**Award
Lecture**

**Surveillance and the Formation of Public
Policy**

Oscar H. Gandy, Jr.

Emeritus Professor of Communication
University of Pennsylvania, US
oscar.gandy@asc.upenn.edu

SSN Outstanding Achievement Award 2016 *Surveillance & Society Biennial Conference, Barcelona.*

This article is based on a keynote speech delivered at the Surveillance Studies Network / Surveillance & Society Conference in Barcelona, April 22nd, and a public lecture delivered at The London School of Economics and Political Science, May 19th, 2016.

Introduction

There is little doubt that we are in a moment of great change, a transition to an altered state of being, one that will be noted by historians, or whatever we will call those beings or entities that have been assigned the responsibility for looking back on the past in order to “make sense” of important shifts in the relationships between us and our environments.

There will be history, and it will be reflected in a host of “records,” that I am confident will include commentary on the social, economic, and cultural transformations brought about by modifications in the systems, norms and patterns of communication enabled by the global network once referred to as “The Internet” (Chadwick 2006).

Among the transformations that will be seen as important, by whatever comparative measures will be in fashion at that time, those that we associate with politics and the public sphere (White 1988) will have undoubtedly claimed positions up near the top. Although what we currently refer to as surveillance, will undoubtedly be known by some other term by then, the role played by the capture, analysis and application of insights derived from communications about politics and the formation of public policies will feature centrally in the evaluative assessments of decisions taken at key moments in those histories of the present and near future.

I am hopeful that I, and others who share my concerns about the kinds of decisions being made with regard to participation in a political process, will actually succeed in bringing about an alteration in our

movement along a path that is currently leading us away from meaningful deliberative engagement in the democratic process (Gutmann and Thompson 2004), and toward rapid polarization, exclusion or withdrawal.

This article will attempt to identify some of the problems, key actors, institutions and technological resources that are bringing about the current transformation of what we mean by public participation in governance. While it will emphasize the role being played by surveillance and analytics, it will also explore the different locales or sites in which the impact of these strategies and tactics will be greater than many of us expect. Finally, it will introduce for consideration a number of proposals, some of which are merely emergent, rather than demonstrably reliable oppositional strategies for limiting the impact of this anti-democratic, socio-technical wavefront on the horizon.

Background

Surveillance within the political environment is not a new phenomenon, it has merely been transformed to a great extent in response to changes in communication technology and social practice, especially those related to marketing and the manipulation of consumer consciousness (Andrejevic 2007: 187-211).

It is also true, however, that politics had already been transformed by earlier efforts to recast the democratic public sphere (Gardner 2011; Garnham 1990; Habermas 1998; White 1988) into a marketplace, often characterized as a “marketplace of ideas” (Peters 2004) where the emphasis on communication and information policy is on the status of individuals as consumers, rather than citizens (Dawes 2014).

It was generally understood that this new political marketplace would be subject to the same logics, techniques, and maldistributed resources that seemed to matter in those other kinds of markets (Dean 2009). It doesn’t take much work to see the parallels between marketing of commercial products and services, and the marketing of political candidates or policy options. There are almost no meaningful differences between the forms of communication used in support of these different marketing goals (Fuchs 2015).

Even though Ryan Calo’s comprehensive assessment (2014) of the nature of what he refers to as “digital market manipulation” was concerned primarily with consumer protection in the market for goods and services, I feel that many, if not most of the same concerns apply to a marketized public sphere. What Calo and others are suggesting is that communication within the marketplace, whether it has been designed to support the management of demand for commercial goods and services, or whether its focus is on political candidates or public policies, has been designed to have the maximum persuasive impact on the members of targeted population segments.

Where the purposes or goals of manipulative communications within traditional commercial markets relate primarily to the production of influence over consumer decisions related to purchases or investments, the goals are somewhat more varied within the public policy arena. Whereas the favored behavioral option for the targeted consumer is an affirmative choice, or purchase, a much greater range of responses may be seen as desirable for particular sorts of political actors. Timely expressions of opposition toward political candidates or policy proposals may be of nearly equal value as demonstrations of support, depending upon an advocate’s point of view (Manheim 2011).

But political engagement involves far more than opposition or support. Political engagement covers a broad range of activities, most of which are subject to the influence of strategic communication flows. Although, as will be discussed below, much of that influence depends upon the kinds of data, information

and insight derived from surveillance, the mere threat of surveillance may also shape the quality, character and extent of political engagement (Kaminski and Witnov 2015).

The threat of surveillance of political activity invites consideration of the role that actual, or only imagined anonymity plays in key aspects of democratic decision-making. James Gardner (2011) provides a rather extensive, but still incomplete list of the kinds of information about our political activities that we might not want to see associated with our names or on Google maps indicating exactly where we live.

In thinking about political data as personal information, Ira Rubinstein (2014) is especially helpful in suggesting that there are many different kinds of data that have value for those seeking to influence the policy process through strategic communication. Some of the differences in data and their value have to do with how the information was acquired in the first place.

Among the most important and readily available information is that which has been supplied because it was required in order to gain access to some resource, such as registering to use Facebook, or even to post a response to an editorial in the local newspaper. Then, there is that massive amount of personal information that people volunteer as part of their effort to achieve visibility and status within some social network (Taddicken 2012). Of course, there is also that information that can be observed from particular vantage points within the network because of the protocols governing how a browser interacts with some website. And finally, as Rubinstein (2014: 874-5) suggests, there is that mass of information about individuals that is the product of statistical analysis. He refers to this as “inferred data.” It is important to consider the substantial distance that there might be between the kinds of supposedly factual or objective data that might had been required by an authority, and that which was volunteered within the context of a social network, and that which has been inferred through the analysis of massive amounts of transaction-generated-information (TGI) (Dahlgren 2013).

By distance, I am implying more than facticity. I am also referring to the kinds of claims about ownership or proprietary interest that an individual might make with regard to any of the characterizations that have been associated with her by an algorithm. Indeed, despite the well-argued appeals for the respect of contextual integrity (Nissenbaum 2004), a much more troubled, and troubling assessment suggests that the challenge of avoiding these normative constraints has become a commonplace burden within already existing centers of “surveillance capitalism” (Zuboff 2015).

Because simple avoidance is unlikely to serve as a defense against legal claims regarding invasions of privacy and the associated harms that result from algorithmic assessments, we can expect to see an expansion in the investments being made by data handlers in an effort to establish and reinforce an expanded set of defenses under the law (Crawford and Schultz 2014). These efforts will ironically involve unprecedented levels of audience segmentation and targeted political marketing.

Political Marketing

The marketing of candidates for public office, and the mobilization of support for, or opposition to particular public policies, all depend upon the collection, processing, and analysis of TGI. Part of what we are coming to understand about the nature of the digital age is the fact that nearly everything we do within the networked environment generates a record that has the potential for being associated in some way with other records in ways that facilitate the development of “actionable intelligence” (Gandy 2011). This strategic intelligence is used within political marketing campaigns to determine which are the best kinds of messages to be delivered through the most effective channels, at the most appropriate times, in order to generate the desired responses within a particular population segment that has been identified as a target.

When marketers talk about segmentation and targeting, they are usually referring to messages that have been designed for the general public. However, not even actively engaged members of the public are considered to be the primary, or the final targets of political messages. Members of the public are only the channels through which the real messages are delivered to the ultimate targets—the decision-makers, the people with the power to turn ideas into actions with consequences that matter.

Political scientists have developed an extensive literature that talks about this process as lobbying (Gilens and Page 2014). I have defined lobbying as a direct “information subsidy” (Gandy 1982). This is where representatives of interest groups seek direct access to legislators and other policy actors to provide information about public policy concerns, and in particular, to provide rationales for supporting one policy option over another. I recognize that this process still involves something of a multi-step flow from the organization, to the lobbyist, to the staff member, to the regulator, or legislator, but there is usually some understanding that the lobbyist is representing the interests of a third party.

Advocacy advertising, on the other hand, is designed to motivate members of the public to contact their legislative representatives and deliver those arguments as though they were the authentic result of debates, discussions and independent research taking place amongst ordinary members of the public. I refer to these as indirect information subsidies (Gandy 1982). Indirect information subsidies are believed to be effective, in part, because of the assumptions that the targets make regarding the motivations of the message source. When a communication source claims to be a concerned member of the public, perhaps even a voting constituent, legitimate individual or collective interest is more likely to be assumed by the ultimate target.

Marketing and the Formation of Public Policy

It is true that public policies are generally thought of as being designed and implemented within government agencies, administrations, and legislatures. However, we have also come to recognize that policies are also developed within the judiciary. Although policies that affect the public interest are also developed with corporations, and within professional organizations, we primarily have to depend upon policies established within the governmental sector to bring about some adjustment of the policies and practices of entities within the marketplace.

While the production of influence within the policy environment is a complex process, and I would suggest that political scientists are still quite some distance from agreement about how goals are most likely to be achieved (Harris and McGrath 2012), there is, however, general agreement that strategic communications campaigns that involve the delivery of carefully crafted messages delivered to particular population segments play a critically important role (Manheim 2011).

However, we are just beginning to consider the role that enhanced technologies of surveillance have come to play in this process (Tufekci 2014; Woolley and Howard 2016). It is important that an assessment of this technology is pursued through a perspective that seeks to minimize the harms that flow from its use within the policy realm. And, while concern about harms to individuals should always be present in one’s analysis and critique, I intend to focus on the harms that are being visited upon the democratic process and its contributions to our collective well-being.

The assessment of technology is multidimensional, in part because of the nature of its impacts are so varied across time, place, and population. We are almost always concerned about its functionality; about how well it serves its purposes. But we are also concerned about its unintended consequences; those primarily considered as collateral damage or externalities.

Uses Matter

This means that our assessments of technology should be extended to include evaluations of the resources that are used in the process of achieving results. Just as we have become concerned about the social cost of carbon as an energy source for our machines (National Academies of Sciences, Engineering and Medicine 2016), we need to be concerned about the social costs of personal information when it is used as a resource in the production of political influence.

Just as with carbon, our concern about the uses of TGI is often shaped by our awareness of the consequences that flow from that use. Policy-relevant decisions about the use of information in ways that affect the life chances of individuals are often framed in terms of a politically relevant social category to which an individual has been assigned. Such an individual might be a member of a protected class, and as a result, the government may have a special interest in ensuring that the technologies being used actually have some discriminatory and predictive power (Barocas and Selbst 2014).

On the other hand, that individual may only be a member of an analytically derived category; one for which there are no widely available data about the reliability or precision of their identification by statistical means. There is likely to be even less information available with regard to the consequences of the avoidance or neglect that might arise for members of such idiosyncratically defined groups (Rouvroy 2012). Although we don't have the data, the theory, or the research that we would need to predict many of those troublesome outcomes, researchers are beginning to develop strategies for evaluating some of the impacts of their use (Mackenzie 2015).

Users also Matter

It also matters who the users are, because the identification of a use does not automatically indicate the character and intentions of the user. The categorical identification of users often determines the limits on their access to and use of politically relevant information about individuals and population segments.

For example, we understand that political parties are privileged actors when it comes to gaining access to information and the resources they believe they need in order to produce and distribute messages designed to help achieve the party's goals (Bennett 2015; Howard and Kreiss 2010). There are still further distinctions to be drawn between long-standing political parties and a host of political action groups, organized and to some degree regulated in terms of their ability to gather and use funds to influence electoral outcomes, in comparison with the near absence of limits on their use of resources to affect public policies more directly.

I actually believe that there are meaningful distinctions to be drawn between profit seeking users of publically organized personal information and private, non-profit or public-interest oriented users of that same information. Yet, the fact that non-profit organizations are routinely organized in support of the interests of corporate actors, as in the mobilization of consumers of health-related products and services (Brennan, Eagle and Rice 2010), or in mobilizing support for the passage of industry-oriented legislation, including referenda at the state level (Hertel-Fernandez 2014; Sullivan 2010), suggests that such distinctions are unlikely to survive the rise in so-called "public-private partnerships," and other less formal relationships.

We have already seen that government agencies in the United States have come to rely upon commercial vendors of personal information as ways to work around the regulatory constraints that had initially been designed to limit both the gathering and the sharing of this kind of information (Dixon and Gellman 2014).

Actors on the Stage and Behind the Screens

There are additional concerns that need to be addressed. When I refer to users I am primarily referring to the policy entrepreneurs (Gandy 2003: 286-8) who are pursuing their individual and collective interests within the policy environment. Often these actors make use of resources within their own organizations to design and implement policy oriented campaigns.

Increasingly, however, they are making use of commercial service vendors to provide the data, skill and technology required to mount a successful campaign (Bennett 2015; Dixon and Gellman 2014). Many of the key actors in this massive and growing industry are multiproduct firms that are able to manage an entire campaign, while others are specialists in gathering publicly available information and combining it with information gathered by other means (Nickerson and Rogers 2014).

Aristotle is one of the older more traditional organizations that provide support for political campaigns in the US and around the world. Its campaigns are prime examples of strategic initiatives designed to generate indirect information subsidies (Rubinstein 2014). Sometimes the policy focus is quite precise and limited, such as getting a particular provision removed from a bill, or an alteration of a regulatory proposal up for consideration within an agency. As a multiproduct firm, Aristotle provides a campaign staff with maps, based on “geo-spatial selection tools,” as well as resources that allow field staff to report contributions, and commitments, as well as the ability to use the data acquired in the field to continually adjust elements of a digital media campaign (Aristotle 2016).

Like Aristotle, Catalist is also a multiproduct firm that provides data, analytics, and toolkits that political operatives use to win elections and to succeed in achieving policy goals. And, like other frontline data brokers, they claim that the information that has been gathered from a variety of sources can be used to model and predict the behavioral responses of the millions of individuals that have been captured within their files (Maghami 2012).

Grassroots vs. Astroturf

At this stage it is important to draw some distinctions between the use of data brokers and consultants like these to mobilize members of the public to deliver appeals to decision-makers to act appropriately, and the delivery of the same messages through organizations, entities, and even “robots” created specifically to create the impression of mobilized public opinion (Murthy et al. 2016).

We tend to refer to grassroots communications as the genuine expressions of deeply felt opinions by the politically engaged. Interest groups, including unions, corporations and business associations engage in grassroots lobbying, where their campaigns are focused on mobilizing their members and segments the public toward expressing their opinions directly to decision-makers within some policy-relevant domain (Walker 2012).

Astroturf, on the other hand, refers to an attempt to produce the same impact on decision-makers as that of a mobilized public, but without the need for any public engagement in deliberation, reflection and political communication. Astroturf communications are artificial, simulated, manufactured, illegitimate, and anti-democratic (McDonnell 2016). But, in the context of the arguments being made here, it is only fair to note that astroturf campaigns don’t rely quite so much upon the surveillance of the public as is common within grassroots campaigns.

Applied Surveillance Technology

I have suggested that we should consider surveillance in the context of policy formation in terms of its function as an applied social technology. I have also suggested that it deserves our attention because of the

sorts of changes that have emerged in the nature of this technology and its use within policy-oriented campaigns (Gandy 2001).

Third-party Tracking

While there are a great many changes in surveillance techniques that have taken place within the digital network environment in that make it difficult to identify which is more important than most others, third-party tracking is probably the leading candidate for that status (Mayer and Mitchell 2012).

It is through the tracking of individuals, or their devices, as they make their way around the web following the links provided by their favorite search engine, or their friends on social media platforms, that so much information is being generated and captured for strategic use within policy oriented campaigns. A great many of the websites that we visit, either leak or actively inform other sites about the kinds of information or activities that we have demonstrated an interest in (Libert 2015). Depending upon the nature of the relations between these parties, a user's identity could either be learned, or confirmed at the same time that the mosaic composition of their profile was being enhanced.

The emergence of third-party tracking services, working as partners or as competitors to earlier providers of list-based communication services, has been quite spectacular in terms of its development as a global phenomenon (Dixon and Gellman 2014).

It wasn't enough for websites to introduce parasitic devices, lovingly called "cookies" onto our browsers, without our knowledge or permission, in order to facilitate the identification of our machines. No, they had to develop cookies that only seemed to disappear after we engaged in a little housekeeping on our browsers. And, when that wasn't enough, they went on to develop "digital fingerprints" to help to identify not only your device, but also to move these snoops closer to identifying someone as the user of particular tools on a particular device within a household or an organization (Calabrese et. al. 2015).

Massive Data and Remote Sensing

We might want to think about some of these developments as an aspect of technological convergence. Changes in the size and portability of networked devices increases the ease with which transactions of interest can be initiated and completed. The fact that these devices are encumbered with a host of environmental sensors, making them part of the "Internet of Things" (Atzori, Iera and Morabito 2010), means that we are going to have to pay more attention to the process of normalization that scholars like Nils Zurawski has referred to in his studies of consumer surveillance (2011).

It is important for us to consider some of the means that have become available to transform this massive amount of data, derived from sensors and TGI, into the kinds of strategic intelligence that enables discrimination within the public sphere. I have suggested that it is useful to think about the use of big data analytics as a kind of "remote sensing," but with critical distinctions yet to be drawn (Gandy 2012). Unlike audio-visual technologies that amplify the signals that are produced as we move through the environment, much of the data that are used in assigning us to analytically generated categories and groups has actually been gathered from the activities of other people, rather than ourselves.

I'm not trying to minimize the importance of the information about specific individuals that are increasingly being aggregated in order to produce a profile that necessarily incorporates some aspects of their individual identity in order to facilitate their identification as a member of a category, class, or group. What I am trying to do is to emphasize the importance of those cues that are based in indirect, rather than direct information about an individual (Bloem et al. 2012). I am referring specifically to the kinds of information that are being used to generate fairly accurate, or reliable predictions regarding the answers about ourselves that we might have been reluctant to provide in response to questions that might not have

even been asked (Tufekci 2015: 209-12) because they were illegal, or simply not considered to be polite or appropriate in a particular context or relationship (Rouvroy 2012).

Knowing the Score

While people may self-identify as members of racial or ethnic groups, especially within the context of social media (Gutmann 2003), they are not likely to have known about, much less, been provided their scores on some of the measures that are being linked with them and others who share their racial, ethnic, or social classifications. There are a great variety of scores which are being assigned to individuals, that most of them know little about (Dixon and Gellman 2014). These include social influence scores, such as Klout and Cred, based on algorithmic evaluations of followers, re-tweets, or other indicators of status as opinion leaders within society.

Unfortunately, many have come to recognize that they don't really have much choice about using resources, or participating in social media, and accepting the rules about scoring that have been established, and then continually modified by these social platform managers (Turow, Hennessy and Draper 2015). More troublesome still, even without regard to concerns about the accuracy of these scores (Shmueli 2010), is the probability that they will be used in the determination of which members of the public will be included in, or excluded from, the stream of information about the issues being examined as part of some public policy debate (Rubinstein 2014: 895-97).

Experiments, Surveys and Predictive Models

We also need to come to terms with the fact that we are all almost certain to be participants in online experiments, most of which are being conducted without our knowledge and consent. These experiments, many of which are quite simple in their design, are actually quite important in terms of the impact they are already having on the level and character of public participation in the democratic process (van Otterlo 2014). Here I am referring to those experiments, referred to as A/B tests, that are being routinely administered to determine which communications cues are likely to be more successful with a particular audience segment in bringing about some desired behavior such as an online contribution to a political campaign.

It is important to consider, however, whether we should decide that all, or even most of these experiments, raise important privacy concerns. Some might believe that they actually represent yet another form of unpaid labor, in which users of social network platforms are contributing to the improvement of technologies that are likely to be used in the manipulation of others, who just happen to be like them in some not immediately obvious way (Gandy 2015).

Social Media Variants

Some readers of this journal might recall the negative public response that arose when it was learned that social networks and news and information platforms were conducting experiments in order to assess the impact that subtle adjustments in the supply of content might have on their users. A fairly important example was the so-called "randomized controlled trial of political mobilization messages" that were delivered to "61 million Facebook users during the 2010 US congressional elections."

When this study by Robert Bond and his colleagues was finally published (Bond et al. 2012) in the journal *Nature*, there was actually very little in the way of a critical public response, despite the significant impact that newsfeeds shared by "friends who had supposedly already voted," had as a nudge toward getting people out to vote.

A much more substantial critical public response emerged in 2014, in response to another Facebook experiment, this time about something called "emotional contagion." In the view of many, this project

seemed to have overstepped the bounds of research ethics because it placed subjects at emotional risk without providing the opportunity for those subjects to grant, or to withhold their informed consent (Meyer 2014; Tufekci 2015).

Electoral Campaigns

These ongoing experiments by internet service providers are slightly different from the kinds of experiments that have become a commonplace within electoral campaigns. Daniel Kreiss and Phil Howard (2010) have noted the almost continuous experimentation that had become a part of the Obama campaign in 2008. It was used to evaluate and then alter the emails being sent out to supporters in an effort to learn which messages were likely to result in more donations. They argued that these and other strategies that were designed to both understand and influence the development of particular orientations among supporters, should be seen as threats to what they called “political privacy” (Kreiss and Howard 2010: 1043). Similar arguments were made earlier with regard to the threats to voter privacy associated with online politics and e-campaigning (Hunter 2002).

Lisa Barnard and Kreiss later (2013) provided a historical trajectory of the movement of electoral campaigns toward identifying more specialized targets within the network environment. Of particular interest among the strategic developments that were put into play during the 2008 election cycle was the decision to go beyond the mobilization of individuals within the existing supporter base, to focus persuasive appeals on those individuals that analytical models had identified as being “undecided.”

These messages were designed, tested and adjusted in order to improve a campaign’s ability to move those people toward using specially developed interactive resources, such as a “tax cut calculator” that the “undecided” could then use to see how much money they would “save” under one of the many plans that the Obama campaign had promised to develop (Barnard and Kreiss 2013: 2053).

As we look back over the design and use of online experiments as aids to strategic communication, it seems pretty clear that there are no limits to the efforts being made to learn more about how to manipulate, or bypass particular segments within the population.

Experimentation in the Public Interest

It is worth noting, however, that many critical scholars actually engage in what most of us would recognize as experiments. But they often do them in an attempt to identify and evaluate some system that they believe discriminates in ways that would lead to cumulative disadvantage (Gandy 2009). For example, the identification of differential patterns in the responses generated by an organization, or its agents, whether human or not, would provide important information about the consequences that might flow from the widespread use of some segmentation technology. Christian Sandvig and his colleagues (2016) have proposed a number of experimental investigations that show great promise along these lines.

Arguably, these periodic assessments of algorithmic deciders could be administered by a government agency, in much the same way that municipal licenses and inspections officers periodically test weights, measures and the content of packages and containers of food products intended for sale. In the meantime, algorithmic audits of the sorts being proposed might still be worth doing, if it weren’t for the legal and ethical problems involved in masquerading as large groups of social network subscribers.

What is There to Be Done?

If we are going to alter the present trajectory of surveillance within the public sphere, we are certainly going to have to confront the need for better articulations of the nature of the harms that are likely to flow from the continued and expanded use of TGI as an aid to manipulative communications (Turow et al. 2012). Unfortunately, it hasn’t seemed to matter very much, at least not in the United States that people

say that they dislike being targeted for communications based on inferential data and algorithmic assessments.

Part of the reason for the lack of a government or corporate policy response seems to be that we have not been able to provide enough compelling examples of individual, or even collective privacy harms that matter very much in comparison to the values of technological advance, and the expansion of profitable businesses that support employment, or increases the direct or indirect flow of tax revenues to government accounts (Bennett 2011). Unfortunately, the values we associate with informed participation of the general public in the democratic process are not easily compared with the economic measures most commonly used in benefit/cost analyses. Among the most important harms to the public sphere, and the democracy that it supports, are those that are associated with the exclusion of some people from deliberation and debate, as well as the absence of a broadly experienced nudge to participate across the range of possibilities for engaging in political activity (Fraser 2007: 11-3).

Technological Confrontation

Of course, we value the contributions being made by the technologically gifted amongst us who have developed counter-measures designed to protect users from devices that enable third-party tracking. However, I suspect that there are not many who are willing to confront the awesome power of the corporate lawyers who are ready to bring the weight of the law down upon them for developing and sharing arguably illegal countermeasures like *Track Me Not*. We owe a tip of the hat to Daniel Howe and Helen Nissenbaum for the dedication, skill and courage that led them to step out onto that particular bridge (Howe and Nissenbaum 2009).

Regulatory Policy

Rather than hoping for the arrival of some reasonably stable technological advantage being achieved by the wizards working in support of contextual integrity and user control over the information they provide as they move through life, it seems clear to me that we need some kind of regulatory intervention. We need a regulatory policy that sets meaningful, and by that I mean enforceable, limits on the collection and use of TGI, especially for uses related to participation in the public sphere. Since it is somewhat easier to regulate business or commercial activity than it is to regulate political speech more directly, it might make more sense to explore the regulation of those organizations whose business it is to engage in the collection, processing and use of personal information in support of political manipulation.

Of course, and unfortunately, restriction on the use of information is not without difficulties; indeed, these difficulties are actually quite substantial. As we noted when we explored differences between users and uses of segmentation and targeting, there tends to be, understandably, far greater latitude given to communicators in the political arena.

Political speech is granted higher regard than commercial speech, and it is therefore subject to fewer limitations on time, place and manner (Bennett 2015). Part of what we will have to confront in the context of that barbed wire around political speech is the fact that the techniques and resources used as aids in the delivery of messages are often granted the same protection as the messages themselves.

In the US, the First Amendment and the protection of political speech would be the first line of defense taken in response to any regulatory challenges to a firm's ability to provide services arguably designed to support the speech act. On the other hand, I believe that it can be argued that segmentation and targeting is antithetical to the rights of audiences to access the kinds of speech that they actually need in order to become informed participants in public policy debates.

Aggressive Action

What I want to offer are some aggressive, and some might say bizarre, ideas. Part of what I have in mind is the development of a challenge to the ruling constructions of speech that combine, or confuse activity, such as profiling, segmentation, and targeting, enabled through surveillance, as speech worthy of defense. Here I am trying to separate the preparation and delivery of a message, from its design and use as a strategic resource.

Despite the tendency within the US to treat money as speech (Broton 2015), I believe that distinctions can and must be drawn between speakers, and their right to speak about certain things. And, although there is some recognition that corporations and other collectivities may in some legal contexts be treated as individuals, it is well past time for us to develop and argue the case once again that corporations are not people, and they do not, and should not have the same rights that are granted to individual human beings.

Tamara Piety (2012) has taken a giant first step in this direction with her book, *The Brandishing of the First Amendment*. She argues that virtually all speech by corporations is commercial speech, and almost none of it deserves constitutional protection against regulatory constraint. Following her arguments along these lines I would certainly want to argue that neither corporations, their executives, nor their agents have the right to engage in political speech designed to reach and influence members of the public.

Take a Leap of Faith

My final recommendation will require most of you to take something of a giant leap of faith. I am asking you to imagine the development and support of an information system optimized for democratic ends that would facilitate the flow of information to individuals based on the diversity and quality of their informational diets.

This is not a regulatory proposal. This is a marketplace proposal that might be subsidized by foundations concerned with the status of democracy. It might also be financed, in part, by taxes imposed upon advertiser-supported information flows, where it is reasonable to assume that the influence of sponsors over media content is substantial, and that its purpose is largely manipulative, rather than informative.

I am asking you to imagine the development of an alternative platform to Google, Twitter and Facebook. This would be one that sees diversity of political opinion, rather than its polarization, as a fundamental requirement of a healthy democracy, and therefore the primary goal of the platform. This beneficial outcome is expected to result from efforts to assist members of the public in developing healthier, more balanced informational diets.

Just as we have widely accepted and automated measures of the readability of texts, I suspect there are already resources based on computational linguistics that would facilitate the assessment of the content of our media diets with regard to ideological or political slants (Bozdog and van den Hoven 2015). Such a change in present patterns of media consumption would require a motivational campaign like many of those which are designed to help people to modify their diets in the interest of their health and well-being.

Such a campaign would have to be managed by cohorts of “trusted agents” rather than government censors. It would probably require the utilization of algorithms to evaluate our information diets and provide gentle nudges along the way. Unlike commercial ventures, however, such a campaign would have to be absolutely and demonstrably free of the threat of surveillance and the unauthorized sharing of personal information with others, any others. This might mean, of course, that assigning such tasks to “intelligent agents” will probably require that those agents are equipped with, or overseen by other agents that “will monitor audit, and hold... programs accountable” (Etzioni and Etzioni 2016).

This also means that, as a matter of principle, those internet service providers whose business it is to help us gain access to information, and to facilitate communication with others, will need to be guided by the same moral, ethical, and professional values that librarians have traditionally been bound by (Van Fleet and Wallace 2003). Whatever you read, hear, or view, should be nobody's business but yours.

References

- Andrejevic, Mark. 2007. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas.
- Aristotle, Inc. 2016. *Campaigns*. Available at: <http://aristotle.com/campaigns/>.
- Atzori, Luigi, Antonio Iera and Giacomo Morabito. 2010. "The Internet of Things: A Survey." *Computer Networks* 54: 2787-2805. Available at: <http://dx.doi.org/10.1016/j.comnet.2010.05.010>.
- Barnard, Lisa and Daniel Kreiss. 2013. "A Research Agenda for Online Political Advertising: Surveying Campaign Practices, 2000-2012." *International Journal of Communication* 7: 2046-66. Available at: <http://ijoc.org/index.php/ijoc/article/download/1746>.
- Barocas, Solon and Andrew D. Selbst. 2015. "Big Data's Disparate Impact." In press, *California Law Review* 105. Available at: <http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf>.
- Bennett, Colin J. 2011. "In defense of privacy: the concept and the regime." *Surveillance & Society* 8(4): 485-496. Available at: <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4184/0>.
- . 2015. "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications." *Surveillance & Society* 13(3/4): 370-384. Available at: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/download/voter_surv/voters.
- Bloem, Jaap, Meno van Doorn, Sander Dulvestein, Thomas van Manen and Erik van Ommeren. 2012. "Big Social: Predicting Behavior with Big Data." *VINT Research Report* (2) of 4. Paris: Sogeti. Available at: <http://labs.sogeti.com/big-social-predicting-behavior-with-big-data-download-the-new-vint-research-report/>.
- Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle and James H. Fowler. 2012. "A 61-million-person Experiment in Social Influence and Political Mobilization." *Nature* 489 September: 295-98.
- Bozdag, Engin and Jeroen van den Hoven. 2015. "Breaking the Filter Bubble: Democracy and Design." *Ethics and Information Technology* 17: 249-65. DOI: 10.1007/s10676-015-9380-y.
- Brennan, Ross, Lynne Eagle and David Rice. 2010. "Medicalization and Marketing." *Journal of Macromarketing* 30(1): 8-22. DOI: 10.1177/0276146709352221.
- Brooten, Lisa. 2015. "Political Speech and the Law." In *The International Encyclopedia of Digital Communication and Society*, edited by Robin Mansell and Peng Hwa Ang. New York: John Wiley and Sons. DOI: 10.1002/9781118290743.wbiecds142.
- Calabrese, Cris, Katherine L. McInnis, G.S. Hans, and Greg Norcie. 2015. "Comments for November 2015 Workshop on Cross-Device Tracking." Washington, DC: Center for Democracy and Technology. Available at: <https://cdt.org/insight/comments-on-cross-device-tracking-to-the-ftc/>.
- Calo, Ryan. 2014. "Digital Market Manipulation." *The George Washington Law Review* 82(4): 995-1051. Available at: http://www.gwlr.org/wpcontent/uploads/2014/10/Calo_82_41.pdf.
- Chadwick, Andrew. 2006. *Internet Politics: States, Citizens, and New Communication Technologies*. New York: Oxford University Press.
- Crawford, Kate and Jason Schultz. 2014. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms." *Boston College Law Review* 55(93). Available at: <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>.
- Dahlgren, Peter. 2013. *The Political Web*. New York: Palgrave Macmillan.
- Dawes, Simon. 2014. "Press Freedom, Privacy and the Public Sphere." *Journalism Studies* 15(1): 17-32. DOI: 10.1080/1461670X.2013.765637.
- Dean, Jodi. 2009. *Democracy and Other Neoliberal Fantasies*. Durham, NC: Duke University Press.
- Dixon, Pam and Robert Gellman. 2014. *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*. San Diego: World Privacy Forum. Available at: www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.
- Etzioni, Amitai and Oren Etzioni. 2016. "AI assisted ethics." *Ethics and Information Technology* 18: 149-56.
- Fraser, Nancy. 2007. "Transnationalizing the Public Sphere: On the Legitimacy and Efficacy of Public Opinion in a Post-Westphalian World." *Theory, Culture & Society* 24(4): 7-30. DOI: 10.1177/0263276407080090.
- Fuchs, Christian. 2015. *Culture and Economy in the Age of Social Media*. New York: Routledge.
- Gandy, Oscar H. Jr. 1982. *Beyond Agenda Setting. Information Subsidies and Public Policy*. Norwood, NJ: Ablex Publishers.
- . 2001. "Dividing Practices: Segmentation and Targeting in the Emerging Public Sphere." In *Mediated Politics: Communication in the Future of Democracy*, edited by W. Lance Bennett and Robert M. Entman, 141-59. New York: Cambridge University Press.
- . 2003. "Public Opinion Surveys and the Formation of Privacy Policy." *Journal of Social Issues* 59(2): 283-299.
- . 2009. *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Burlington, VT: Ashgate.

- . 2011. “Consumer Protection in Cyberspace.” *Triple C: Cognition, Communication, Cooperation* 9(2):178-89. Available at: <http://www.triplec.at/index.php/tripleC/article/viewFile/267/241>.
- . 2012. “Statistical surveillance: Remote sensing in the digital age.” In *Routledge Handbook of Surveillance Studies*, edited by Kirstie S. Ball, Kevin D. Haggerty and David Lyon, 125-32. New York: Routledge.
- . 2015. “Toward a Political Economy of Framing: Putting Inequality on the Public Policy Agenda.” *The Political Economy of Communication* 3(2): 88-112. Available at: <http://www.polecom.org/index.php/polecom/article/view/60>.
- Gardner, James A. 2011. “Anonymity and Democratic Citizenship.” *William & Mary Bill of Rights Journal* 19: 927-957. Available at: <http://scholarship.law.wm.edu/wmborj/vol19/iss4/6>.
- Garnham, Nicholas. 1990. “The Media and the Public Sphere.” In *Capitalism and Communication: Global Culture and the Economics of Information*, edited by Fred Inglis, 104-114. Newbury Park, CA: SAGE Publications.
- Gilens, Martin and Benjamin Page. 2014. “Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens.” *Perspectives on Politics* 12(3): 564-81. Available at: <http://dx.doi.org/10.1017/S1537592714001595>.
- Gutmann, Amy. 2003. *Identity in Democracy*. Princeton, NJ: Princeton University Press.
- . and Dennis Thompson. 2004. *Why Deliberative Democracy?* Princeton, NJ: Princeton University Press.
- Habermas, Jürgen. 1998. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Translated by William Rehg. Cambridge, MA: The MIT Press.
- Harris, Phil and Conor McGrath. 2012. “Political Marketing and Lobbying: A Neglected Perspective and Research Agenda.” *Journal of Political Marketing* 11(1-2): 75-94. Available at: <http://dx.doi.org/10.1080/15377857.2012.642745>.
- Hertel-Fernandez, Alexander. 2014. “Who Passes Business’s “Model Bills”? Policy Capacity and Corporate Influence in U.S. State Politics.” *Perspectives on Politics* 12(3): 582-602. DOI:10.1017/S1537592714001601.
- Howard, Philip N. and Daniel Kreiss. 2010. “Political Parties and Voter Privacy: Australia, Canada, the United Kingdom, and United States in Comparative Perspective.” *First Monday* 15(12). Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/297_5/2627.
- Howe, Daniel C., and Helen Nissenbaum. 2009. “TrackMeNot: Resisting Surveillance in Web Search.” In *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, edited by Ian Kerr, Carole Lucock and Valerie Steeves, 417-36. New York: Oxford University Press.
- Hunter, Christopher D. 2002. “Political Privacy and Online Politics: How E-Campaigning Threatens Voter Privacy.” *First Monday* 7(2). Available at: <http://firstmonday.org/ojs/index.php/fm/article/viewArticle/930/852>.
- Kaminski, Margot E. and Shane Witnov. 2015. “The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech.” *University of Richmond Law Review* 49: 465-518. Available at: <http://ssrn.com/abstract=2550385>.
- Kreiss, Daniel and Philip N. Howard. 2010. “New Challenges to Political Privacy: Lessons from the First U.S. Presidential Race in the Web 2.0 Era.” *International Journal of Communication* 4:1032-50. Available at: <http://ijoc.org/index.php/ijoc/article/viewFile/870/473>.
- Libert, Timothy 2015. “Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites.” *International Journal of Communication* 9: 3544-61. Available at: [https://timlibert.me/pdf/Libert-2015-Exposing Hidden Web on Million Sites.pdf](https://timlibert.me/pdf/Libert-2015-Exposing%20Hidden%20Web%20on%20Million%20Sites.pdf).
- Mackenzie, Adrian. 2015. “The Production of Prediction: What Does Machine Learning Want?” *European Journal of Cultural Studies* 18(4-5). DOI: 10.1177/1367549415577384.
- Maghami, Neil. 2012. *Catalist for Victory: How Nonprofits and Unions Have Struggled to Re-elect President Obama*. Capital Research Center. Available at: <http://capitalresearch.org/wp-content/uploads/2012/10/OT11121.pdf>.
- Manheim, Jarol. B. 2011. *Strategy in Information and Influence Campaigns*. New York: Routledge.
- Mayer, Jonathan R. and John C. Mitchell 2012. “Third-Party Web Tracking: Policy and Technology”. Paper presented at the IEEE Symposium on Security and Privacy (SP). May 20-23, San Francisco. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6234427>.
- McDonnell, Mary-Hunter 2016. “Radical Repertoires: The Incidence and Impact of Corporate-Sponsored Social Activism.” *Organization Science*, January. DOI: 10.1287/orsc.2015.1017.
- Meyer, Robinson. 2014. “Everything We Know about Facebook’s Secret Mood Manipulation Experiment.” *The Atlantic*. Available at: <http://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>.
- Murthy, Dhiraj, Alison B. Powell, Ramine Tinati, Nick Ansead, Leslie Carr, Susan J. Halford and Mark Weal. 2016. “Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital.” *International Journal of Communication* 10: 4952-71. Available at: <http://ijoc.org/index.php/ijoc/article/viewFile/6271/1806>.
- National Academies of Sciences, Engineering, and Medicine. 2016. *Assessment of Approaches to Updating the Social Cost of Carbon: Phase 1 Report on a Near-Term Update*. Committee on Assessing Approaches to Updating the Social Cost of Carbon, Board on Environmental Change and Society. Washington, DC: The National Academies Press. DOI: 10.17226/21898.
- Nickerson, David W. and Todd Rogers. 2014. Political Campaigns and Big Data. *Journal of Economic Perspectives*. 24(2): 51-74. www.aeaweb.org/articles?id=10.1257/jep.28.2.5.
- Nissenbaum, Helen. 2004. “Privacy as Contextual Integrity”. *Washington Law Review* 79: 119-57.

- Peters, John Durham. 2004. "The 'Marketplace of Ideas': A History of the Concept." In *Toward a Political Economy of Culture: Capitalism and Communication in the Twenty-First Century*, edited by Andrew Calabrese and Colin Sparks, 65-82. Lanham, MD: Rowman & Littlefield.
- Piety, Tamara R. 2012. *Brandishing the First Amendment: Commercial Expression in America*. Ann Arbor: The University of Michigan Press.
- Rouvroy, Antoinette. 2012. "The End(s) of Critique: Data-behaviourism vs. Due-process." In *Privacy, Due Process and the Computational Turn*, edited by Mireille Hildebrandt and Ekatarina De Vries. New York: Routledge. Available at: http://works.bepress.com/antoinette_rouvroy/44.
- Rubinstein, Ira. S. 2014. "Voter Privacy in the Age of Big Data." *Wisconsin Law Review*. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447956.
- Sandvig, Christian, Kevin Hamilton, Karrie Karahalios and Cedric Langbort. 2016. "When the Algorithm Itself Is a Racist: Diagnosing Ethical Harm in the Basic Components of Software." *International Journal of Communication* 10: 4972-90. Available at: <http://ijoc.org/index.php/ijoc/article/download/6182/1807>.
- Shmueli, Galit. 2010. "To Explain or Predict?" *Statistical Science* 25(3): 289-310. Available at: <http://projecteuclid.org/euclid.ss/1294167961>.
- Sullivan, Laura. 2010. "Prison Economics Help Drive Ariz. Immigration Law." *NPR News Investigations*. Available at: <http://www.npr.org/2010/10/28/130833741/prison-economics-help-drive-ariz-immigration-law>.
- Taddicken, Monika. 2012. "Privacy, Surveillance, and Self-Disclosure in the Social Web: Exploring the User's Perspectives via Focus Groups." In *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, edited by Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval, 255-72. New York: Routledge.
- Tufekci, Zeynep. 2014. "Engineering the Public: Big Data, Surveillance, and Computational Politics." *First Monday* 19(7). Available at: <http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097>.
- . 2015. "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency." *Colorado Technology Law Journal*. <http://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf>.
- Turow, Joseph, Michael X. Delli Carpini, Nora A. Draper and Rowan Howard-Williams. 2012. "Americans Roundly Reject Tailored Political Advertising." *Scholarly Commons*. Annenberg School for Communication, University of Pennsylvania. Available at: http://repository.upenn.edu/asc_papers/398.
- , Michael Hennessy and Nora Draper. 2015. "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation." Report. Philadelphia, PA: The Annenberg School for Communication, University of Pennsylvania. Available at: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.
- Van Fleet, Connie and Danny P. Wallace. 2003. "Virtual Libraries—Real Threats: Technostress and Virtual Reference." *Reference & User Services Quarterly* 42(3): 188-91.
- van Otterlo, Martijn. 2014. "Automated Experimentation in Walden 3.0: The Next Step in Profiling, Predicting, Control and Surveillance." *Surveillance & Society* 12(2): 255-72. Available at: <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/walden3/walden>.
- Walker, Edward T. 2012. "Putting a Face on the Issue: Corporate Stakeholder Mobilization in Professional Grassroots Lobbying Campaigns." *Business and Society* 51(4): 561-601.
- White, Stephen K. 1988. *The Recent Work of Jürgen Habermas: Reason, Justice and Modernity*. New York: Cambridge University Press.
- Woolley, Samuel C. and Philip N. Howard. 2016. "Political Communication, Computational Propaganda, and Autonomous Agents." *International Journal of Communication* 10: 4882-90. Available at: <http://ijoc.org/index.php/ijoc/article/viewFile/6298/1809>.
- Zuboff, S. 2015. Big other: Surveillance capitalism and the prospects of an information civilization". *Journal of Information Technology* 30: 75-89. Available at: <http://www.palgrave-journals.com/jit/journal/v30/n1/pdf/jit20155a.pdf>.
- Zurawski, Nils. 2011. "Local Practice and Global Data: Loyalty Cards, Social Practices, and Consumer Surveillance." *The Sociological Quarterly* 52: 509-27.