Data Protection Is More Than Privacy

*Deni Elliott**

Privacy has become a catch-all concept for discussing who controls data in the digital world. The legalistic view chips at data controller processes to detail minimal requirements for user consent. A larger set of ethical issues become evident when digital data collection and use are viewed in the context of user intent and belief instead of starting with what data collectors can be legally allowed. It is important to parse the larger ethical issues so that problematic behaviours developed at the dawn of the digital age do not morph into conventional assumptions. A vignette involving higher education is offered here, rather than one describing an organisation with solely commercial interest, to show how ethical issues arise even when data collector and user ostensibly share goals of use. Many institutions of higher education collect data in one or more of the following ways:

In the weeks before the start of the academic year, Gerri joined other incoming first-time-in-college students for a three-day freshman orientation on the college campus. She'd sign multiple forms, choose a major, and learn how to use her ID card to access the library and recreational facilities, enter her residence hall, and pay for meals. She'd also get to know other students and the school's academic expectations.

Orientation had the feel of summer camp. The atmosphere was relaxed, staff were enthusiastic and welcoming, and the peer ambassadors were engaged and empathic with the first timers. But, every moment had been carefully planned, based on predictive data analysis. The college's goal was to turn these newly admitted students into graduates in four years who would then become lifelong donors. Every student counted in the school's performance metrics. Over time, several hundreds of data points would be gathered on each, including class attendance, grades, time spent in elective labs and in the library, email exchange between student and professors, and even aspects of campus life including how and when students took advantage of the school's meal plan, their recreational facility use, and card swipes indicating what time they returned to their residence halls for the night. Low performance in class or other concerns could trigger the aggregation of all of a student's data for analysis so that advisers had as much information as possible before reaching out to the student to provide assistance.

Although this school hadn't initially been Gerri's first choice, she had been convinced by recruiters who cited successful students and how well Gerri matched them in de-

DOI: 10.21552/edpl/2019/1/5

* Deni Elliott holds the Poynter Jamison Chair in Media Ethics and Press Policy at the University of South Florida. She is co-author of *Ethics for a Digital Era* (Wiley Blackwell Publishers 2018).

mographics and interests. Nine months' prior, Gerri had completed a detailed survey for the Student Search Service when she took her college admissions test. She voluntarily completed surveys, allowed cookies, and shared her contact information on college and university websites so that she could see which fields of study were recommended for her. And what motivated prospective student could turn down the opportunity to learn about specifically-tailored scholarships? Gerri had felt overwhelmed by texts, emails, and glossy brochures from the dozens of schools that reached out to her based on her test scores. She also received a surprising amount of communication from colleges that she contacted 'organically,' in her own web-based search of colleges and universities. In the end, it was easiest to choose the college with recruiters who took the most interest in her.

By the time Gerri attended orientation, the college had compiled enough information to predict in which classes she might require tutoring and how to help her adjust to campus life. Although advisers used that material in helping Gerri choose classes, they did not offer to review their aggregation of data with her.

Years ago, freshman orientation would have subjected Gerri and her peers to a mountain of paperwork. Now, electronic forms with 'I Agree' buttons and automatic signature options made the process far less cumbersome. Gerri scrolled through the various forms, searching for signature lines, and declined written copies, as did her peers.

If she had read, rather than skimmed past the privacy policy, she might have noticed the following:

- *The school would not sell her personally-identifiable information without her consent, but the policy didn't explain how she might have given consent;*
- *The school linked to external websites, including Google, a for-profit learning management system, and a bookstore. The school claimed no control over whether these affiliated third-party vendors might contact her regarding goods and services;*
- *The school would not make decisions based on automated processing of her personal information, but the policy didn't mention that identifiable data could be aggregated;*
- *Personal information, including sensitive information, would be shared throughout the university for the college's or her benefit, including fundraising;*
- *She could disable cookies or decline to share information, but this would interfere with her ability to use the school's website.*

Legal scholars on both sides of the Atlantic might argue about how the GDPR and accompanying expansion of laws and regulations in the US would address digital data collection in this case or fail to do so. Here I argue that considering such use only as a question of privacy ignores relationships between individuals and organisations and

misses other ethical issues. If we think of the issue from the perspective of the intent and beliefs of the user, we understand that organisations that claim to be operating in the best interest of users should create transparent policies that honour those relationships.

Assumed Opt-In: Opting in for a choice theoretically provides more control for users than giving them the burden of opting out, but not when their consent is assumed. Assumed consent in the virtual world consists of boxes being pre-checked, signing users up for further contact with an organisation and for marketing or use by third-parties. Instances of assumed consent are often found when users are distracted by the task at hand: for example, they are looking for the large brightly coloured 'Continue' or 'I Agree' button to move from one page to the next. The pre-checked boxes are intentionally presented in a less-significant place and colour, based on eye-tracking research that show that users are likely to focus on the more prominent and sought-after button. This is an ethical problem because the visual display does not allow any but the most careful user to have valid consent. The boxes are easy to uncheck. But first they have to be noticed.

Undue Influence: Undue influence undermines consent in conditions in which the inducement to agree is strong enough that the user is unlikely to choose not to participate. College and university websites provide good examples in which consent is less than voluntary. Personal information, including sensitive information, must be provided to the school for admissions decisions and, if the student is accepted, the information is retained and much more is collected. Students must use the school's website to access the learning management system required for all classes and to access library and other support services. As access to some end is perceived as necessary by the user, consent to the means to that end is suspect. If consent were based on transparency and attention to the relationship between organisation and individual, educated consent could be confirmed by asking users to complete a short quiz between consent and access. Quiz items should affirm that users know how their data will be collected and used and that they are aware of reasonable options. Choosing not to sign up for the school's website is not a reasonable option for a student seeking a college education.

Deception: Withholding or not telling users information counts as deception if users have a right to weigh that information in making choices in their individual interest. Withholding or not telling in these instances counts as cheating. As a physical world example, if I delay telling a student that he is doing poorly in my class because I need to keep the enrolment number high until the drop period is over, I have withheld information that he might use in making the decision to switch to a more basic course. I have cheated him in not allowing him to have access to information that is rightly his to consider. True consent depends on users having access to all information that they would find relevant in choosing among options. Silence can be as ethically problematic as stated falsehoods. For example, if not told differently, college students are likely to assume that email correspondence with their instructors is private and perfor-

mance on individual assignments is known only to their instructors and themselves. When meeting with an academic adviser, few students would guess that the adviser knows that they came in quite late the night before and slept in, missing both breakfast and their morning classes. When users believe that they are operating at liberty, but they are subjected to surveillance, they have been deceived. This is particularly egregious in a setting, such as a college or university, that is designed to promote the user's interest. Paternalism provides seeming justification for collecting data regarding an individual without his or her knowledge if used for the individual's own good, but it is not adequate justification when the organisation is working with competent, rational adults who are capable of providing educated consent. Students should be informed of personal data aggregation and given the opportunity to decline such monitoring.

Digital data collection has changed how individuals see themselves and the choices organisations make in their own interest or in the purported interests of individuals. Data collection and evidence-based analysis can enhance decision making but can also lead to the erroneous conclusion that what can be measured is all that matters. Transparency with users stands in contrast to practices such as opt-in assumptions, undue influence, and withholding information that users have the right to know. Government, commerce, and citizens should ideally work together to ensure that individuals are able to participate in the 21st century without exchanging personal choice and identity for aggregated data points.