OPEN TECHNOLOGY INSTITUTE

NEW AMERICA

DATA AND DISCRIMINATION: COLLECTED ESSAYS

EDITED BY SEETA PEÑA GANGADHARAN
WITH VIRGINIA EUBANKS AND SOLON BAROCAS

TABLE OF CONTENTS

OCTOBER 2014

Introduction: Data-Based Discrimination

SEETA PEÑA GANGADHARAN
SENIOR RESEARCH FELLOW, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

INTRODUCTION

Despite significant political and cultural transformations since the Civil Rights movement and other social upheavals of the Sixties and Seventies, discrimination remains a problem. And while persistent inequities stem from a complex set of factors, digitally automated systems may be adding to these problems in new ways.

These systems run on the data produced in our daily digital meanderings and on algorithms trained to identify patterns among different data points. The result of these computerized calculations include predictions of our future behavior, recommendations for the purchase of one product or another, advice that we modify our behavior, feedback and adjustments to the operation of computer controlled systems, and more. From White House officials to civil rights advocates to "quants" and "techies," many have begun to question the power of algorithmically driven systems to categorize, nudge, prime, and differentially treat people in ways that can exacerbate social, economic, and racial inequities.[1]

In late 2013, New America's Open Technology Institute (OTI) began organizing a research convening to explore these concerns. Our goal was to unravel basic aspects of data-based discrimination, an umbrella term that I use to refer to processes of algorithmically driven decision-making and their connection to injustice and unfairness in society. We wanted to examine what's at stake for society and contemplate how to grapple with problems that might arise. We decided to hold the event as part of an annual meeting of the International Communication Association (ICA), which draws academics from around the world, and issued a call for proposals to ICA community and beyond, on the topic of data and discrimination. The event, held on May 22, 2014, in Seattle, Washington, featured a dozen researchers that ranged from tenured professors to doctoral students. They presented papers that fell into one of three thematic categories: "Discovering and Responding to Harms," "Participation, Presence, and Politics," and "Fairness, Equity, and Impact."

The collection of papers presented here—and edited with the assistance of two researchers at the convening, Virginia Eubanks and Solon Barocas—reflects most of that day's investigations as new ideas that germinated in ensuing months. Altogether the papers aim to provide basic information, attempt to provoke discussion and debate, and, hopefully, suggest trajectories for further research and writing, including in areas unexplored or under-addressed.

In the pages that follow, the authors address data-driven discrimination in a wide variety of contexts, for example, health, public utilities, and retail. They identify a broad range of concerns, such as the difficulty of replicating data collection and analytics processes whose inspection might reveal insights into discrimination by algorithm. They examine the networked nature of harms, and the role of law, including social policies, that set the

Different data we reveal through our daily digital habits represent tiny pieces of our identity. When aggregated and analyzed using different big data techniques, these data profiles may run counter to how we define ourselves and impact our ability to shape personal destinies. Photo by Michael Mandiberg. CC BY-SA.

terms of development and deployment of automated, data-driven systems. The authors also contemplate a broad set of solutions: revealing weaknesses of existing transparency and accountability mechanisms in order to forge new and better ones, mobilizing data-driven processes to ameliorate discrimination, and broadening public discussion on the future uses and consequences of data-driven systems in order to influence choices about their development and deployment.

As we head into an era of more and more data collection, analysis, and use, the urgency of producing sound research and analysis cannot be understated. There's a real threat that the negative effects of algorithmic decision-making will disproportionately burden the poorest and most marginalized among us. Grappling with the complexity of data-driven discrimination is no easy task, and this collection marks one modest step in bringing to light processes and problems that otherwise might remain invisible and unquestioned.

Index

1. United States, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. See also The Leadership Conference on Civil and Human Rights, *Civil Rights Principles for the Era of Big Data*, February 2014, http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html; Alistair Croll, "Big Data is Our Generation's Civil Rights Issue, and We Don't Know It," *O'Reilly*, August 2, 2012, http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html; Cathy O'Neil, "How Can We Regulate Around Discrimination?" *mathbabe* [blog], February 24, 2014, http://mathbabe.org/?s=discrimination.

Acknowledgments

I would like to thank the Ford Foundation for its support of OTI's work on data and civil rights. Also, thanks to New America colleagues Josh Breitbart, Greta Byrum, Gina Barton, Ryan Gerety, and Kevin Bankston for their input along the way. The final acknowledgment goes to Virginia Eubanks and Solon Barocas for assisting in the editing process and helping to translate research for broader audiences.

Part 1: Discovering Harms

OCTOBER 2014

An Algorithm Audit

CHRISTIAN SANDVIG
ASSOCIATE PROFESSOR, COMMUNICATION STUDIES AND SCHOOL OF INFORMATION, UNIVERSITY OF MICHIGAN

KEVIN HAMILTON
ASSOCIATE DEAN OF RESEARCH, COLLEGE OF FINE AND APPLIED ARTS AND ASSOCIATE PROFESSOR OF NEW MEDIA AND PAINTING, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

KARRIE KARAHALIOS
ASSOCIATE PROFESSOR, COMPUTER SCIENCE AND DIRECTOR, CENTER FOR PEOPLE & INFRASTRUCTURES, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

CEDRIC LANGBORT
ASSOCIATE PROFESSOR, AEROSPACE ENGINEERING AND CO-DIRECTOR, CENTER FOR PEOPLE AND INFRASTRUCTURES, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

AN ALGORITHM AUDIT

When it is time to buy a used car, many consumers turn to the advice of a trusted third-party like the Consumers Union, publisher of Consumer Reports. While we may not know anything about how cars work, Consumer Reports operates a test track where automotive experts run cars through their paces. Even better, to devise its public rating for a particular model Consumer Reports sends current owners a survey to draw conclusions from their past experiences. Finally, Consumer Reports is trustworthy because it is a non-profit advocacy organization collectively organized by consumers with no relationship to the auto industry.

We need a Consumer Reports for algorithms.

Invisible Algorithms Dominate Our Everyday Life

Computer algorithms now dominate our daily life, providing our communication with our family and friends, our search for housing, our media preferences, our driving directions, the advertisements that we see, the information we look up, encryption of our data for our privacy, and more.

Yet there is a tremendous gap between public understanding of algorithms and their prevalence and importance in our lives. For instance, the majority of Facebook users in a recent study did not even know that Facebook ever used an algorithm to filter the news stories that they saw.[1]

Unfair Algorithms, Undetectable Without Help

Algorithms differ from earlier processes of harmful discrimination (such as redlining) in a number of crucial ways. First, algorithms that affect large number of people (e.g., the Google search algorithm) are complicated packages of computer code crafted jointly by a large team of engineers.

These algorithms represent trade secrets.

Second, the computer code for an algorithm does not make it interpretable. At the level of complexity that is typical for these systems, an algorithm cannot be interpreted by reading it. Even an expert in the area (or the algorithm's authors) may not be able to predict what results an algorithm would produce without plugging in some example data and looking at the results.

Third, algorithms also increasingly depend on unique personal data as inputs. As a result, the same programmatically generated Web page may never be generated twice.

Finally, we have little reason to believe the companies we depend on will act in our interest in the absence of regulatory oversight. Almost every major operator of an Internet platform, including Google, Twitter, Facebook, Microsoft, and

"Dislike Graffiti." Photo by zeevveez. CC-BY-2.0.

Apple, has already been investigated by the U.S. government for violations that include anti-competitive behavior, deceptive business practices, failing to protect the personal information of consumers, failing to honor promises made to consumers about their own data, and charging customers for purchases that they did not authorize.[2]

Testing the Platforms that Test Us

Luckily, a method exists for researchers to look inside these complicated, algorithmically driven computer decision systems: the "audit study".[3] This method, which serves as *the* most respected social scientific method for the detection of racial discrimination in employment and housing, uses fictitious correspondence. For instance, an audit study might submit fictitious resumes targeted at a real employer or fictitious housing applications targeted at a real landlord. In these studies, researchers test the fairness of an employer or landlord by preparing two or more equivalent documents which reflect equal backgrounds, including levels of education and experience, but which only vary according to race. For example, researchers could manipulate the fictitious applicant's race between the two conditions of "Emily" and "Lakisha" to signal "Caucasian" vs. "African-American" to a prospective employer. The difference in employer responses to two otherwise identical resumes therefore measures racism.

In the spirit of these real-life audits of employers and real estate agents performed by journalists and watchdog organizations, we propose that the

Lemons at a market. Photo by MarcusObal. CC-BY-SA-3.0.

recent concerns about algorithms demand an audit of online platforms. In essence, this means Internet platforms powered by large amounts of data (e.g., YouTube, Google, Facebook, Netflix, and so on) that are operated via secret computer algorithms require testing by an impartial expert third party. These audits will ascertain whether algorithms result in harmful discrimination by class, race, gender, geography, or other important attributes.

Although the complexity of these algorithmic platforms makes them seem impossible to understand, audit studies can crack the code through trial and error: researchers can apply expert knowledge to the results of these audit tests. By closely monitoring these online platforms, we can discover interactions between algorithm and data. In short, auditing these algorithms demands a third party that can combine both expert and everyday evaluations, testing algorithms on the public's behalf and investigating and reporting situations where algorithms may have gone wrong.

Lemon Warnings in a Data-Driven Society

We envision a future where Internet users can know in advance if a search box is planning to take advantage of them; platform "lemon warnings" that can explain the operation of faulty or deceptive social media sites; and quality rankings which tell us when an algorithm is working for us or for someone else.

Index

1. Christian Sandvig, Karrie Karahalios, and Cedric Langbort, *Uncovering Algorithms: Looking Inside the Facebook News Feed*, In the Berkman Center Seminar Series: Berkman Center for Internet & Society, Harvard University (July 22, 2014): http://cyber.law.harvard.edu/events/luncheon/2014/07/sandvigkarahalios.

2. US Department of Justice, *United States v. Microsoft Corporation*, Civil Action No. 98-1232 (1999): http://www.justice.gov/atr/cases/ms_index.htm#other; Federal Trade Commission, *In the matter of Twitter, Inc., a corporation*, File number 092 3093 (2010): http://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation; Federal Trade Commission, *In the matter of Google, Inc. a corporation*, File number 102 3136. (2011): http://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter; Federal Trade Commission, *In the matter of Facebook, Inc., a corporation*, File number 092 3184 (2011): http://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc; Federal Trade Commission, *In the matter of Apple, Inc., a corporation*, File number 112 3108 (2014): http://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc.

3. Devah Pager, "The Use of Field Experiments for Studies of Employment Discrimination: Contributions, Critiques, and Directions for the Future," *The Annals of the American Academy of Political and Social Science* 609, no. 1 (2007): 104-33.

OCTOBER 2014

Health Privacy Online: Patients at Risk

TIM LIBERT
PHD CANDIDATE, ANNENBERG SCHOOL FOR COMMUNICATION, UNIVERSITY OF PENNSYLVANIA

HEALTH PRIVACY ONLINE: PATIENTS AT RISK

Unprotected Information-Seeking

According to the Pew Internet and American Life project, over 70 percent of U.S. adults go online to seek health information.[1] Such information comes from a variety of sources ranging from government agencies to non-profit organizations, commercial websites, newspapers, discussion forums, and beyond. These sites, like many others, often rely on third parties to deliver advertisements to their users. In so doing, sites that are a source of health information also grant advertisers the opportunity to track users and learn about their interests.

While many users likely assume that legal protections apply to information about their health-related browsing habits, few, if any, regulations actually bear on this type of activity. Website operators and other third parties can glean details about users' health concerns and health status from their browsing behavior that may be intentionally or inadvertently misused. Health privacy policies in the Big Data era need a fresh look.

Evidence of Information Leakage

In order to explore the potential risks to health privacy online, I recently analyzed over 80,000 health-related web pages and determined that 90 percent leaked user information to outside parties.[2] The amount of information leaked varies in degree, but nearly always includes the address of the page currently being visited, which can be very revealing. For example, noticing that a user has visited http://www.cdc.gov/cancer/breast/, an advertiser may reasonably infer she has a concern with breast cancer. This type of information leakage is a widespread problem. My study demonstrated that 70 percent of health-related websites have addresses which contain information on specific symptoms, treatments, and diseases.

Equally Common Problem on Commercial and Non-Commercial Websites

Most often the parties collecting data are online advertisers who are not subject to extant health privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA). These advertisers can track users on commercial sites such as WebMD, but also government and non-profit sites such as the Centers for Disease Control (CDC) and the Mayo Clinic. It is not surprising that commercial sites, which rely on advertising revenue to operate, allow advertisers to monitor their users, but it is surprising that government and non-profit entities supported by tax dollars and donations do.

As it turns out, non-commercial sites often utilize outside services to analyze their website traffic and facilitate social media sharing, which online advertisers provide free of charge in order to learn more about users. To take one example, as of April

The WebMD page for "Breast Cancer" initiates connections to nearly 30 outside domains, including to one owned by the data broker Acxiom. Image by Tim Libert.

2014, a user visiting the CDC website would have had their browsing information transmitted to Google, Facebook, Pinterest, and Twitter.

Risks of User Identification

While advertisers do not learn the name of a user during individual page visits, the aggregated browsing behavior of users can nevertheless paint a revealing portrait of who they are, presenting two risks: user identification and commercial discrimination.

In the first instance, advertisers which learn that a particular user has a specific illness may misuse or leak this information. Occasionally, third parties that can observe when users visit specific health sites also possess information about users' real names. Facebook, for instance, could easily create a link between logs of health-related web browsing and an identifiable person. Even if users place trust in companies like Facebook, such information, as is evident in the ever-present cybercrime headlines, may be stolen by criminals and leaked online.

Furthermore, data collection on health websites is also being performed by so-called "data brokers" who sell personally identifiable information to a range of clients. A recent U.S. Senate hearing revealed that the data broker MedBase200 has sold lists of individuals under the headings of "rape sufferers", "domestic abuse victims", and "HIV/AIDS patients".[3] Where MedBase200 got this data is unclear, but there is little doubt that bad actors could purchase and abuse this information.

Existing health privacy laws like HIPAA do not apply on the web. "Nurse Shredding Papers for HIPAA Compliance." Image by Compliance and Safety. CC-BY-SA.

Risks of Commercial Discrimination

The second risk is that even without their names being disclosed, those interested in health conditions may be disadvantaged commercially. Online advertisers use aggregate browsing information to place users into "data silos", marking the desirable as "target" and the less fortunate as "waste".[4] Given that over 60 percent of bankruptcies are medical related,[5] it is possible that those with an interest in specific health conditions may be categorized as waste and thereby denied the favorable discounts and interest rates given to those in the target category. If health-related browsing behavior happens to correlate with a commercially desirable outcome, online advertisers may subject users with certain health conditions to less favorable treatment even if they have no such intentions. Preventing inadvertent outcomes of this sort is not trivial, as advertisers may struggle to distinguish between information which is sensitive and that which is not.

An Ounce of Prevention Is Worth a Pound of Cure

While there is not yet clear evidence of misuse of health-related browsing information, as with medicine, an ounce of prevention is worth a pound of cure.

Three strategies can immediately reduce the risks to users seeking health information online. First, government and non-profit websites which use services that leak user data to advertisers should investigate and utilize the many privacy-friendly solutions for page metrics and social media sharing. Second, while commercial actors have drawn up industry guidelines for self-regulation, the FTC has stated that such efforts "have failed to provide adequate and meaningful protection".[6] Therefore, there is an opportunity to craft policies and legislation which would better protect user health information. Third, software engineers working for online advertisers may take the initiative and create intelligent filters which analyze incoming data to ensure that sensitive medical data is never stored or acted upon.

These three strategies each involve achievable goals, and may go a long way in protecting some of the most vulnerable members of our society.

Index

1. Fox, Susannah, and Maeve Duggan. *Health Online 2013*. Washington, DC: Pew Internet and American Life Project, 2013. http://www.pewinternet.org/2013/01/15/health-online-2013/

2. Libert, Tim. "Privacy Implications of Health Information Seeking Online." *Communications of the ACM*, In Press.

3. U.S. Congress. Senate. Committee and Commerce, Science, and Transportation. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, 2014. http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

4. Turow, Joseph. *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth*. New Haven: Yale University Press, 2012.

5. Himmelstein, David U., Deborah Thorne, Elizabeth Warren, and Steffie Woolhandler. "Medical Bankruptcy in the United States, 2007: Results of a National Study." *The American Journal of Medicine* 122 (2009): 741-746.

6. U.S. Federal Trade Commission. *Protecting Consumer Privacy in An Era of Rapid Change. A Proposed Framework for Business and Policymakers, Preliminary Staff Report*, 2010. http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

OCTOBER 2014

Locating Discrimination in Data-Based Systems

DARREN STEVENSON
PHD CANDIDATE, COMMUNICATION STUDIES DEPARTMENT, UNIVERSITY OF MICHIGAN

LOCATING DISCRIMINATION IN DATA-BASED SYSTEMS

A Knowledge Deficit

The video game *DataDealer.com* offers a playful take on digital privacy, personal information collection, and questionable data use by firms. Players take on the role of an unscrupulous data broker, stepping into the largely opaque world of personal information brokerages, where companies aggressively collect, use, trade, and sell individuals' data. Players collect data about unsuspecting individuals, selling it to others. In the game's opening trailer, someone is denied housing, insurance, and a job based on personal information held by firms.

While each of these practices is subject to regulation, the game reflects mounting concern with the various ways firms collect, combine, analyze, and monetize the details of our digital lives. Indeed, the game plays on growing anxieties over the commercial use of personal data, the specifics of which are typically unknown to the public.

Are these fears justified? Thus far, and to the dismay of civil rights advocates, policymakers, and regulators, the answer is we simply do not know. To date, these concerns have stemmed more often from speculation than observation. And the absence of concrete examples has tended to forestall meaningful debate and regulation.

I want to briefly suggest two reasons why it has been relatively difficult to detect instances of discrimination in today's big data ecosystem and offer some suggestions for how we might combat this knowledge deficit.

Technical Challenges

First, while the potential for data-based discrimination has grown dramatically in recent years, tools to parse how these systems function have not developed in parallel. There have been few, if any, economic incentives encouraging their development. As a result, there are scarce options available to analyze and make transparent the inner workings and effects of these systems themselves.

To study how algorithms and platforms function, instead researchers must typically go through labor-intensive manual processes. This includes tasks like manually varying search engine queries and meticulously altering one's user profile or internet protocol address in search of different treatments or outcomes.

One way we might combat this technical barrier is to develop software and best practices to support robust audit studies of information systems. The most prominent example of audit studies offline includes submitting multiple nearly-identical résumés to job solicitations, altering applicants' names and selecting names commonly associated with certain races. All else being equal, observed differences in response rates can be attributed to rather discrete forms of discrimination.

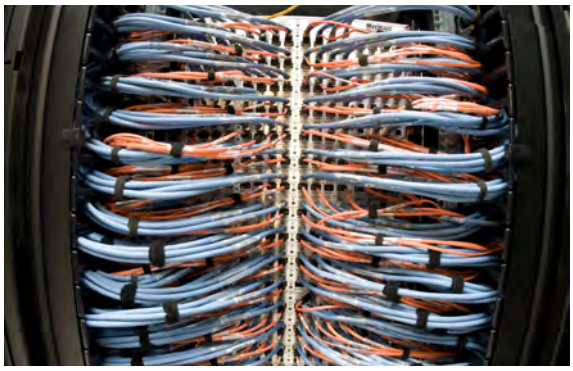
Digital information systems play increasingly important roles in determining social outcomes, including things like credit pre-approvals and pre-screenings for job applicants. "data path Ryoji.Ikeda – 3." Photo by r2hox. CC-BY-SA 2.0

Advancing computational audit studies will require detection methods well tuned to the underlying technologies of current commercial systems. For instance, if a decision support system handling employment pre-screenings or credit card approvals relies on connecting disparate personal data, machine learning, and Bayesian reasoning, then developing auditing software of similar sophistication may be necessary to test for prejudicial outcomes.

Legal Challenges

Second, attempts to detect discrimination in information systems also face significant non-technical challenges. Typically, commercial service providers maintain strict terms of services to prevent outsiders from abusing or studying their technology. Often these represent blanket attempts to prevent competitors from analyzing, understanding, and then either reverse engineering or gaming their systems.

Additionally, multiple well-intentioned but overreaching laws have created legal barriers, effectively criminalizing most attempts at studying online systems, regardless of intent. The most notable is the Computer Fraud and Abuse Act (CFAA), which allows the government to prosecute anyone who violates a website's terms of service.[1] Nearly any attempt by researchers to investigate how proprietary information systems function, even in search of discrimination, is likely to violate terms of service. These laws have the perverse result of protecting data-driven commercial systems from even the most basic external analysis.



Sophisticated computational tools leverage the power of information networks to provide our digital conveniences. But this complexity makes it hard to detect discrimination in these systems. Photo by Argonne National Laboratory. CC-BY-NC-SA 2.0.

An intelligent overhaul of CFAA is needed. To begin, the law should not grant firms the right to unilaterally shield from any outside scrutiny the systems that play such a vital role in our lives. Furthermore, attempts to detect misuse of data should not fall under the same law as malicious hacking or efforts to reverse engineer a competitor's technology. The law needs to be updated and made sensitive to these differences ensuring it does not proscribe socially beneficial probing of data-driven decision-making.[2] Given the stakes, a complete prohibition of external examination is simply unacceptable. Carving out exceptions for these kinds of analyses would allow researchers to leverage the power of audit studies applied computationally.

Coordinated Efforts

Of course, overhauling current laws will require coordinated efforts, including gaining the support of industry representatives. Additionally, developing computational audit studies will require substantially more technical know-how than traditional audit studies, more than printing up and mailing out fake résumés with different names. But again, the challenging nature of the problem is no excuse for not pursuing it.

We can do much better than speculate. We can enact smarter legislation that protects the interests and trade secrets of firms and allows outsiders to hold them accountable for misuse. We can develop tools and software to test for systematic mistreatment and disparate impacts. Empirical insights into the functioning of these systems could also reveal that current fears are largely misplaced. Developing a clear path for examining these systems is one way we might better know the extent of the problem at hand, and then, if there really is a problem, how to work towards solutions.

Index

1. Greyes, Natch. "A New Proposal for the Department of Justice's Interpretation of the Computer Fraud & Abuse Act: Note." *Virginia Journal of Law and Technology*, 17 (Winter 2013): 293-354. http://www.vjolt.net/vol17/issue4/v17i4_292_Greyes.pdf.
2. Some efforts to reform CFAA are currently underway, see https://www.govtrack.us/congress/bills/113/hr2454 and https://www.govtrack.us/congress/bills/113/s1196. However, these efforts have stalled out due to current Congressional dysfunctions and inaction. see Fox-Brewster, Thomas. "Aaron's Law is Doomed Leaving US 'Hacking' Law Broken." *Forbes* (August 6, 2014). http://www.forbes.com/sites/thomasbrewster/2014/08/06/aarons-law-is-doomed-leaving-us-hacking-law-broken/.

OCTOBER 2014

Big Data and Unattainable Scholarship

ERIK BUCY
REGENTS PROFESSOR OF STRATEGIC COMMUNICATION, TEXAS TECH UNIVERSITY

ASTA ZELENKAUSKAITE
ASSISTANT PROFESSOR OF COMMUNICATION, DREXEL UNIVERSITY

A SCHOLARLY DIVIDE

How Accessible is Big Data?

Recent decades have witnessed an increased growth in data generated by information, communication, and technological systems, giving birth to the "Big Data" paradigm. The availability of Big Data discriminates in any numbers of ways: between analysts who sift through reams of available data points to discover patterns of behavior in users and users who (largely unwittingly) generate data for analysis; between marketers who conduct segmentation studies to more effectively target consumers and consumers who are targeted by an increasingly number of tailored ads; and, recently, between scholars who have access to Big Data to perform novel analyses and researchers who lack the technological savvy to extract Big Data for modeling.

The proliferation of Big Data analysis creates inequities within the research community.

The promising world of unprecedented precision and predictive accuracy that Big Data conjure thus remains out of reach for most social scientific researchers, a problem that traditional media did not present. The uneven dynamics of this curious but growing "scholarly divide" between researchers with the technical know-how, funding, or inside connections to extract data and the mass of researchers who merely hear Big Data invoked as the latest, exciting trend in unattainable scholarship evokes the notion of a scholarly divide.

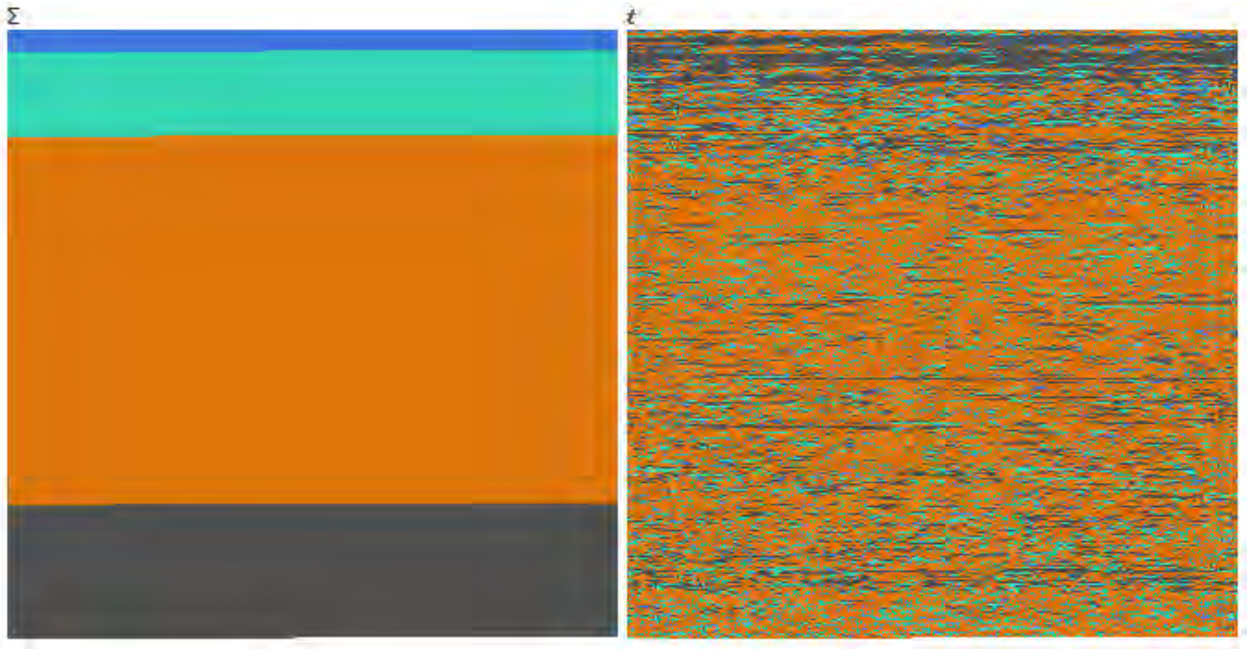
Complexity and Covertness

This situation has several causes. First, consider the complexity of the system architecture that makes the collection of Big Data possible. To a large extent, the unavailability of Big Data derives from the automatic or *covert* way it is collected. Unlike traditional media contents, which are published or broadcast *overtly* and within public view, much user-generated content is covertly gathered as a byproduct of software design decisions, and the unintended traces left behind by users. These digital traces are comprised of metadata of user activities, registration and location logs, and tweets, likes, and posts to social media. Other expressed preferences, in the form of purchases, opinions, and reviews are recorded while users navigate their way through networked systems. And did we mention DVRs? The portrait of actual television viewing available to the research community has never been more precise—if you have access.

Access to data has become an important discriminating factor in new technology research.

Because covert data are inaccessible without system-level access and understanding, the ability to retrieve and model Big Data is becoming as important to traditional academic training as classic research methodology and analysis.

Prior to digitalization, mass media contents were



Data visualization of casualties in the Iraq conflict created by Kamel Makhloufi. Blue represents casualties as a result of friendly fire, green represents military casualties from the host country, orange is civilians, and grey is enemy combatants. Time is progressing in the right hand image from the top left to bottom right. Data was scraped from the *Guardian*. Photo by Kamel Makhloufi, CC-BY-2.0.

generated from a central source, they were not proprietary in nature, and seldom was user-generated data integrated into programming, as they now are. Focused on the dissemination of information that was plainly visible, rather than the capture and storage of consumer data that would never be shared, mass media did not raise concerns about the representativeness of available content and audience analysis was conducted by means of separate data collections, typically large scale surveys.[1]

"Data Gatekeepers"

Now, with the growth in data types, particularly user-generated content and information contained in data logs, and the ownership of these data by media companies and technology firms, access to data has become an important discriminating factor in new technology research.[2] In this new sociotechnical configuration, users generate data not as members of a media audience but as subscribers to, or registrants in, a private information or communication service. Proprietary platforms such as Facebook require users to register on their social media sites to access services. Ironically, services largely consist of mini-subscriptions to the content of other users, in the form of news feeds and updates from networked "friends."

As more data streams emanate from more platforms than ever before, access to data remains limited and largely out of reach to all but a handful of selected researchers with the technical chops, award-worthy ideas, or connections to put together a winning proposal.[3] Indeed, the most interesting, log-based data are locked by private providers. Twitter recently accepted applications from academics to mine its data archive, but these

A New York City municipal data center. Photo by the NYC Department of Information Technology and Telecommunication, CC BY-NC-SA 2.0.

awards only went to a select few—and were decided by Twitter. In this sense, technology companies are becoming the new data gatekeepers and indirectly regulate the amount of new (public) knowledge that scholars can generate.

Technology companies are the new data gatekeepers.

From a research standpoint, then, what should be overt is kept covert. Theoretically, this situation is problematic. On the one hand, the research community builds and verifies new concepts and knowledge on the basis of publically available data (the government-funding model)—and publishes the results of data analyses for all to see; on the other hand, in certain domains of research, private data (and perhaps intelligence) appear to be gaining the upper hand over public data and knowledge in the volume and precision of information available. In digital and social media research (as with marketing and consumer research), access to user data has a direct impact on the value generation associated with scholarly analysis.

Increasingly, (social) media research is becoming dependent on computer science training, interdisciplinary collaboration, and corporate cooperation. Scholars in the social sciences and even humanities, used to working within their own research enclaves of like-minded theorists and methodologists, are becoming dependent on computer scientists to mine this brave new world of data-derived insights. Programming ability is no longer an exotic tool but a must-have skill, pushing social science towards *computational* science. And at a time when federal funding for social science is under threat (witness yearly efforts in Congress to defund National Science Foundation support for political science research), there is money for Big Data R&D, as with the Obama administration's $200 million initiative to "access, organize, and glean discoveries from huge volumes of digital data" announced in 2012.[4]

Solutions

Researchers who eschew computational collaboration from more technical disciplines will increasingly find themselves relegated to manual data collection and interpretive license over a relatively small amount of content that is publicly available. To reduce this developing scholarly divide, training in Big Data should include the tools and techniques of *covert* data extraction and analysis—means of discovery every bit as important as traditional methods. With the growth of Big Data, graduate training should move towards requiring programming as a skill or outside area. And scholarly associations should sponsor workshops and forge ties with industry to leverage access to data. Otherwise, the future of Big Data research seems to be one of increasing segregation, divided on the basis of subdisciplinary training and expertise.

Index

1. Axel Bruns, "Faster Than the Speed of Print: Reconciling 'Big Data' Social Media Analysis and Academic Scholarship," *First Monday 18*, no. 10 (2013): http://firstmonday.org/ojs/index.php/fm/article/view/4879/3756#p3.
2. Sometimes, the availability of data is in the hands of users, as when Facebook or Twitter users opt to keep their postings or tweets private; even so, the company itself retains access to all user information.
3. Klint Finley, "Twitter Opens Its Enormous Archives to Data-Hungry Academics," *Wired.com* (February 6, 2014): http://www.wired.com/2014/02/twitter-promises-share-secrets-academia/.
4. U.S. Executive Office of the President, Office of Science and Technology Policy, "Obama Administration Unveils 'Big Data' Initiative: Announces $200 Million in New R&D Investments" [press release] (Washington, DC, March 29, 2012): http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf.

Part 2: Participation, Presence, Politics

OCTOBER 2014

Retailing and Social Discrimination: The New Normal?

JOSEPH TUROW
ROBERT LEWIS SHAYON PROFESSOR OF COMMUNICATION, ASSOCIATE DEAN FOR GRADUATE STUDIES, ANNENBERG SCHOOL FOR COMMUNICATION, UNIVERSITY OF PENNSYLVANIA

LEE MCGUIGAN
PHD CANDIDATE, ANNENBERG SCHOOL FOR COMMUNICATION, UNIVERSITY OF PENNSYLVANIA

EVERYDAY TARGETING

The retail environment is a central location where the data-technology industry is habituating people to new realities around surveillance and the personalization of the commercial sphere. From a policy perspective it's crucial to understand whether these developments bode a new normal for U.S. society.

In-Store Media

As in-store media become digital, they tie into people's handheld mobile lives and transform the ways retailers relate to one another and to their customers. A major contemporary development is the interconnection of three developments: mobile devices, location tracking and social media. According to eMarketer, in the U.S., nine out of ten American adults now have a cell phone, and 57 percent own a smartphone. About eight in ten (81 perecent) people send or receive text messages, up from 65 percent in 2009. Sixty percent access the web via mobile; fifty percent download apps; and 40 percent of Facebook revenues now come from mobile.

Retailers see these media as both threats and opportunities. The threat comes from "showrooming"—the use of mobile devices to check prices and social-media opinions about a product while in a physical store and to purchase it less expensively from the device instead of from their physical location. The opportunity comes from the technological ability to link the in-store (or near-store) location of individuals to other behavioral data gleaned from the mobile devices as well as to purchasing and demographic information previously collected by the store. Physical store executives believe this approach can lead to the kinds of personalized offers that will discourage showrooming and encourage in-store loyalty.

On the surface, these activities seem simply to be a struggle among sellers, but they have profound societal importance. These new retailing technologies habituate people to new realities around surveillance and personalization throughout society. Even more than the marketers and government agencies which "do surveillance," the retail institution is playing a critical everyday role in shaping society's understanding and experience of friendship, sharing, privacy, and anonymity. It is creating what philosopher Charles Taylor terms a new "social imaginary," meaning the public's common understanding of how the world works and what is "normal."[1]

The New Dynamics of Retailing

The new social imaginary of retailing involves a full reshaping of the store and its relation to the shopper based on surveillance and data interpretation. Here we can only mention some of the major changes taking place.

Reshaping the store's relation to the shopper entails creating data-based and interactive interactions between the individual shopper and

A traditional way of signaling price to consumers in an 1886 summer catalog from Grands Magasin de la Samaritaine. (PD-art).

the merchant. In the words of the Forrester consultancy, the new norm is "a company in which customer knowledge is drawn from everywhere, created centrally, and shared across the entire enterprise, so all stakeholders can act upon it and measure the results."[2] Doing this means seeing a known person as potentially always a shopper. It requires new approaches to customer relationships, identities, and loyalty.

The reshaping of the store refers to the merchant's ability to alter the physical and digital manifestations of their messages, deals, and prices based on the merchant's data-driven understanding of the individual shopper. Among the technologies emerging for these ends are geo-fencing, Bluetooth low-energy and WIFI tracking, facial recognition, digital-loyalty programs, and various mobile payment technologies. The reshaped deal comes out of the new approaches to the shopper and the store. Data points collected through the online and offline tracking technologies allow retailers to act differently toward customers based on the worth a merchant places on each person and how it affects the deal he or she receives. Two primary factors in creating dynamic deals involve an understanding of the shopper's "lifetime value" to the merchant and the dynamic nature of competitors' prices online and off.

Large-Scale Considerations

The large-scale habituation of the population to surveillance through shopping impacts both the retailing institution and society at large. The programs are transforming the architecture of physical and digital retailing, and the relationship between the two, in ways that make the selling environment increasingly dynamic and mutable for sellers and the individual prospect. Sellers will have to change prices constantly, introduce new products rapidly, and continually adopt new ways to define, identify, track, re-evaluate, and keep customers they define as winners. As for shoppers, the new dynamic environment will add to their stress about product quality and cost and create uncertainty regarding what stores know about them, how the stores score them, and what impact these processes have on them.

As public emporiums make greater use of customer-value algorithms, they begin to treat customers differently from one another based on information unknowable even by the customers themselves. Retailers—or the algorithms they apply to their customer databases—decide what constitutes attractive shopping agendas, information, and prices, targeting certain people rather than others. Through it all, knowingly and not, retailers are transforming data analysis into a force to be reckoned with. It seems likely, for example, that social stress about individuals' place and value in society will rise with their uncertainty regarding what stores know about them, how the stores score them, what discount offers they present to them, and what other inducements they provide compared to what they offer other people. Shopper targeting based on arcane findings of

Index

1. Taylor, Charles. *A Secular Age*. Cambridge, MA: Harvard University Press, 2009.
2. Sarno, Jody. *The Age of the Customer Requires a More Intelligent Enterprise*. Cambridge, MA: Forrester Research, January 24, 2014. https://www.forrester.com/The+Age+Of+The+Customer+Requires+A+More+Intelligent+Enterprise/fulltext/-/E-RES112082 (accessed October 8, 2014).

OCTOBER 2014

The State of Data: Openness and Inclusivity

TIM DAVIES
PHD CANDIDATE, WEB SCIENCE, UNIVERSITY OF SOUTH HAMPTON

This work was supported by a Research Placement Grant from the "NEMODE—New Economic Models in the Digital Economy" programme funded by Research Councils UK (RCUK).

RE-ARCHITECTING AN INCLUSIVE OPEN DATA STATE

The Data-Lens of the State

The data architecture of the modern state is being quietly redesigned. In parallel, central registers are being rationalized, periodic surveys replaced with flows of proprietary big data, and other datasets opened up through data portals and open data policies. And although in practice policies are rarely data-driven (it unsurprisingly turns out that political concerns generally trump data when it comes down to the vote), the data the state holds does shape the debates and scaffolds the delivery of policies and public services.

The categories that exist inside government datasets, and the balance of datasets that make it into the public domain, contribute to a landscape in which certain policies are easier to design or implement than others.

Certain groups become easier to see (or surveil), while other groups effectively disappear—unseen through the data-lens of the state.

Seeing the State

The open data movement has hopes of "seeing the state."[1] And in our complex modern states, effective scrutiny of power requires (amongst other things) access to machine-readable datasets. Yet, in calling for government data to be made open it's important to consider a number of potential data and discrimination challenges.

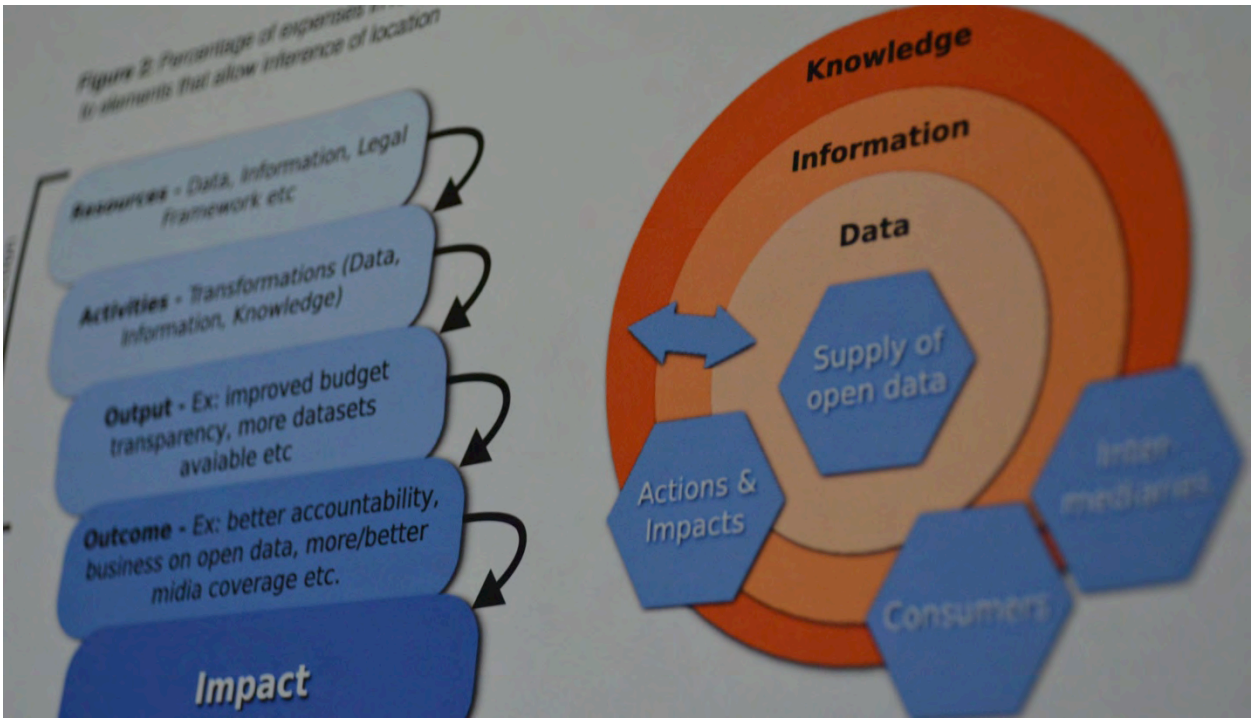
Selective Opening of Data

First, when open data initiatives leave it to governments to decide which datasets to release, rather than creating a legally backed right to data for citizens, governments retain the power to release data strategically. They may select the datasets least likely to enable critical scrutiny, or may, as the current right-of-center UK administration did, focus on releasing decontextualized spending data, fuelling a discourse about profligate public spending in order to legitimize public sector cuts that have since been shown to impact heavily on marginalized groups.[2]

Securing a right to data, and articulating the core elements of an "accountability stack" of datasets,[3] are all vital to ensure open data can provide a platform for true transparency, accountability, and open public discourse.

Privacy Paradox

Second, the demand for raw and disaggregated data creates a privacy paradox. It's generally accepted that datasets containing personal information of citizens should not be released in



Research poster exploring the layers involved in creating and using open data. Intermediaries workshop at Open Knowledge Festival, Berlin 2014. Photo by **Open Data Research Network**. CC-BY-2.0.

full, but rather derived datasets or aggregate statistics should be released. Aggregation helps prevent individuals being singled out and discriminated against through the data.

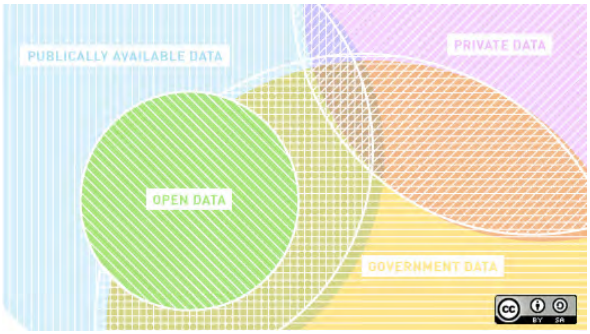
However, in practice true anonymization is becoming harder to achieve as the number of datasets that can be cross-referenced grows.[4] At the same time, efforts at anonymization and aggregation may lead to small groups being omitted from the data that gets placed into the public domain, making them invisible in policy discussions. For example, a small number of people with a rare but serious medical condition in a local area may simply disappear when the data is "bucketed" in order to have big enough aggregate groups for it to be suitable for release.

A deeper debate about semi-open forms of data-sharing is needed to ensure privacy can be protected, while public access to data for scrutiny and more participatory policy-making can be expanded.[5]

Setting Standard Categories

Third, many of the datasets being "opened" are, in practice, new datasets. How they are designed has important consequences. These datasets are being constructed based on new data standards in the process of being made available as open data. Many government open data policies have matured from talking of "raw data now," to developing long-term plans to build new "national data infrastructures."[6]

Standards determining the categories used in a dataset affect what it is possible to know from that



"What Open Data Means and What It Doesn't." Image by OpenSource.com.

data in the future, and how easy it will be to use the data in different ways. Right now, many governments are focusing on commercial re-use of data, and so are interacting mostly with industry partners as they develop new data standards. Civil society involvement in shaping these new data architectures of the data is essential to ensure they are inclusive and sensitive to social issues.

Carefully designed standards can support decentralized decision making and action, yet often standards lead us in the other direction, towards more centralized systems, where "edge-cases" and minority needs are left out. We need to do more to understand the implications of the standards currently being built. Additional critical attention is also needed when it comes to the introduction of new flows of private data into policy making (for example, states are experimenting with use of large-scale sensor or social media data).

If data or the algorithms used to analyze it cannot be effectively opened to widespread public scrutiny then we need to ask whether the data should really be used to set or implement laws?

Bringing Greater Attention to the Architecture of Dataset-State

Moves to make government data open-by-default are one element in the contemporary re-architecting of the dataset-state. Whether these new architectures will ultimately support more inclusive public policy, or end up enabling deliberate or unintended discrimination in policy making and implementation is a question in need of much more attention than it currently receives.

Index

1. Monika, Bahur, Marcia Grimes, and Niklas Harring, "Seeing the State: The Implications of Transparency for Societal Accountability," *QoG Working Paper Series* (2010): 15; James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press, 1999), 464; Tom Slee, "Seeing Like a Geek," *Crooked Timber* (2012): http://crookedtimber.org/2012/06/25/seeing-like-a-geek/.
2. Jo Bates, "The Domestication of Open Government Data Advocacy in the United Kingdom: A Neo-Gramscian Analysis," *Policy and Internet* 5, no. 1 (2013): 118–137.
3. William Perrin, "Good Governance, The Accountability Stack and Multi-Lateral For a," *Indigo Trust*. (2012): http://indigotrust.org.uk/2012/11/12/good-governance-the-accountability-stack-and-multi-lateral-fora/; Timothy Davies, *Open Data Barometer: 2013 Global Report* (London: World Wide Web Foundation, 2013).
4. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 (2010): 1701-1777, http://uclalawreview.org/pdf/57-6-3.pdf.
5. Teresa Scassa, "Privacy and Open Government," *Future Internet* 6, no. 2 (2014): 397–413, DOI:10.3390/fi6020397
6. Timothy G. Davies, "Open Data Policies and Practice: An International Comparison," *SSRN* (2014): DOI:10.2139/ssrn.2492520.

OCTOBER 2014

(Un)Ethical Use of Smart Meter Data?

JENIFER SUNRISE WINTER
ASSOCIATE PROFESSOR, SCHOOL OF COMMUNICATIONS, UNIVERSITY OF HAWAI'I AT MANOA

A MEASURED APPROACH

Smart Meters: The Internet in the Built Environment

We typically think of the Internet as something virtual that we deliberately access via our computers, tablets, and smartphones. In reality, the everyday world around us is becoming part of the Internet, often without us realizing it.

A good example of this is the smart grid, the next-generation electrical power grid intended to upgrade and replace aging infrastructure, enhance energy conservation, and provide real-time information for both customers and utility decision making. Smart meters, a component of the smart grid, are energy meters installed at residences that can capture a constant stream of data about your home's energy use. This data is stored and analyzed by the electric company to identify energy usage patterns, and you may also be able to get feedback in real-time. In the United States, the *American Recovery and Reinvestment Act* of 2009 funded more than $3.4 billion in grants for smart grid development, and by July, 2013, nearly 40 percent of households in the United States were equipped with a smart meter.[1]

Moral Metering

At first, it might seem that the collection of data about our energy use is not too worrisome, especially when there is the possibility of meaningful benefits, such as lessening our reliance on oil or lowering the cost of energy use.

However, the introduction of residential smart meters poses a number of ethical challenges related to security, privacy, and "ensuring social justice both in terms of access and cost of electric power service."[2]

The Devil Is in the Detail

First, the amount and level of detail of the data collected will greatly increase. Each appliance in our homes gives off a unique signature based on its energy use, and even the specific television programs or movies we watch can be deduced.[3] Manufacturers are also increasingly introducing "smart appliances" with features such as remote control apps for smartphones, which can interface with smart meters and control them (e.g., turn off certain appliances during peak energy-use periods).[4]

Absent appropriate security and privacy policies, our data may potentially be transferred or sold (willfully or not), and they may be combined with other data about us.

Smart meter hacking is another well-documented issue, and there is potential for bad actors to spoof energy usage or conduct surveillance for the purpose of committing crimes.

Smart meter. Photo by Ellin Beltz.

For example, security researchers hacking smart meters were able to determine how many personal computers or televisions were in a home, as well as what media were being consumed.[5]

Citizens' Expectations

In my interviews with citizens about how they expect data collected from smart meters to be used, participants have expressed concern about unauthorized use and sharing of personal data. One citizen noted that, "Ideally, I hope there are constraints on the sharing of this information, that there is this wall of consent that you have to go through, even though it's annoying… but who knows? It's so hard to anticipate how information will move, because there are ways it can be leaked." Another concern was the blurring distinction between our homes and public space: "Honestly, I don't personally feel that I am doing anything, like, unethical or illegal in my home, but I know there are people that feel that what they do in their own home should not be information that should be available to people outside the home."

Some citizens were also concerned about the possibility of inferences made from smart meter data, such as medical information or political views that could be used to discriminate in an unjust manner. As one participant noted, "[T]he energy use itself would not be troublesome, but perhaps it could give clues to the types of devices that people have in their homes. So, for example, if you have a certain health problem, and a certain device is used in the home is used to help you, then companies could access or make assumptions or inferences into the types of health problems you have."

A residential electricity meter. Photo by Dwight Burdette. CC-BY-3.0.

Even where data are stripped of personally identifiable information to protect your identity, inferences based on other data could pinpoint you and leave you at risk for harm. *The problem is not that these technologies exist—as most participants welcomed any potential way to improve energy efficiency, security, or cost savings.* However, as one participant explained, "[R]ight now, for most people, they are looking at the consumer side of it. They are *very* excited about the possibilities of electronics being more responsive and alert, and so I think that part of it is great. But I think in the long term, eventually, we have to think about how is energy data being used? What inferences can people make from it? What companies will be collecting data. That's also equally important."

A More Measured Approach

The problem is that citizens are not fully informed about related risks and that most are not yet a part of the discussion about what personal data is collected, how it is used, and who has access to it.

How can we reap the many benefits of technologies like the smart grid/smart meters without risking a loss of personal privacy, loss of a job or housing, or government intrusion into one's home life?

Transparency is a necessary first step. We need to have more awareness about what data are being collected and have a say about whether they will be shared beyond their original context. We have a right to take part in the discussion about what personal information is actually needed to provide meaningful improvements to our lives, and to set boundaries when we believe the collection poses no larger individual or community benefit.

The development of smart grid technology should take citizens' privacy concerns into account from the very start through techniques like Privacy by Design.[6] Citizens should not be forced to choose between privacy and energy conservation (or privacy and cost savings). Designed with privacy at their core, the smart grid can enhance our lives while simultaneously protecting our data.

Index

1. Innovation Electricity Efficiency Institute. *Utility-Scale Smart Meter Deployments: A Foundation for Expanded Grid Benefits*. Washington, D.C.: Innovation Electricity Efficiency Institute, 2013.

2. Kostyk Timothy, and Joseph Herkert. "Computing Ethics: Societal Implications of the Emerging Smart Grid." *Communications of the ACM* 55(11) (2012): 34-36.

3. Mills, Elinor. "Researchers Find Smart Meters Could Reveal Favorite TV Shows." *CNET* (January 24, 2012), http://www.cnet.com/news/researchers-find-smart-meters-could-reveal-favorite-tv-shows/.

4. McDaniel, Patrick, and Sean, W. McLaughlin, Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy* 7(3) (2009): 75-77.

5. Brinkhaus, Stephen, Dario Carluccio, Ulrich Greveler, Benjamin Justus, Dennis Löhr, and Christoph Wegener. "Smart Hacking for Privacy." Presentation to the 28th Chaos Communication Congress (2011), http://events.ccc.de/congress/2011/Fahrplan/events/4754.en.html.

6. See http://www.privacybydesign.ca/.

OCTOBER 2014

Spammers, Scammers, and Trolls: Political Bot Manipulation

SAMUEL WOOLLEY
PHD CANDIDATE, DEPARTMENT OF COMMUNICATION, UNIVERSITY OF WASHINGTON, SEATTLE

DATA-DRIVEN DECEIT

Social bots, bits of code that generate content and mimic real social media users, are nothing new. Since the launch of Friendster and MySpace, social networking platforms have regularly featured fake accounts. Savvy programmers, spammers, and promoters use these automated profiles to generate clicks ("like" stuff and sell stuff), pad follower lists (fake popularity), and collect information (sort, borrow, and steal data). According to news reports, Facebook has more than 83 million illegitimate accounts, and Twitter—approximately 20 million.[12]

Loops of Manipulation and Misdirection

What *is* relatively new and on the rise is the cunning use of social bots by politicians, astroturf activists, and ideological extremists.[345] These "political" bots and the messages they produce represent a new form of discriminatory computational propaganda.[6] Via targeted spamming and other tactics, political bots drown out oppositional voices, demobilize activists, and promote the status quo.

For example, in South Korea, public servants in the cyber warfare unit of the Defense Ministry used bots to propagate messages in favor of President Park Geun-hye and Saenuri Party, including some which attacked political rivals. Though discerning the precise impact of these messages is difficult, their occurrence has heightened concern throughout the country: President Park won the election by a margin of a million votes.[7] In Syria, intelligence officials have also used bot followers to both bolster government credibility and stymie opposition within a context of civil unrest.[8] Meanwhile, the militant group, Islamic State of Iraq and Syria (ISIS), uses bots to trick Twitter, giving the world the impression of having a large following on social media, when in fact it "ghost-Tweets" its messages.[9] Because messages come from otherwise ordinary functioning, legitimate Twitter accounts, Twitter filters aimed at curbing socially mediated hate speech fail to detect these examples of bot messaging.

Political bots have the capacity to produce an unending loop of manipulation and misdirection. Any political group can buy and deploy a bot as easily as an individual zealot: as a recent *New York Times* article put it, friends and influence are cheap and for sale online.[10] New developments in social bot technology allow fake accounts to operate in complex, multifaceted, ways. These pieces of software not only search for and collect data from social media sites—by scraping sites for individual and group identifiers—they also use this data on such sites to manipulate, censor, and isolate specific populations.

As a result, political bots are able to impact online identity building by blurring the line

In the last three years, social bots have become a driving force for political manipulation and data-driven deceit on social media sites. "Help from Mr Handyman." Photo by Christopher Isherwood.

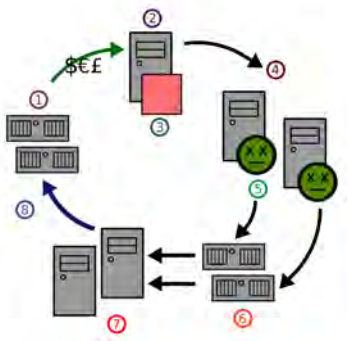
between fake and real users. How might young people, for instance, be affected by political messaging from friendly and real-seeming bot accounts?

The online popularity and influence of politicians is also tainted by the presence of bots. A recent *Politico* piece reported that bots have "infiltrated nearly every politically linked account from the White House to Congress to the 2016 campaign trail."[11]

Finally, aspects of peoples' ability to make cross-cultural connections via social media are also at stake. What happens when a religious or cultural group is drowned out by a bot-led barrage of hateful messages that seem to come from other, oppositional groups?

Activists vs. Bots

While few responses to bot-generated social media attacks exist, some innovators are beginning to experiment with alternate uses of bot technologies in a political context. A technologist at the Electronic Frontier Foundation created Block Together, which allows users to collect and share lists of blocked users with their social networks, including bots that pollute social media feeds.[12] "Watchdog" bots help with transparency efforts by monitoring Wikipedia edits coming from government I.P. addresses.[13] An anti-abortion bot gained international attention when Internet users turned its own design against it, forcing it to tweet Rick Astley lyrics (instead of anti-abortion



"Circle of spam." (1) Spammer's web site (2) Spammer (3) Spamware (4) Infected computers (5) Virus or trojan (6) Mail servers (7) Users (8) Web traffic. Diagram of sending spam e-mails. Photo by odder.

messages).[14] Trolling-the-trollers may become a way to promote social causes or combat automated political manipulation.

Looking Forward

The type of computational propaganda wrought by bots represents one of the most significant developments in social media. Bot software will continue to evolve, and the presence of artificial intelligence on social media platforms will grow. Because of this, it is essential to build understanding of how governments use and interact with security firms and hackers who program and deploy bots for political use. The opinions of these bot builders, and of those who track and disable bots, will be crucial to combating new types of data-driven discrimination.

Index

1. "Facebook has more than 83 million illegitimate accounts," *BBC News* (August 2, 2012): http://www.bbc.com/news/technology-19093078; Keith Wagstaff, "1 in 10 Twitter Accounts is Fake, Says Researchers," *NBC News* (November 25, 2013): http://www.nbcnews.com/tech/internet/1-10-twitter-accounts-fake-say-researchers-f2D11655362.
2. Emma Woollacott, "Why Fake Twitter Accounts are a Political Problem," *New Statesman* (May 28, 2014): http://www.newstatesman.com/sci-tech/2014/05/why-fake-twitter-accounts-are-political-problem; Rachael Levy, "ISIS Tries to Outwit Social Networks," *Vocativ* (June 17, 2014): http://www.vocativ.com/world/syria-world/isis-tries-outwit-social-networks/; David Zax, "Truthy Sleuths Track Twitter 'Turfers," *Fast Company* (October 26, 2010): http://www.fastcompany.com/1697973/truthy-sleuths-track-twitter-turfers.
3. Samuel Woolley and Philip N. Howard, "Social Media, Revolution, and the Rise of the Political Bot," In *Routledge Handbook of Media, Conflict, and Security* (New York: NY, forthcoming).
4. Choe Sang-Hun, "South Korean Officials Accused of Political Meddling," *New York Times* (December 19, 2013): http://www.nytimes.com/2013/12/20/world/asia/south-korean-cyberwarfare-unit-accused-of-political-meddling.html.
5. Norah Abokhodair, "Discovering the Twitter botnet," *Medium* (October 23, 2013): http://norahak.wordpress.com/2013/10/23/discovering-the-twitter-botnet/.
6. J.M. Berger, "How ISIS games Twitter," *The Atlantic* (June 16, 2014): http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.
7. Ian Urbina, "I Flirt, I Tweet. Follow Me at #Socialbot," *New York Times* (August 10, 2013): http://www.nytimes.com/2013/08/11/sunday-review/i-flirt-and-tweet-follow-me-at-socialbot.html?_r=0.
8. Darren Samuelsohn, "Pols Have a #fakefollower Problem," *Politico* (June 11, 2014): http://www.politico.com/story/2014/06/twitter-politicians-107672.html.
9. Amanda Hess, "Twitter Won't Stop Harassment on Its Platform, So Its Users Are Stepping In," *Slate* (August 6, 2014): http://www.slate.com/blogs/future_tense/2014/08/06/twitter_harassment_user_created_apps_block_together_flaminga_and_the_block.html.
10. Patrick Macguire, "A New Twitterbot is Tracking Canadian Government's Wikipedia Edits," *Vice* (July 14, 2014): http://www.vice.com/en_ca/read/a-new-twitterbot-is-tracking-the-canadian-governments-wikipedia-edits.
11. Rebecca Rose, "Anti-Abortion Twitter Bot Trolled to Death," *Jezebel* (September 24, 2014): http://jezebel.com/anti-abortion-twitter-bot-trolled-to-death-1638910841.

Part 3: Fairness, Equity, Impact

OCTOBER 2014

Big Data and Human Rights

VIRGINIA EUBANKS
NEW AMERICA FELLOW; ASSOCIATE PROFESSOR OF WOMEN'S, GENDER AND SEXUALITY STUDIES, UNIVERSITY AT ALBANY, SUNY

AUTOMATING CONTROL

Big Data & Social Policies for the Poor

Big data seems new and sexy, so we ignore its past and concentrate on its most recent manifestations: the collection of online commerce data, government monitoring of cell phones and email. But the use of large electronic data sets to track, control and discipline U.S. citizens has a long history, going back at least thirty years.

Databasing efforts responded to new technologies that could streamline government process, of course, but also to social movements' successes highlighting corruption and bias in public programs. The National Criminal Information Center (NCIC) and New York's Welfare Management System (WMS), for example, were designed in 1967 and 1971, respectively, at the height of efforts by the civil rights and women's movements to expose discrimination in law enforcement and public assistance.

High-profile corruption and government surveillance scandals—the Frank Serpico case, COINTELPRO and the Church Commission—exposed systemic police and intelligence community abuses that horrified the nation. New groups, many of them women of color, were suing for—and winning—equal access to public assistance, an end to discriminatory and arbitrary rules, and the right to retain benefits when engaged in fair hearings.[1]

The Rise of Technologies of State

New digital technologies were integrated into public services under the banner of making policy more fair, transparent and efficient. However, by the early 1970s, a worsening recession threatened efforts to end discriminatory practices in law enforcement and welfare. More people became eligible for programs that enjoyed less public support. Tough economic times resulted in what was widely reported as an "urban crime wave," bolstering support for law-and-order tactics.

Caught between increasingly stringent equal protection and due process rules and community backlash against spending, elected officials and state bureaucrats performed a political sleight-of-hand. They commissioned expansive technologies that *supplanted*, rather than supporting, the decision-making of frontline public service workers. Automated processes and algorithms increasingly replaced the discretion of welfare caseworkers, police officers, and public school teachers. While this solution curtailed the worst of discriminatory treatment by individual public servants, stereotypes about the meaning and the targets of public programs were built in to the original code of these systems, leaving a structural legacy of racism, classism, and sexism.

Design documents from the New York State archives show that an explicit goal of the WMS, for example, was to curtail the growth of welfare programs. The system was built to "reduce unauthorized or excessive payments," strengthen penalties against welfare recipients, "look over the shoulder of caseworkers," and provide increased state oversight of local social service offices.

A 2009 CompStat meeting in Los Angeles. Photo by Eric Richardson. CC-BY-NC-SA.

These "social specs" for public service technology were based on time-worn, race- and class-motivated assumptions about welfare recipients: they are lazy and must be "prodded" into contributing to their own support, they are prone to fraud, and they are a burden to society unless repeatedly discouraged from claiming their entitlements. Designers also drew on stereotypes about public employees: that they lack motivation to do their jobs well, are generally incompetent, and need oversight to limit their discretion.

Computerized Decision-Making

Early databases developed into the intelligent decision-making systems in public services today: NCIC begat CompStat which begat predictive policing and fusion centers; WMS was the first step towards the automated eligibility systems we've seen in Indiana and elsewhere.[2]

Digital systems are primary decision-makers in public policy.

These early big data systems were built on a specific understanding of what constitutes discrimination: personal bias. Discrimination can only be individual and intentional, a caseworker applying welfare eligibility rules more strictly to African American mothers, a police officer finding white citizens somehow less suspicious. By contrast, computers judge "fairly," applying rules to each case consistently and without prejudice.

According to legal scholar Danielle Keats Citron, digital systems today go beyond applying procedural rules to individual cases; instead, these systems *are primary decision-makers in public policy*.[3] A computer system can terminate your food stamps, exclude you from air travel, purge

Paper is an increasingly rare site at the front desk of the nation's public assistance offices. In some states, eligibility determinations are automated and are managed by call centers, not caseworkers. "Welfare Office." Photo by Jacob Norland. CC-BY-2.0.

you from the voter rolls, or decide if you are likely to commit a crime in the future. This presents significant challenges to due process, procedural safeguards of administrative law, and equal protection assurances. How can you prove a discrimination case against a computer? Can due process be violated if an automated decision-making system is simply running code?

Solutions

The "social specs" that underlie our decision-systems and data sifting algorithms might be called *legacy system prejudice*. Uncovering and reprogramming them is a key challenge to creating fair data policy.

So is evening out power relationships around access and control of information. Participatory approaches to public service IT design may result in more effective decision-making, better matching of resources to needs, more timely feedback, and improved relationships between recipients, workers, and government.

For example, in most social service offices, computer displays and case data are only visible to workers, not recipients. By simply adding a second monitor showing recipients real-time case information, eligibility determinations, and available resources, public service programs could equalize casework relationships, provide more appropriate support, and increase recipients' self-determination.

Legacy system prejudice is a key challenge to fair data policy.

Co-designed digital systems can lead to outcomes that are both more effective and more just. The self-sufficiency calculator for New York City, designed by the Women's Center for Education and Career Advancement with their partners and clients, helps adults get the support and resources they need to stay in the workforce—and with a live person on hand to assist individuals in sharing and evaluation of financial needs.[4] Notably, the calculator is programmed to make sure that individuals receive the maximum entitlement they are allowed by law—not to construct roadblocks that weed out all but the most desperate.

It may be impossible to root legacy prejudice completely out of our existing big data systems. However, shifting public service IT design processes away from expert-based, top-down models to more participatory approaches and challenging assumptions about public service recipients and employees will go a long way to achieving more just outcomes.

Index

1. For more information on the welfare rights movement's challenges to discrimination in the public service system, see Frances Fox Piven and Richard A. Cloward, *Poor People's Movements: Why They Succeed, How They Fail* (New York: Vintage Books, 1979). For more on the Church Commission, see the report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans*, 94th Cong., 2nd sess., 1975.
2. For more on the Indiana welfare eligibility automation, see Colin Wood, "Nobody Wins in Indiana vs. IBM Lawsuit, Judge Says," *Government Technology*, July 19, 2012: http://www.govtech.com/health/Nobody-Wins-in-Indiana-vs-IBM-Lawsuit-Judge-Says.html.
3. Danielle Keats Citron, "Technological Due Process," *Washington University Law Review* 85 (2007): 1249-1313.
4. The self-sufficiency calculator can be found at http://www.wceca.org/self_sufficiency.php.

OCTOBER 2014

The Networked Nature of Algorithmic Discrimination

DANAH BOYD
PRINCIPAL RESEARCHER, MICROSOFT RESEARCH; FOUNDER, DATA & SOCIETY RESEARCH INSTITUTE

KAREN LEVY
POSTDOCTORAL ASSOCIATE, INFORMATION LAW INSTITUTE, NEW YORK UNIVERSITY; FELLOW, DATA & SOCIETY RESEARCH INSTITUTE

ALICE MARWICK
ASSISTANT PROFESSOR, FORDHAM UNIVERSITY; DIRECTOR, MCGANNON INSTITUTE FOR COMMUNICATION RESEARCH

YOUR POSITION IN THE NETWORK MATTERS

It's Who You Know

We live in a highly networked world, in which our social connections can operate as both help and hindrance. For some people, "who you know" is the key to getting jobs, or dates, or access to resources; for others, social and familial connections mean contending with excessive surveillance, prejudice, and "guilt by association."

Along with information about who you *know*, technical mechanisms that underlie the "big data" phenomenon—like predictive analytics and recommendation systems—make imputations about who you *are like*, based on your practices and preferences. If two people like Zydeco music and rare birds, they might be more likely to purchase the same products. Similarly, you are more likely to share tastes with your friends than with a random stranger. Marketers can gain tremendous insight from this information. But while this may be useful to find customers or limit the financial risk of insurers, these same mechanisms, left unchecked, can lead to discriminatory practices.

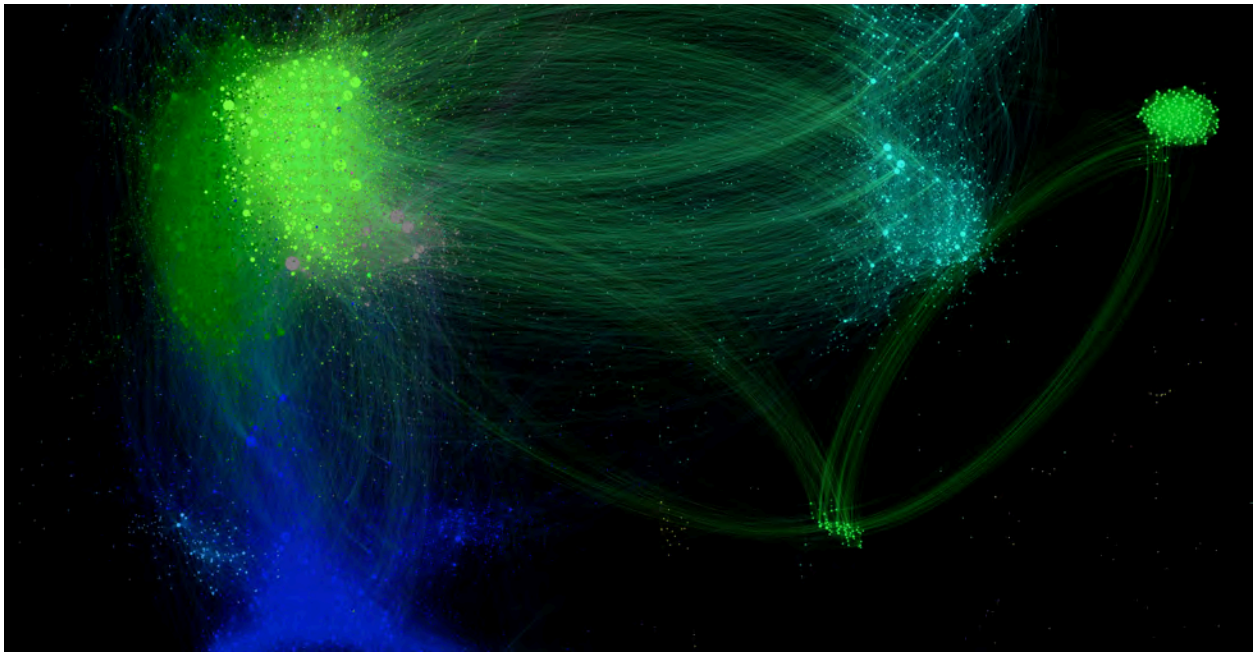
Across the board, we must recognize that we have very little control over how information about us is gathered and used, and that the networked nature of modern life can lead to very different outcomes for different groups of people—despite our aspirations to equal opportunity.

Discrimination by Network?

In the United States, most companies are required to be equal opportunity employers; discrimination on the basis of race, sex, creed, religion, color, and national origin is prohibited. Additional regulations forbid many employers from discriminating based on age, disabilities, genetic information, military history, and sexual orientation. However, there is nothing stopping an employer from discriminating on the basis of personal network. Increasingly, algorithmic means of decision-making provide new mechanisms through which this may occur.

There is nothing stopping an employer from discriminating on the basis of personal network.

The social network site LinkedIn is useful for both employers and employees. The latter often use the site to create a public résumé. In doing so, they don't just list their previous work experience, but they also identify who they know and solicit endorsements from these connections. Employers use LinkedIn and other social network sites to determine "cultural fit," including whether or not a candidate knows people already known to the company. This process rewards individuals on the basis of their networks, leading companies to hire people who are more likely to "fit the profile" of



People's networks reveal a lot about who they are through whom they know. The structure of a social network graph may appear innocuous, but these networks are often shaped by race, class, ethnicity, religion, gender, and other protected categories. Networks can easily be discerned from social media. Visualization by Gilad Lotan. CC-BY-SA.

their existing employees—to the detriment of people who have historically been excluded from employment opportunities. While hiring on the basis of personal connection is by no means new, it takes on new significance when it becomes automated and occurs at large scale.

What's at stake in employment goes beyond the public articulation of personal contacts. While LinkedIn is a common tool for recruiting and reviewing potential professional employees, fewer companies using it for hiring manual or service labor. For companies who receive thousands of applicants per opening—especially those who are hiring minimum wage or low-skill labor—manually sorting through applications is extremely time consuming. As a result, applicant tracking and screening software is increasingly used to filter candidates computationally, especially at large enterprises. Don't have the right degree? Rather than getting a second glance because of your experience, you're automatically screened out. Didn't use the right buzzword in your list of skills? Your application will never surface. This creates a new challenge for potential applicants who must learn to game the opaque algorithms that they encounter before a person actually takes a glance at them. Such knowledge is often shared within personal networks, so much so that if you're not properly connected, you might not even know how to play the game. While such systems create ethical dilemmas, it is unclear who should be accountable for the potential discrimination such systems exacerbate.

Applying for a job is increasingly mediated by technology, both explicitly and implicitly. Photo by Richard. CC-BY-SA 2.0.

Solutions

Discussions around privacy and fairness in a data-centric world typically rest on the notion of individual control over information, but our networks reveal a great deal. While American law and much of society may focus on the individual, our identities are entwined with those of others. Algorithms that identify our networks, or predict our behavior based on them, pose new possibilities for discrimination and inequitable treatment.

Networks are at the base of data analytics, yet our social and legal models focus on the individual.

Networks are at the base of how contemporary data analytics work. Yet, our social and legal models focus on individual control over information, individual rights, and individual harm. Discrimination law can no longer be solely regarded as guaranteeing rights for an individual member of a protected class. The notion of a protected class remains a fundamental legal concept, but as individuals increasingly face technologically mediated discrimination based on their positions within networks, it may be incomplete.

In the most visible examples of networked discrimination, it is easy to see inequities along the lines of race and class because these are often proxies for networked position. As a result, we see outcomes that disproportionately affect already marginalized people. And, yet, as these systems get more sophisticated, it becomes increasingly hard to understand what factors are inputted or inferred in complex algorithms that seek to distribute limited resources. This is not simply a matter of transparency; many of those who design or use these systems have little understanding of how algorithmic decisions are made based on the millions of points of data fed into the system.

We must rethink our models of discrimination and our mechanisms of accountability. No longer can we just concern ourselves with immutable characteristics of individuals; we must also attend to the algorithmically produced position of an individual, which, if not acknowledged, will be used to reify contemporary inequities. Racism, sexism, and other forms of bigotry and prejudice are still pervasive in contemporary society, but new technologies have a tendency to obscure the ways in which societal biases are baked into algorithmic decision-making. Not only must such practices be made legible, but we must also develop legal, social, and ethical models that intentionally account for networks, not just groups and individuals.

Index

1. Barocas, Solon, and Andrew D. Selbst. "Big Data's Disparate Impact." Paper presented at *Privacy Law Scholar's Conference,* June 5, 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.
2. Citron, Danielle, and Frank Pasquale. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review* 89(1), 2014.
3. Levy, Karen, and danah boyd. "Networked Rights and Networked Harms." Paper presented at International Communication Association's *Data & Discrimination Preconference*, May 14, 2014. http://www.datasociety.net/initiatives/privacy-and-harm-in-a-networked-society/.
4. Marwick, Alice, and danah boyd. "Networked Privacy: How Teenagers Negotiate Context in Social Media." *New Media & Society*, In press. DOI: 10.1177/1461444814543995.
5. Rosenblat, Alex , Kneese, Tamara, and danah boyd. "Networked Employment Discrimination." *Data & Society Working Papers*, 2014. http://www.datasociety.net/initiatives/future-of-labor/.

Acknowledgments

We would like to thank Alex Rosenblat and Tamara Kneese for their helpful insights as we embarked on this project. We would also like to acknowledge the feedback that we have received from participants at different events, including: "The Social, Cultural, & Ethical Dimensions of 'Big Data,'" the Privacy Law Scholars Conference, and the International Communication Association's Data & Discrimination Preconference.

OCTOBER 2014

Putting Data to Work

SOLON BAROCAS
POSTDOCTORAL RESEARCH ASSOCIATE, CENTER FOR INFORMATION TECHNOLOGY POLICY,
PRINCETON UNIVERSITY

PUTTING DATA TO WORK

Working the Data

Big data promises a future of fairer hiring decisions, a future in which an applicant's prospects no longer turn primarily on the reputation of her alma mater. Empowered by so-called "workforce analytics," companies will instead tap new sources of data that capture qualities that are demonstrably more predictive of job performance and more proximate to the skills demanded of the job.[1]

The New York Times, for example, describes how the tech start-up Gild seeks out talented programmers whose lack of traditional credentials might render them invisible or inscrutable to employers. Gild instead looks to the popularity of users' code on GitHub, which the company views as a far stronger sign of skill, evident in other developers choosing to reuse the code.[2]

This recruitment strategy and others like it have been rightly embraced as a way to overcome some of the structural impediments to finding capable job candidates in historically disadvantaged populations—candidates who have fewer opportunities to obtain the traditional training that others commonly highlight when applying for jobs.

The White House has even endorsed this approach, heralding companies that perform similar kinds of analyses as important new actors in the fight against prejudice and bias in hiring.[3] And if these new predictors of talent are widely adopted, the reasoning goes, a more diverse workplace will naturally follow.

A Particular Kind of Problem-Solving

There are good reasons to welcome these developments, but consider, for a moment, the specific problem that data are helping to solve in this case—and the problems that they are not.

Hiring managers adopt these tools to improve the process of searching for and sorting between job candidates. As a recent story in the BBC explains, "[a]nalysis of historic data from tens of millions of job applicants, successful or otherwise, is helping employers predict which new candidates are likely to be the best based on a comparison with the career paths, personalities and qualifications of previously successful employees."[4] This entire approach to hiring assumes that future job performance depends exclusively on the qualities of the applicant. Taken as both unproblematic and unchangeable are the institutional policies or norms that affect who is more likely to excel at a

Workforce analytics have tended to focus entirely on one side of the equation, offering a plethora of new techniques to assess workers and far fewer tools to evaluate the effects of workplace policy.

Workforce analytics have tended to seek out model employees rather than model workplaces. Photo by Chris Salt. CC-BY-NC-SA 2.0.

job or pass through the ranks.

There is an important alternative explanation for any finding that suggests that people with certain characteristics are less likely to be effective on the job: that the conditions of the workplace are less conducive to their flourishing.

Assessing the Role of the Workplace

Workforce analytics have tended to focus entirely on one side of the equation, offering a plethora of new techniques to assess workers and far fewer tools to evaluate the effects of workplace policy. Indeed, most applications of data mining reduce human resource decisions to a matter of arriving at the right choice of candidate, and accept as a given the conditions that contribute to uneven rates of success among different parts of the workforce.

Consider what this might mean for groups that have been—and remain—subject to discrimination. For women, data mining could have the perverse effect of legitimating or obfuscating the formal policies and subtle dynamics that account for differences in their career paths or perceived success in the workplace.

With some thought, however, data could illuminate areas of corporate practice that keep women from being as prosperous as their male colleagues.

Working Out the Cause of the Problem

Though such uses of data are relatively rare, there are some instructive examples. Google, for instance, noticed that the company failed to promote its female employees at the same rate as

Data can illuminate the dynamics that keep historically oppressed and disadvantaged populations from finding as much success on the job as their peers. Photo by Eric Constantineau. CC BY-NC 2.0.

men who received similar evaluations, suggesting that women faced some artificial barriers to advancement.[5] Social scientists have documented similar disparities in many other areas of employment and have offered many explanations ranging from outright prejudice to implicit bias to far more subtle organizational and structural factors.[6]

In this instance, however, Google was able to probe its data further, test hypothesized explanations, and tease out the primary mechanism at work. The company's unusual approach to promotion, in which employees have to self-nominate, seemed to play an important role. For a whole host of reasons, women had been less likely to put themselves up for consideration. Google was able to adjust its strategy to compensate for these dynamics and to bring promotion rates among women and men closer to parity.

Much More Work to Do

Data has many potential roles to play in advancing the interests of the historically oppressed and disadvantaged. Purging prejudice and implicit bias from the up-front sorting of job applicants is an important goal, however unrealizable.[7] But far more work needs to be done that leverages data to both expose and address the institutional and structural conditions that continue to unfairly shape the career paths and prospects of many members of society. Data can and should reveal opportunities to adjust workplace policy and practice that give equally capable employees an equal chance at success.

Index

1. Don Peck, "They're Watching You at Work," *The Atlantic*, November 20, 2013, http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.
2. Matt Richter, "How Big Data Is Playing Recruiter for Specialized Workers," *New York Times*, April 27, 2013, http://www.nytimes.com/2013/04/28/technology/how-big-data-is-playing-recruiter-for-specialized-workers.html.
3. United States White House, *Ready to Work: Job-Driven Training and American Opportunity*, July 2014, http://www.whitehouse.gov/sites/default/files/docs/skills_report.pdf.
4. Matthew Wall, "Does Job Success Depend on Data Rather than Your CV?" *BBC*, October 1, 2014, http://www.bbc.com/news/business-29343425.
5. Cecilia Kang, "Google Data-mines Its Approach to Promoting Women," *Washington Post*, April 2, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/02/google-data-mines-its-women-problem/.
6. Devah Pager and Hana Shepherd, "The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets," *Annual Review of Sociology* 34 (August 2008): 181–209.
7. Solon Barocas and Andrew Selbst, "Big Data's Disparate Impact," September 14, 2014, http://ssrn.com/abstract=2477899.