Privacy Position Statement

Dilma Rousseff, the ousted president of Brazil, once said, "Without the right of privacy, there is no freedom of speech or freedom of opinion, and so there is no democracy."[1] This was a year or so before the investigations that led to her impeachment, so her remarks even then were surely somewhat self-serving. But that doesn't make her wrong, and the issue she raised is flying under most of our 21st-century radar, along with a range of other concerns about what becomes of all the information we freely share online.

We install apps, click on new services, and make purchases all the time. When we do so, we are entering into a relationship with our internet service providers, with the vendors who sell to us, and with our government at all levels. And this relationship is largely based on a foundation of trust: we trust those with whom we share our information and our cash not to abuse that trust by passing on our information to those whom we might not, in fact, trust at all.

Is that trust justified? And even if nothing nefarious is afoot in the increasing digitization of our lives, are other traps lying in wait for us?

Do you worry that important information, whether highly personal to individuals or crucially important to commercial enterprises, is routinely stored in vast databases that are largely under the control of private corporations, such as Amazon, Google, and the various telecommunications

---

[1] Speech to the United Nations, September 24, 2013. Without Privacy There Ca#6F4503

companies? Meanwhile, the troubling uses to which these datasets can be put remain mostly opaque to most citizens.

Would having all of that data under the control of the central government make you feel better? Didn't think so. Our concerns are not so much with which entity has our data as with the fact that so much information about us is now available to so many and that we don't have any effective control over the ways it is gathered, stored, and used.

As our technologies have advanced, new possibilities for commerce, bureaucratic administration, and political involvement have emerged, and they are working profound changes in how we live together. From the halcyon days of the 1990s when a widely heard mantra was "information longs to be free," we now find ourselves in a very different place. Today, information is not free in any of the senses of that word. All kinds of information about us -- our receipts and spending habits, our browsing histories and what they reveal about us, and our social connections -- have become commoditized and are used both to target our buying habits and to serve our needs for political and social affiliation. Here's a capsule summary of how the world of marketing has been altered:

> Even the words we say on Twitter, the things we like on Facebook, the websites we tend to visit, and the sound of our voices can be turned into a fairly detailed psychological profile, and the potential for trading this data is by no means confined to the world of marketing. The insurance, financial services, dating, and recruitment industries are all interested in the data, and few platforms would have launched or been funded if it weren't for the prospect of monetizing their users'

> personal data, which is the price we pay for anything that's free. Needless to say, there are many potential dangers (and ethical issues) associated with the proliferation of digital profiling, from hacking, to discrimination, to an Orwellian surveillance state. There's a big difference between what companies could and should know.[2]

To show how far corporations can take their monitoring of our information, consider that the Bose corporation now faces a suit filed by Kyle Zak that alleges that Bose collected information about him that he did not give them permission to have, much less hold onto.[3] The company defends itself by arguing that the information collected by the Bose Connect App is never sold or used to identify individuals. The statement from Bose said, "We don't wiretap your communications, we don't sell your information, and we don't use anything we collect to identify you -- or anyone else -- by name.[4] The matter of trust appears again.

But the Bose headphones in question are just one of many devices that constitute the so-called "internet of things" – devices and appliances that perform services for us but are also connected to the internet. The courts will adjudicate the Bose issue, but the question of where the legal lines will be drawn remains an open one.

---

[2] Tomas Chamorro-Premuzic and Nathalie Nahai, "Why We're So Hypocritical About Online Privacy," *Harvard Business Review*, May 1, 2017. Available at https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy.
[3] Hayley Tsukayama, "Bose Headphones Have Been Spying on Customers, Lawsuit Claims," Washington Post, April 21, 2017, updated with a response from Bose, available at https://www.washingtonpost.com/news/the-switch/wp/2017/04/19/bose-headphones-have-been-spying-on-their-customers-lawsuit-claims/?utm_term=.d20a774d0d09
[4] *Ibid*.

If that's not disturbing enough, how about when such means are used with regard to children in public schools.? The Electronic Frontier Foundation launched an effort in 2015 to raise awareness of student privacy issues when students use district-issued digital devices:

> [W]e have found that educational technology services often collect far more information on kids than is necessary and store this information indefinitely. This privacy-implicating information goes beyond personally identifying information (PII) like name and date of birth, and can include browsing history, search terms, location data, contact lists, and behavioral information. Some programs upload this student data to the cloud automatically and by default. All of this often happens without the awareness or consent of students and their families.[5]

What's more, the issue of student privacy becomes even more central as educators make increasing use of cloud computing and a range of technologies in pursuit of personalized learning. Mouse clicks and eye movements are monitored and collected in order to be responsive to a learner's needs. Policies about confidentiality and curation (where? how long?) of such data are essential.[6] Big Data and the uses to which it can be put will be central to the future of education, of technology, and of our democratic society.

---

[5] Spying on Students- Scho#6F0237.

[6] Joel Reidenberg et al., "Privacy and Cloud Computing in Public Schools," Center on Law and Information Policy, Fordham University, 2013, available at http://ir.lawnet.fordham.edu/clip. This reference and the text it refers to come from the comments made by AECT members to a draft of this document.

Most of these developments came about as ways to make 21st-century life more organized and easier to navigate. Need to buy something? Let Amazon help you find it and bring it to your door. What's more you'll also be able to find out what others who share your tastes and interests have bought. Want to undertake a self-improvement program? Lose weight? Learn a language? Get up and start exercising? Applications available for your smart phone or tablet will track your learning, catalog your activities, keep track of caloric intake, and funnel all that information back to you to keep you on track toward your goal. Need to know about the upcoming elections? One click on a major party's web site will not only provide reams of information but at the same time will add your name to a massive list of contacts and potential donors. And before you know it, you'll start receiving information and solicitations that will continue for months -- or even years -- into the future.

What's not to like about our hyper-connected age? By appealing to our self-interest, our new communication technologies have undertaken to solve problems for us; no need for our actual participation until it's time to click on the shopping cart icon or pull the voting lever. The deliberative process has been taken over by unseen algorithms that operate deep in the background of the digital ecosystem.

And therein lies the problem that our new technologies present for democracy. To be effective, democracy requires that opposing voices be heard. When we consider such matters as how we live together in society, what is in the public interest, or how competing demands of citizens are adjudicated, our differences need to be settled through debate and

negotiation. And the competing economic, legal, and ethical debates must be public and transparent.

That presents a problem for those institutions that would mine the mother lode of Big Data to give us what we want even before we ask. Those who would sell to us don't want transparency with regard to information if that means letting the competition into the game. Those who would manage our political lives don't want transparency if that means we might be exposed to a range of differing opinions. And the lack of transparency bodes ill for the health of our democracy.

The forces that have combined to create this new threat to democracy are not overtly bent on doing evil. But the power of consumer markets, governments' desire to satisfy the demands of their people, and the need for efficiency in the delivery of goods and services have all combined to ensure that more and more information will be gathered, stored, and used in ways that undermine the active and intelligent involvement of citizens. And that involvement is a prerequisite for a functional democracy.

The institutions that make use of our collective data -- whether government and administrative or commercial -- are seeking efficiencies: better ways to meet our needs, to keep the peace, to make decisions about public policy, or to manage our social lives together. They make use of algorithms that seek to know as much about us as possible, so that they can offer us a smoother, less rocky path to the good life. In exchange, we hand over the tiller of the ship of state. Our needs are met, we expend less effort in the process, and we

avoid confronting our own prejudices. In exchange, we have traded our democratic birthright for a bowl of digital pottage.

What to do now? The answer is far from obvious, but the urgency of responding is starkly clear, especially for organizations whose purpose is to enhance education and learning. The Electronic Frontier Foundation has a number of relevant projects under way. Just one example is an examination of the privacy concerns raised by "vehicle to vehicle" communication that will surely be part of our driverless future.[7] At the same time, the Berkman Klein Center for Internet and Society at Harvard University has a broad range of projects exploring most aspects of cyber security and privacy.

An organization such as the Association for Educational Communications and Technology will surely find itself embroiled in this issue in the coming decade, for it is these new electronic technologies of communication and commerce that lie at the heart of this emerging problem. It would be wise for organizations to be proactive and to develop policies with regard to the risks to our body politic that these technologies are creating. Calling attention to the problem and spreading the word widely are sure to be among the first steps that are needed.

How might AECT begin any such effort to enlighten the public? Certainly, a first step would be to raise the issue at the annual conference in Jacksonville,

[7] Jamie Williams, "Danger Ahead: The Government's Plan for Vehicle-to-Vehicle Communication Threatens Privacy, Security, and Common Sense," Deeplinks Blog, available at https://www.eff.org/deeplinks/2017/05/danger-ahead-governments-plan-vehicle-vehicle-communication-threatens-privacy.

Fla., in 2017. But other possibilities exist as well. Perhaps even before the Jacksonville conference, AECT's board should develop a plan to alert the membership to the growing danger that our lack of control over our information poses for our democracy.

Among the possible components of any such plan of action might be the use of print outlets and, perhaps even more important, social media to engage members and enable them to share their thoughts. An action plan might be developed to help those members with a particularly strong interest to organize and hold meetings in their communities and to conduct webinars designed to build a knowledge base on the issue among the general population. This last activity would be especially appropriate for those members who have specialized knowledge and expertise in this area.

These activities (and others that the board and membership might come up with) clearly align with AECT's strategic plan, will serve to inform a wider audience about AECT, and will thus increase its visibility and credibility as a professional organization.