Confidentiality, Privacy, and Institutional Review Boards

March 31, 2015

Nancy Eisenberg

Anthony E. Kelly is Professor of Educational Psychology at George Mason University and is a Senior Advisor to the Directorate of Education and Human Resources at the National Science Foundation. Kelly's interest in research methodology led to two NSF grants for the study of online learning of mathematics with the late mathematician Mika Seppälä (his colleague from Finland), which posed unanswered questions on privacy. A third NSF grant supported an interdisciplinary conference on privacy and Institutional Review Board practices, which informed this opinion piece. I heard about the interdisciplinary conference and some of the issues that were discussed among that group. Given the tremendous importance of how we deal with privacy and related human-subjects issues to the future of the field, and the fact that we often are rather uninformed about these issues and/or are out of the loop on decision making about them (at least, I am), I asked Kelly to share some of his thoughts on this issue with APS members.

-Nancy Eisenberg

Anthony Kelly

In 2011, amid growing concerns about electronic privacy, the Department of Health and Human Services published, and is now seeking comments on, an Advance Notice of Proposed Rulemaking (ANPRM) concerning the Common Rule, which guides IRB panels. Among the commentaries submitted in response to the ANPRM is a 2014 National Research Council report written to specifically address proposed revisions to the Common Rule.

Beyond changes to the rules governing IRBs, scientists working in the US must navigate a host of additional federal-level privacy regulations: The Department of Education's Family Educational Rights and Privacy Act, the Federal Trade Commission's Children's Online Privacy Protection Act (COPPA), and Health and Human Service's Health Insurance Portability and Accountability Act (HIPAA) are all undergoing changes. Commercial ventures that profit from the collection of data on individuals and groups, which are regulated under the Federal Trade Commission's Fair Credit Reporting Act, and evolving consumer protection laws will also impact the regulatory landscape for privacy. Meanwhile, the White House has sponsored a national series of meetings on privacy (Executive Office of the President, 2014a, 2014b) and is preparing a student privacy bill modeled on a similar state bill from California. In addition, a range of congressional, Executive Branch, and state efforts have emerged to define and protect privacy through data sharing, scientific openness, and transparency while balancing commercial and security interests.

For those collecting data overseas (e.g., via MOOCs, e-learning, or other sources), privacy and data protections are also in flux. For example, the European Parliament voted in 2013 to approve the EU General Data Protection Regulation. While not final, this regulation has stipulations about explicit consent to collect data and a "right to erasure" of personal data. The regulation would also set limits on predicting or inferring variables such as work performance, socioeconomic status, location, or health.

Since no further guidance has appeared on the Notice of Proposed Rulemaking/Common Rule, IRB panels, especially those concerned with confidentiality related to the Internet and other electronic records and privacy, presently must act in a context of uncertainty: These IRBs are facing privacy

concerns that are unprecedented. The concerns are tied to the use of personally identifiable information (PII) such as names, addresses, and phone numbers, as well as other identifiers (McCallister, Grance, & Scarfone, 2010).

Daily, we engage in *active* online interactions via websites, social media, credit card transactions, and the myriad behaviors that leave digital traces of our activities and habits. Our *passive* behaviors may also be captured via face recognition, eye tracking, voice printing (see work at the Institute for Intelligent Systems at the University of Memphis), stylometrics (see the work at Rachel Greenstadt's lab at Drexel University), or even gait analysis (Ran, Zheng, Chellappa, & Strat, 2010). Further, our ambient states of being are being recorded as *metadata* (see de Montjoye, Radaelli, Singh, & Pentland, 2015) from the burgeoning Internet of Things, those billions of devices that can robotically collect data on our location, the number of steps we take, our home heating habits, and even the items we keep in our refrigerators (see share.cisco.com/internet-of-things.html). Inferences are also being generated about us from the behaviors and metadata profiles of others — with or without our knowledge or consent. The correlation of active, passive, and metadata sources puts IRB commitments to confidentiality of subjects at great risk.

PII extends beyond names and addresses to personal disclosures and to persistent and durable associations, which may not only describe our past and current behavior but also infer health and other conditions, predict our future behavior, determine our risk profiles for insurance or bank loans, or influence our employability (e.g., inferences about our health may be used, illegally, as the basis for employment discrimination). Indeed, data on inferred health conditions may raise HIPAA questions. For example, measures of cognitive and executive function collected for improving learning may predict cognitive-degenerative conditions such as Alzheimer's disease (see the work of Curtis Tatsuoka at Case Western Reserve University). How should this range of potential inferences impact the process of seeking informed consent from research subjects?

Designing algorithms for successfully *de*-identifying data (e.g., stripping it of PII) is an area open for study. However, *re*-identification of data — and the ensuing reintroduction of privacy problems — is proving highly tractable given the exponential growth of relatable active, passive, and metadata on individuals and groups. Moreover, in social media or MOOC settings, subjects may disclose personal data (e.g., via postings or essays) that cannot be easily de-identified, stripped, or obscured.

Although researchers can encrypt data or place them behind secure firewalls, protecting data from hacking and other security breaches is daunting. In any event, sequestering or obscuring data works against calls for greater data transparency, rechecking of results by other researchers, replication of results, and the reproducibility of methods.

The challenges facing IRBs are, therefore, unavoidably complex and evolving. Issues of informed consent assume not only the capacity of the subject to understand data-mining algorithms or neural nets that make opaque inferences about a subject's current or future behaviors or conditions but also the capacity of the researcher to explain these processes in understandable language (Brunton & Nissenbaum, 2013). Compounding the problem is the need for rules on obtaining consent for downstream studies that may use the many forms of subjects' collected and inferred data to inform research questions that may not have been imagined when the original study was proposed. For example, under what circumstances can data from a memory study be appropriated later by unknown researchers for a study on cognitive-degenerative disease? What of genetic information that is posted on data

websites following NIH requirements? Moreover, can the data and metadata from those who volunteer be used to infer the views, behaviors, dispositions, and conditions of those who may have refused to volunteer or who were never approached? What does consent and withdrawal of consent mean in this milieu? Also of concern are the rights of future generations, who may face negative consequences as a result of their family members' disclosure of genetic or identifiable data in the present.

Since there is yet no socially accepted baseline for privacy and personal risk, and only a nascent public awareness of how data are gathered and may be used, what principles should guide the obtaining of consent for such wide-ranging data gathering? Ethically, against which risk baseline is the "minimal risk" of participation in a study to be judged and explained? How should ratios of costs and benefits for subjects and society be computed?

Perhaps the solution will be some form of generalized consent accord. Technology and software users already enter into a generalized consent accord when they click (perhaps without fully reading) the terms of service. In the future, trusted institutions such as universities may ask students to agree to a global assent to use data collected about them for permissible ends, such as improving learning. Perhaps patients will sign similar consent accords for medical treatment. On the other hand, if institutions lose the trust of their participants, unknown biases may be introduced into research with nonrandom entry into or nonrandom attrition from generalized consent accords. If generalized accord becomes accepted practice, the Common Rule may allow IRB panels to categorize more research activities as exempt. IRBs would then devote time to the hard cases: those clear violations of fairness, beneficence, and justice described in the Belmont Report, the conceptual document from which the Common Rule derives. These cases may include inferring mental health conditions from nonclinical data or by nonspecialists; exploiting vulnerable populations, including undocumented immigrants and drug users; causing loss of employment; or circumventing privacy controls for data on children and students.

Fundamentally, it is incumbent on the research community to stay abreast of these developments and associated regulations and legislations and to remain an advocate for the value of scientific discovery while pointing out its limitations. Further, professional societies must educate the public about abstract concepts such as identity, autonomy, agency, the right to privacy, and related values such as anonymity, security, and commercial profit. When it comes to confidentiality and IRBs, the research community must demonstrate in all of its actions that it remains worthy of public trust.

This material is based upon work supported by the National Science Foundation under Grant No. 1419055.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation. œ

References and Further Reading

Brunton, F., & Nissenbaum, H. (2013). Political and ethical perspectives on data obfuscation. In M. Hildebrandt & K. de Vries (Eds.), *Privacy, due process, and the computational turn* (pp. 164–188). New York, NY: Routledge.

de Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. (2015). Unique in the shopping mall: On

the reidentifiability of credit card metadata. *Science, 347,* 536–539.

Executive Office of the President (2014a). *Big data and privacy: A technological perspective*. Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

Executive Office of the President (2014b). *Big data: Seizing opportunities, preserving values*. Retrieved from http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (Eds.). (2014). *Privacy, big data, and the public good: Frameworks for engagement*. New York, NY: Cambridge University Press.

McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to protecting the confidentiality of personally identifiable information (PPI): Recommendations of the National Institute of Standards and Technology*. (NIST Special Publication 800-122). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Ran, Y., Zheng, Q., Chellappa, R., & Strat, T. M. (2010). Applications of a simple characterization of human gait in surveillance. *IEEE Transactions on Systems, Man, and Cybernetics, Part B, 40*, 1009–1020.

US National Research Council (2014). *Proposed revisions to the Common Rule for the protection of human subjects in the behavioral and social sciences*. Washington, DC: National Academies Press.