. However, the encryption only prevents accidental transmission. Describing it as a "Web-wide problem", Facebook states that they are looking forward to working with the Web standards community and browser developers in the future to develop a more complete fix. Facebook has had trouble with the disclosure of user IDs before. In May, Facebook revealed that IDs were being sent to advertisers when users clicked on certain ads on Facebook pages. In some cases, advertisers received the ID of the user who clicked on the advertisement, as well as the ID of the person whose page the user was viewing at the time. The disclosure of user IDs, which has always been a sensitive issue for companies doing business on the web, is becoming more of a hot-button issue as public awareness of the issue increases. It has already attracted the attention of lawmakers

who have asked Facebook to outline the steps it is taking to protect consumer information. While there is no foolproof method to prevent widespread disclosures of personal information, a two-pronged approach, using both technological solutions and a careful framing of contractual protections may help mitigate the problem and avoid the possibility of increased legislative oversight or intervention. One technological solution would be the increased use of encryption in connection with coding, storing and transmitting user IDs and other personal information. However, while encryption could prevent unauthorized disclosures, such technological solutions must be coupled with clear contractual obligations on the part of the various stakeholders to ensure their proper use and implementation. For example, publishers, ad service providers, search providers, developers and others who rely on the use, analysis and disclosure of user data could include in their various agreements provisions requiring that encryption and/or other data security technologies be implemented in connection with the transfer of data between the parties. The agreements could also include provisions that spell out how the parties may use personal data (for example, only for internal use in connection with fulfilling obligations under the underlying agreement), and more critically, include specific restrictions and prohibitions on use (for example, prohibiting the sharing of such information with third parties). Additionally, the inclusion of provisions requiring the maintenance of records of data practices which would be available for audit might also lead to increased vigilance. Although these measures place increased burdens on the various stakeholders, absent further technological developments, they may be the best way to convince regulators (and the public) that the industry is serious about protecting consumers' privacy. Websites can also take steps on their own to beef up their security policies. In recent months, Facebook has been working to increase their protection of user data. Following an investigation by the Canadian Privacy Commissioner, Facebook limited the access that applications have to private information. Unless the user grants additional permission, the application can only view information in the user's public profile. (For our previous article on the Canadian Privacy Commissioner's investigation, see here.) In early October, Facebook implemented a new tool to help users control what information applications can access, in response to criticisms that its privacy settings were too complicated. And, after these latest disclosures, Facebook announced a "clarified" privacy policy stating that user IDs cannot leave an application. In the event that a developer needs to share information with an advertiser or content provider, they must use an anonymous identifier. Whether or not these revised policies actually provide more protection to users' privacy is yet to be seen. However, it is probably not a stretch to say that the coming months will bring similar revelations and changes across the Web. We will continue to monitor this and other developments in the ongoing debate over privacy on the internet.

Related Areas of Focus

Media, Technology & Commercial Transactions