Privacy in the Age of Augmented Reality

Abstracts presented by

**Alessandro Acquisti**
Professor of Information Technology and Public Policy,
Co-Director of Center for Behavioral and Decision Research, Carnegie Mellon University

**Kevin Fu**
Professor of Computer Science & Engineering,
College of Engineering

**Martha S. Jones**
Arthur F. Thurnau Professor, Associate Professor,
Department of History and Department of Afroamerican and African Studies, College of Literature, Science, and the Arts; Affiliated LSA Faculty, Law School, Co-Director, Program in Race, Law & History

**Erin L. Krupka**
Assistant Professor of Information,
School of Information

**Catharine A. MacKinnon**
Elizabeth A. Long Professor of Law,
Law School

**Moderated by:**

**Jeff MacKie-Mason**
Dean of the School of Information; Arthur W. Burks Collegiate Professor of Information & Computer Science, Professor of Information, School of Information; Professor of Economics, College of Literature, Science, and the Arts; Professor of Public Policy, Gerald R. Ford School of Public Policy
Alessandro Acquisti

Privacy in the Age of Augmented Reality
I will present a series of results from studies and experiments investigating the economics of privacy, the behavioral economics of privacy, and privacy in online social networks. The studies highlight surprising trade-offs that emerge from the protection or sharing of personal information, the inadequacy of "notice and consent" mechanisms for privacy protection, and the future of privacy in an augmented reality world in which online and offline personal data will seamlessly blend.

Face Recognition and Privacy in the Age of Augmented Reality
Alessandro Acquisti, Ralph Gross, Fred Stutzman

We investigate the feasibility of combining publicly available Web 2.0 data with off-the-shelf face recognition software for the purpose of large-scale, automated individual reidentification. Two experiments illustrate the ability of identifying strangers online (on a dating site where individuals protect their identities by using pseudonyms) and offline (in a public space), based on photos made publicly available on a social network site. A third proof-of-concept experiment illustrates the ability of inferring strangers’ personal or sensitive information (their interests and Social Security numbers) from their faces, by combining face recognition, data mining algorithms, and statistical re-identification techniques. The results highlight the implications of the convergence of face recognition technology and increasing online self-disclosure, and the emergence of “personally predictable” information, or PPI. They raise questions about the future of privacy in an “augmented” reality world in which online and offline data will seamlessly blend.

An Experiment in Hiring Discrimination via Online Social Networks
Alessandro Acquisti and Christina M. Fong

Online platforms offer workers and firms a new channel for job market screening and matching. However, little is known about how job candidates’ online information influences employers’ hiring decisions. We investigate how the hiring behavior of U.S. employers is affected by their online search activity and the information they find online about job candidates. We create profiles for job candidates on popular online social networks, manipulating information that is protected under either federal or state laws but that can often be inferred from individuals’ online presences. We submit job applications on behalf of the candidates to over 4,000 U.S. employers, and compare interview invitations for a Muslim candidate relative to a Christian candidate, and a gay candidate relative to a straight candidate. We find that only a sizable minority of U.S. employers likely searched online for the candidates’ information; hence, the overall effect of the experimental manipulation is small. However, we find that discrimination against the Muslim candidate relative to the Christian candidate varied significantly with employer characteristics. Employers in areas with higher proportions of Republican voters were significantly less likely to call back the Muslim candidate. The
results are robust to using either state- or county-level data, to controlling for firm, job, and geographical characteristics, and to various model specifications. The findings suggest that, although hiring discrimination via online social networks may not be yet widespread, online disclosures of personal traits can have a significant effect on the hiring decisions of a self-selected set of employers.

**Misplaced Confidences: Privacy and the Control Paradox**  
Laura Brandimarte, Alessandro Acquisti, and George Loewenstein

We test the hypothesis that increasing individuals’ perceived control over the release and access of private information—even information that allows them to be personally identified—will increase their willingness to disclose sensitive information. If their willingness to divulge increases sufficiently, such an increase in control can, paradoxically, end up leaving them more vulnerable. Our findings highlight how, if people respond in a sufficiently offsetting fashion, technologies designed to protect them can end up exacerbating the risks they face.

**Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency**  
Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, George Loewenstein

In an effort to address persistent consumer privacy concerns, policy makers and the data industry seem to have found common grounds in proposals that aim at making online privacy more “transparent.” Such self-regulatory approaches rely on, among other things, providing more and better information to users of Internet services about how their data is used. However, we illustrate in a series of experiments that even simple privacy notices do not consistently impact disclosure behavior, and may in fact be used to nudge individuals to disclose variable amounts of personal information. In a first experiment, we demonstrate that the impact of privacy notices on disclosure is sensitive to relative judgments, even when the objective risks of disclosure actually stay constant. In a second experiment, we show that the impact of privacy notices on disclosure can be muted by introducing simple misdirections that do not alter the objective risk of disclosure. These findings cast doubts on the likelihood of initiatives predicated around notices and transparency to address, by themselves, online privacy concerns.
Are There Evolutionary Roots To Privacy Concerns?  
Alessandro Acquisti, Laura Brandimarte, and Jeff Hancock

We posit and investigate an evolutionary account of privacy concerns. Since evolution rewards the ability to detect and react to threats in an organism’s physical environment, many species have developed perceptual systems specially selected to assess sensorial stimuli for current and material risks. For humans, those stimuli may have included the perception of the presence of other entities, including human beings, in one’s proximal physical space, and the ability to rapidly differentiate between friends, strangers, and potential foes. Under such account, territorial and bodily privacy concerns may have evolved from actual safety and security considerations; modern informational privacy concerns may be distant evolutionary byproducts of those ancestral systems. While it is not possible to test such conjecture directly, indirect evidence compatible with the account can be obtained by investigating the impact that external stimuli in the physical world have on privacy behavior in cyberspace. We present the design and preliminary results of a stream of controlled experiments with human subjects, in which we explore the influence that offline cues and stimuli, indicating the presence of other human beings in the proximal space of a subject, and processed partly unconsciously by our brains, can have over online disclosure behavior. The experiments are ongoing. Preliminary results are directionally consistent with the proposed hypotheses, but not significant.
Kevin Fu

1. A widely taught engineering principle is that security and privacy must be built into a system; it cannot be effectively bolted on after the fact. Unfortunately, security and privacy tend to get ignored until a "unthinkable" crisis, at which point the system is difficult or impossible to fix. Google didn't encrypt all its backend systems until *after* the Snowden disclosures. Facebook did not curb use of unencrypted connections until *after* the Blacksheep hacker tool. Buffer overflows and poor password hygiene was not taken seriously until *after* the 1988 Morris Internet Worm. The open source community did not re-engineer OpenSSL until *after* HeartBleed. Target did not implement sufficient information security until *after* a massive data breach. It's like insurance; no one wants it until they need it. What advice do you have to incentivize computer system designers to respect security and privacy as core design requirements early in the engineering process rather than as an afterthought?

2. There's been a significant amount of attention to transparency of government surveillance, but why has the public not given the private sector as much scrutiny? Are we so naive as to think that corporate America has a serious commitment to consumer privacy when today consumers are the product being sold to advertisers? Where is the Edward Snowden of the private sector?

3. In the decades to come, the world is likely to see implantable devices that augment the mind and body rather than merely treat disease or support health and wellness. The technology will likely disrupt societal norms, and raise complex ethical questions. How is the interpretation and expectation of privacy likely to evolve as the line blurs between people and technology?
Martha Jones

Historians have a curious relationship to privacy. Our research frequently intrudes upon expectations of privacy. My field, early African American history frequently delves into spheres deemed private: personal correspondence, diaries, account books, DNA. Privacy aside, Professor Acquisti’s work raises questions.

Digital humanists are already using face recognition software to match images against a large data sets, and the results are exciting. The African American photographic archive is vast. But research has been constrained by the anonymity of the subjects. What if face recognition software might aid us in reconstructing that archive. Are there concerns for humanists who advance their work through such technologies? It appears that other fields are being subject to serious ethical scrutiny. Are historians getting off too easily?

Might be left out of the data be as troubling as being included? Take the census – that nineteenth century big data set. Enslaved people were enumerated without names, only by sex and age. Black Americans are thus hampered in their ability to trace their family pasts, as are historians in their ability to analyze the lives of slaves. Even today, the relative undercounting of African Americans leaves them out of political processes and policy debates. The late twentieth brought about two census changes: respondents themselves chose their racial identity, and, as of 2000, respondents could check more than one race. The results have confounded our comparative analysis of the data. How should big data projects accommodate shifting social and cultural norms and how do they contribute to them?

Finally, those amassing big data can be sure that they historians of the future will come looking for their records. How such data will be recorded, archived, and made available for future scholarly use.
Erin Krupka

At the junction of any computer system with its human user there is an opportunity for designers to nudge users to provide personal information. While in many cases information sharing can be for benevolent purposes, these techniques can be harnessed for more insidious purposes as Alessandro and colleagues’ most recent work on facial recognition and SSN prediction demonstrates. Despite the fact that there is strong concern for protecting privacy, several studies highlight the dichotomy between professed attitudes and actual self-revelatory behavior (Tedeschi 2002; Spiekermann 2001; Acquisiti and Gorssklags 2005; Acquisti and Ralph 2006). Some of the explanations for the dichotomy reside in the hurdles that hamper individuals' privacy-sensitive decision making: incomplete information, misplaced confidence, biases, cognitive limitations and heuristics specifically evolved to monitor being monitored that lead us astray. These hurdles make privacy valuations appear inconsistent and disclosure or sharing behavior often surprising. In effect, social systems that embody the mantra “public-by-default, private-through-effort” (Boyd, 2011), force the user to define “privacy” and to navigate the trade-offs for themselves with whatever cognitive tools and heuristics they have at hand. It is in these situations that social norms – context and group dependent heuristics that prescribe rules of conduct – emerge. Thus, while the values surrounding privacy are not in a state of flux, the infrastructure through which we interact and the associated social norms that govern behavior are. Future battles over privacy will be fought in the social arena and will be focused on the norms that govern interaction on these platforms.
Catharine A. MacKinnon

Acquisti et al’s work assumes that the relevant internet disclosures and revelations begin voluntarily, and that privacy is intrinsically protective. Neither is the case for offline sexual abuse or in most online sexual abuse either. Online, sexual predators stalk unwilling victims in anonymity; use prostituted women and children by live feed in real time; “rape” avatars in chat rooms; surveil, steal, and disseminate intimately violating visual and verbal materials for voyeurism, revenge, reputation destruction, bullying, and sexual harassment. Rapists videotape their rapes and trade or post them, sometimes for blackmail. Pornography is the largest single use of the internet, providing a huge profit motive to use people to make it, spreading sexual abuse in its wake. Sexual abuse is a significant dimension of so-called augmented reality, for which the internet provides a window as well as a vector.

Privacy has never provided significant protection from sexual and other violence against women. On the contrary, it creates a setting for intimate abuse and shields it from recourse. Structurally, for example, interpersonal closeness tends to keep rape and domestic battering from prosecution on the view that such relationships are properly private. Possession of guns in private homes, the most dangerous place for women, is recognized as a right without weighing its effects on them. Doctrinally, the consumption of obscenity at home is protected as a privacy right, as if its user can be presumed alone there and the materials have no effects, a canard long empirically disproven. The people used to make pornography, and those on whom it is further acted out, have no meaningful privacy from it. The recent recognition of rights to gay sex on a privacy rationale proceeded on the view, unevidenced and unwarranted, that no sexual abuse is possible between persons of the same sex.

Once sexual abuse is understood as a violation of gender equality, as it is internationally, privacy emerges as perhaps intrinsically unworkable as protection in this sphere, and possibly others.