WASHINGTON INTERNET DAILY

March 18, 2010 Thursday

'Sensitive' Data Must Get Higher Protection Defining It Another Matter

SECTION: Vol. 11 No. 52

LENGTH: 959 words

The prevalence of sharing intimate details of one's life on Facebook and Twitter, and several ways that data can be used after initial collection, raise problems for the government in defining what's 'sensitive' and deserves more protection under the law, experts told the FTC's last privacy workshop Wednesday. Though some groups have called for equal and more protective treatment of all information because of the potential it could become sensitive down the line, commission lawyers were told that a lack of distinctions inevitably would lead to worse treatment for private or embarrassing data. One potential solution is to designate as sensitive certain groups of users, rather than a particular type of data.

A physical address ordinarily wouldn't be sensitive unless its Internet publication carried a risk of physical or mental harm, said WiredSafety Director Parry Aftab. That could include racial harassment against a person's home identified on Facebook or a burglary resulting from a person tweeting about their vacation, she said. But information that's not 'truly private' may not be sensitive, said Lior Strahilevitz, deputy dean of the University of Chicago School of Law: An ordinary person's HIV infection could be prohibited from use but not that of former basketball star Magic Johnson, for example. The U.S. 'sectoral' regulatory approach further confuses the issue, said Pam Dixon, executive director of the World Privacy Forum: When a person applies for a loan to pay for medical treatment, is their resulting data medical or financial? 'It gets very messy because it all starts to spill over the borders,' she said.

The Children's Online Privacy Protection Act can provide a helpful template for considering which groups besides children under 13 can be considered 'sensitive users,' said Kathryn Montgomery, a professor at American University's School of Communication. Users 13 and older may need additional protection, if not the same level as COPPA, because they routinely disclose personal information in social media and may not understand how they put themselves in harm's way, she said.

Location data is a double-edged sword because limiting publication may harm other groups, Strahilevitz said. Criminal history information by geography published online, such as for sex offenders, may negatively affect offenders but help minorities looking for work, he said, citing a study: Employers tend to hire more black men in areas with 'transparent' criminal data because employers' racial prejudices are countered with actual statistics. The FTC and Congress will 'have to confront these wrenching tradeoffs.'

It would be a 'step too far' to designate all location data sensitive, since users may tip their location voluntarily -- that's the point of the RobMeNow website that aggregates social feeds mentioning a person's location, said Catherine Harrington-

McBride, an FTC lawyer in the Division of Privacy and Identity Protection. The problem with location data is they're collected automatically for the most part, without a user's explicit consent for every collection, Montgomery said. 'You really have no idea' whether data used in a profile was submitted voluntarily by the user or came from monitoring their locations, since all data are mashed together. Regulating the initial collection may be tougher than the secondary uses of data, Aftab said: The rule could be that 'for commercial uses you need to know where it came from' to use data.

Collection of sensitive data could 'chill' some beneficial uses of the Internet, such as teens looking up sexual health information, Montgomery said. Pharmaceutical marketing in particular often uses unbranded websites that could be collecting data about users that they wouldn't want anyone to know, she said. Young people have 'shifting norms' and increasingly object to others using their public information in a way they don't like, such as employers checking their Facebook profiles, said Anita Allen, a deputy dean at the University of Pennsylvania. The risk of harm is the proper benchmark for the FTC to use in devising protections, said Jim Harper, **Cato Institute** director of information policy studies. The FTC's privacy principles as originally proposed in 2000, if fully adopted, could have preempted innovative new business models from Google, Facebook and now social location service Foursquare, he said.

While data collection may be inevitable whenever someone visits a website, its use can be further regulated depending on the source, Montgomery said. This would allow kids to visit websites, for example, without being subject to behavioral targeting. Lee Peeler, president of the National Advertising Review Council, said the industry has already taken this view as an extension of COPPA regulation -- no targeting without parental consent. The World Privacy Forum's Dixon said industry groups can't be entrusted to decide what's sensitive, because efforts to date have resulted in 'incredibly weak' self-regulation: There must be 'honest tension' between business and users. Michelle Rosenthal, another FTC division lawyer, said language could be brought over from business-to-business contracts where two parties agree not to share data with third parties. Allen called on the FTC to use 'coercive and paternalistic' measures to protect users.

Regardless of the difficulties in defining what's sensitive, regulators must do it, because 'hierarchies in law' are crucial for laws to work, Strahilevitz said. Privacy law can learn much from trade-secrecy law, in which companies that indiscriminately stamped materials 'trade secret' got smacked down by judges: 'By abusing it you're not really sending a signal ... that this is to be taken seriously.' -- Greg Piper