Is Respondent Validation Legal?

Weeding Out Cheater-Repeaters and Professional Respondents Could Bring Legal and Regulatory Problems

By Howard Fienberg

It goes by many terms, but respondent validation involves collecting, applying and tracking across time and space, potentially personally identifiable information (PII) to figure out if research participants are cheating, repeating or otherwise undermining the quality of studies in which they participate (either knowingly or unknowingly).

In the Real World

The most obvious attempts at respondent validation arise at in-person focus groups. Checking a person's identification (usually a driver's license) is a seemingly straightforward method to ensure they don't fake their way into a focus group. And keeping track of that information is a seemingly straightforward way to prevent respondents from participating too frequently, as long as respondents are given adequate notice and consent. Maintaining that information long-term could be a problem. Sharing that information with other facilities/companies is much more problematic – and absent robust notice and consent, possibly illegal.

British Columbia provides an interesting test case of this kind of validation. Numerous bars there implemented a program called BarWatch, whereby they would photograph everyone entering the bar, scan their driver's license and share the information in a common database. Rather than combating survey cheater-repeaters, BarWatch aimed to track and tag "rowdy" (violent) bar patrons, holding the data indefinitely. In August, the province's Information and Privacy Commissioner, David Loukidelis, ruled that the databases could be maintained for only 24 hours. Loukidelis did allow that BarWatch could hold onto data about any customers that had actually caused a problem.

This makes for a potential best practice (notwithstanding other applicable laws and with the understanding that British Columbia's laws are likely different from other territories). Such a validation system (at one facility or across many facilities) may pass legal muster, with appropriate notice and consent, but likely only for tracking cheaters. Intent will often matter to government authorities, such that they will allow measures to prevent fraudulent activity, but no more than that, especially since unnecessary data storage invites data security hazards.

In the Digital World

Digital respondent validation methods, like machine identification and digital fingerprinting, appear legal in the United States – for now – although they may not fare the same in the European Union, where the data protection authorities feel that a simple IP address constitutes protected PII.

Unfortunately, there are serious domestic threats to these methods just over the horizon.

For instance, at an RSA Security Conference this past spring, privacy activist and Electronic Frontier Foundation attorney, Jennifer Granick, declared that the authentication process for most online banking and much of e-commerce violates consumer privacy. She admitted that it was useful to help prevent fraud, but felt that a bank should not have to collect regular data on when, how often or from where a consumer accesses a bank account or commerce site. Granick reasoned that such information can be combined with other personal information to create detailed profiles of consumers.

Although industry security experts argued for the privacy protections inherent in their methods, activists remained unconvinced. Activists and some academics in attendance all agreed that using that information for anything other than fraud prevention, including selling the information, would constitute a privacy violation.

Legislators and Regulators are Watching

As we discussed in this column in the

(Continued on page 40)

(Continued from page 39)

June issue of *Alert!* ("Online Behavioral Tracking: Implications of Regulation"), Congress, the Federal Trade Commission, and various state legislatures are considering regulating or restricting online data collection. At least at the federal level, that focus has narrowed to passive data collection across multiple sites. That means that they might look the other way when it comes to passive data collection within a single site, but exercise their muscle if any kind of collection or tracking occurred beyond that single site.

Even as their focus may have narrowed, the scope of legislation being crafted in the House Energy & Commerce Committee is quite harrowing. Telecommunications & the Internet Subcommittee Chairman Rick Boucher (D-VA) and full committee Ranking Member Joe Barton (R-TX) aim to require opt-in consent for all online data collection.

MRA is working with a group of volunteers to develop our own self-regulatory standards. While a few legislative voices, such as Subcommittee Ranking Member Cliff Stearns (R-FL), argue for robust notice and opt-out as a more manageable standard, the window for the research profession to head off more severe regulation online may be closing.

What Can Researchers Do Right Now?

Absent a framework, codes or guidelines specific to respondent validation, researchers and research buyers should proceed with three key best practices in mind:

1) Notice: Simply mentioning your validation processes in your privacy policy or in a research participation agreement is only a start. More robust notification, including signage at a physical focus group facility or pop-up notices on Web sites, should be implemented. Education of research participants is important.

2) Consent: Informed opt-in, while admirable, may not be practical for many validation processes. But an obvious opportunity for opt-out is a must.

3) Efficiency: Do not collect more information than you need for validation purposes and do not keep it any longer than necessary.

Disclaimer: The information provided in this article is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. MRA advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.

Howard Fienberg is MRA's director of government affairs.