The pace of social, economic, and political change in the last two decades is nothing short of stunning. The neat divisions between the East and West political blocs came crashing down with the dismantling of the Berlin Wall, and global integration and the rise of the BRIC (Brazil, Russia, India and China) is reconfiguring global economic relations. These dramatic changes, however, pale in comparison to the impact information communication technologies (ICTs) are having on every aspect of our lives. In particular, ICTs have changed dramatically both the nature of commerce and its relationship to the state. Specifically, ICTs infuse our consumer identities into the market machine and the security state through the digital footprints that we leave as we go about our daily lives. Meanwhile, citizens are increasingly unable to configure their political identities within states that are market- and security-oriented.

This chapter examines the contraction of the public sphere in which political identity is contested and created through negotiations within a geographically defined community. At the same time that our identities are being commodified for commercial transactions using ICT techniques, neoliberal discourse stifles our identity as citizens. Its emphasis on the primacy of the market elevates the role of the individual economically while downplaying the importance of the connection between the individual as citizen to the state. Security measures
taken in response to the events of September 11, 2001, have further constrained the ability of citizens to question this new citizen identity: draconian surveillance policies and technologies have flowed outward from the United States to other nations, leading to a dramatic reconfiguration of the institutions and purpose of the state. The state’s most important function for its citizenry now appears to be to provide security, and personal information-sharing among public and private institutions means that anonymity is practically impossible. Moreover, the distinction between public and private in individual, organizational, and sectoral terms is blurring to such an extent that it is difficult to distinguish between them. Ironically then, as citizens become atomized into individual consumers, they are simultaneously losing the autonomy that comes with having a private space into which they can retreat. Consumer profiling done by corporate entities for the purpose of selling products, combined with a political discourse that emphasizes security over freedom, makes for a toxic mix that systematically corrodes not only personal autonomy but agency as well.

What is lost to individual civic agency in the articulation of our collective identity through market activities is the expression of a larger common good that is not market- or security-related. As autonomous individuals with tenuous connections to each other in political community, we are increasingly vulnerable to the vagaries of unfettered market forces. As communal bonds weaken, citizen identity is replaced by consumer identity in the global and virtual marketplace. The intersection of these individual shifts in identity with new technologies and security interests contributes to the decline of a citizenry that understands that it has both rights and responsibilities, both of which are contested in the public sphere. This decline will have serious consequences for the health of democratic systems.

Let us look first at understanding how public and private (or personal) spaces have been conceptualized before the advent of the ICT revolution. The next question to take up is how the neoliberal reconstruction of the public sphere and the impact of the U.S. Patriot Act on individual autonomy are shaping notions of public and private space in the digital age. These reconfigurations are reshaping not only public discourse, but our conception of ourselves as citizens of a political community. This chapter uses Canadian examples to support its assertions, but this is a global phenomenon that, thanks to the Internet, has facilitated both hegemonic and reactive discourses that do not respect territorial boundaries.
THE PUBLIC, THE PRIVATE, AND POWER WITHIN PERSONAL PLACE

In the essay “The Virtual Sphere” Zizi Papacharissi makes a distinction between public sphere and public space. While the difference between public and private is easy to grasp, the difference between a public space and the public sphere is more subtle. Referring to thinkers such as Dewey (1927) and Tocqueville (1990), Papacharissi notes, “the term ‘public’ connotes ideas of citizenship, commonality, and things not private, but accessible and observable by all.” She remarks, “participation in public affairs contribute[s] significantly to an individual’s sense of existence and self-respect” (2002: 10). It is not simply free universal access to information gathered in a public space that is crucial to the public sphere, but active participation, its creation as a site of social activity, and rational discourse constituting a collective public will. As Papacharissi observes: “A virtual space enhances discussion; a virtual sphere enhances democracy” (11). Goldberg (2011) concurs: he cautions that the nature of cyberspace as a zone of democratic discussion does not constitute the direct transfer of an ideal public sphere, if one still exists, to online contexts. Papacharissi concludes that the privatizing forces of capitalism today create a mass commercial culture that stands in place of a public sphere; the Internet in this context constitutes what can only be considered a public space.

The ideal configuration of the public sphere has long been an object of interest to those concerned with politics and democracy. Robert Putnam (1995) argues that communal bonds that come from a variety of associational networks are critical to fostering social cohesion that supports participation in public affairs. These networks comprise the dense thicket of relationships that together form civil society. As the size and activities of government contract, the importance of civil society grows with respect to both service provision and social cohesion, as groups within it step into the void left by the state. The role of ICTs in facilitating new identities within civil society has attracted much scholarly attention; the most salient point for this analysis is that identity creation is happening in a public space as opposed to the public sphere. What is missing from Papacharissi’s analysis is consideration of how cyberspace is fundamentally changing individuals’ ability to draw a line between their private and public personae. Privacy is the tool that is used to delineate the line between the personal and the public, both in its social and its disciplinary/regulatory forms.

The notion that group deliberation produces the best public policy has been advocated by writers as diverse as Dewey (1927), Habermas (1989), and Etzioni...
While a public “space” provides another forum for discussion, it should not be conflated with the public “sphere”—an arena that should be inclusive, include a diversity of opinion, and should produce policy that reflects a plurality of viewpoints. If certain groups are systematically excluded, the public sphere fails to live up to the democratic ideal. So, for example, Fraser (1992) notes that those who have been excluded from or marginalized within the dominant public sphere will create a counter sphere. Clearly, the Internet and social media provide powerful new tools for alternative messaging. However, as Papacharissi points out:

When individuals address random topics, in random order without a commonly shared understanding of the social importance of a particular issue, then conversation becomes more fragmented and its impact is mitigated. The ability to discuss any political subject at random, drifting in and out of discussions and topics on whim can be very liberating, but it does not create a common starting point for political discussion. Ultimately, there is a danger that these technologies may overemphasize our differences and downplay or even restrict our commonalities. (2002: 20)

Papacharissi’s analysis is particularly useful for this discussion of public spaces and spheres because she recognizes that cyberspace is both public and private space. “Cyberspace provides new terrain for the playing out of the age-old friction between personal and collective identity; the individual and community” (2002: 20). Internet communities allow individuals to connect with other like-minded individuals in online communities of interest. These communities in turn help shape individual identity. Hannah Arendt argues that these communities of interest are increasingly becoming the new public sphere: “The polis is not the city-state in its physical location; it is the organization of the people as it arises out of acting and speaking together . . . no matter where they happen to be” (2005: 198). What differentiates traditional communities of interest from those mediated by technology is scale. ICTs can broaden the discourse by rendering geographic boundaries meaningless, while simultaneously fragmenting the discourse among participants who share fewer identity bonds. Moreover, self-selection in or out of communities of interest means that, by Papacharissi’s definition, these fora are public spaces as opposed to spheres. Without mediation by the state that gives voice to the marginalized, the public space is limited in its utility in creating collective identity for a territorially defined political community.
What is missing from Papacharissi’s analysis is a consideration of how cyberspace is fundamentally changing individuals’ ability to draw a line between their private and public personae. Privacy is the tool that is used to delineate the line between the personal and the public, both in its social and in its disciplinary/regulatory forms. In the information era, this is best defined as “information privacy.” Privacy rights proponents cite the 1890 article by Samuel Warren and Louis Brandeis, “The Right to Privacy,” as the first articulation of “the right to be let alone.” Warren and Brandeis were motivated to write this article because of the advent of photography, which allowed print media to engage in “sensationalist” journalism by circulating candid images of individuals without their consent. What was previously private could now be “shouted from the rooftops” by a journalist equipped with a camera. Clearly, Warren and Brandeis could not begin to conceive of the technologies that, a hundred years later, would allow shouts on the rooftop to be heard instantly all around the globe by anyone who has a cellphone with a WiFi connection. While the Warren and Brandeis article signals the beginning of modern concern for digital privacy, it should be noted that privacy concerns date back to ancient and early modern societies such as the Greeks, Hebrews, and English Puritans. Privacy in its most basic physical form is generally seen as a place of solitude to which one can retreat for quiet reflection and contemplation (Stefanick 2011: 34).

Yet privacy has a dark side as well. The feminist call to arms—“the personal is the political”—was one of the earliest attempts to expose “privacy” as a tool for the domination of individuals; in this case, men rely on privacy to oppress women within the confines of the home. Feminists identify the traditional line that distinguishes the private realm of the “family” from the public sphere of the community as a tool that reproduces the societal suppression of women’s rights in their most intimate relationships. What happened behind closed doors was not subject to discussion in the public sphere, even if it involved violence or sexual assault. According to Catherine MacKinnon, the “right of privacy is a right of men ‘to be let alone’ to oppress women one at a time” (MacKinnon, 1989). While this is particularly true with respect to intimate relationships, declaring that transparency is impossible because personal privacy must be protected is increasingly used as a shield behind which those in positions of authority can hide, enabling them to engage in activities that oppress individuals, free from public scrutiny.

Is radical transparency the answer then? According to Foucault the disciplinary power of transparency is far more effective in enforcing social conformity
than is physical punishment (1977: 195–228). Using Bentham’s concept of the panopticon prison where inmates are constrained by the possibility of being watched, Foucault argues that the norms of society and its subsequent expectations serve to constrain personal autonomy. In short, their actions are constrained by reflexive consciousness. Formerly, Foucault and others focused attention on the state as the site where social norms were defined, contested, and enforced. But the power of the monopoly state has given way to the distributed power of the networked state. This suggests the emergence of a synopticon state, as articulated by Thomas Mathieson (1997): rather than the single agent that watches multiple people, the many watch the few. This can result in citizens watching those in power, thus forcing accountability on those in positions of power. The networked state, however, suggests that sites of power are distributed, thus disrupting the potential power of the synopticon society. An example of this is the introduction of “Internet Eyes” in the United Kingdom. This CCTV monitoring company streams video live to subscribing viewers, who report suspicious activity to police in exchange for points toward an online game. Thus the synopticon state also suggests that the many watch not only state officials but also each other. Crowd-sourcing crime prevention suggests a scenario that is less useful from a democratic perspective; the mob watching the individual, exerting “justice” on those who deviate from social norms.

What becomes apparent from this brief overview of the conceptualization of public and private space/sphere is that, while they help to construct an analytical framework, the divisions are contested. Moreover, it is evident that Internet technology has the potential to shift the ground under our feet. The spread of neoliberalism adds additional complexity by fundamentally transforming public institutions and the roles they play in society.

NEOLIBERALISM AND THE RECONSTRUCTION OF THE PUBLIC SPHERE

One of the biggest contributors to the shrinking of the public sphere as a place where citizenship is defined is the infusion of neoliberal thinking into all aspects of government. With its focus on maximizing individual autonomy through enhanced rights to private property and the ability to engage in market-based activities, this approach advocates mimicking the private sector in almost all aspects of social, political, and economic life. With respect to the organization of state institutions, neoliberalism dictates the adoption of private-sector management practices, dramatically reducing or contracting out services to the
private and not-for-profit sectors, and decentralizing authority by transferring functions to regional authorities or community boards. It effectively hollows out and de-centres the state by removing it from its pedestal of social control. The newly reconfigured state has the capacity to “steer” the direction of society but its success is dictated by its responsiveness to the market-based currents in which it is embedded. The notion of “governance” as opposed to “government” reflects this important shift in emphasis. Governance recognizes the plurality of rules and actors that influence society; societal “steering” thus becomes a networked process of negotiations among societal units whose position in the power structure is not fixed. Actors exchange information and negotiate rules and processes for managing common affairs. The rise of ITCs facilitates the information flows among actors; when this happens the flow breaks down institutional distinctions.

These developments are part of a larger reconfiguration that sees states focusing on new priorities and assuming new roles. Joachim Hirsch argues that the post-WWII welfare state is transforming into the “national competitive state.” He notes that “this type of state concentrates on the mobilization of all productive forces for the purpose of international competition, setting aside the former politics of materially based social and political integration” (1997: 45).

In other words, politics are being taken out of government in order to focus on “efficiency” defined in economic terms. In the twentieth century, public service was organized around core public administration values. In contrast, the twenty-first century’s public service model comprises the “networked” organization that embodies neoliberal values. As Chakrabarty and Bhattacharya (2005) observe: “Globalization has led to a ‘marriage’ between corporate discipline and entrepreneurial spirit, with the government discarding its traditional image of ‘a doer.’ Seeking to accommodate ‘the market impulse,’ the government has become ‘an enabler.’” Indeed, Sorenson describes the state in even weaker terms: “the state has become a differentiated, fragmented, and multi-centered institutional complex that is held together by more or less formalized networks” (Sorensen, 2006: 100). A major shortcoming of this new conception of the complex networked state is that it hinders transparency. Particular interests may have an advantage that is not easily seen, let alone acknowledged.

The change in the form and function of the state is the result of a larger ideological change wherein the proper role of government is restricted to apolitical or technical activities. This necessarily downplays the role of the state in facilitating social construction that promotes inclusion, equity, and equality.
Instantaneous communication; the transnational character of most economic and political functions; and the emphasis on a smaller, leaner bureaucratic state combine to produce a new approach to public administration, referred to as “the New Public Management” (NPM).

NPM is premised on the notion that small government is good government, and that management practices from the private sector should be applied to the public sector. Productivity through competition is achieved by contracting out service provision to the private sector or to nonprofit organizations. It also involves the use of private sector managerial perspectives, geared toward “customer” satisfaction and the use of risk management techniques to minimize exposure to disruptive forces. In the world of information management, analyzing customer preferences and shopping habits against their demographic information provides critical marketing information. Every time a consumer uses a loyalty card to receive “members benefits,” a breadcrumb is left on the data trail that comprises digital identity. This data provides crucial information to a retailer concerned about product placement, and also to those who buy and sell personal information. Such bodies of data are also critical to governments in the development of public policy.

Habermas (1987) refers to this infiltration of the public sphere by the private as the “colonization of the lifeworld.” He argues that it is this intrusion of instrumental logic from the private, commercial sphere into the public, cultural sphere that is responsible for the crisis of legitimacy that currently experienced by established democracies. Low participation rates in voting testify to this; neoliberal governments use citizen loss of faith in their state institutions to claim that they have no option but to allow the private sector to devour the public. But perhaps the hollowing out of the state is precipitating the legitimation crisis?

The hollowing out of the state means several things. First, as the money citizens contribute to the state lessens through decreased taxation rates, citizens care less about the state. Specifically, as consumers, we tend to be most concerned about things that we pay for, especially those things with a high price tag. In addition, the contraction of global services in favour of targeted services means that the state becomes increasingly irrelevant to those who pay the most taxes (but now receive the least benefit). Second, many of the public goods delivered by the state are not “products” but are ephemeral contributions to community health and wellness, such as the support of recreation, festivals, and art and culture. Taxpayers who identify as customers of state services will
have difficulty locating the product they are paying for. The decrease in “public goods,” as well as the significance of these tangible and intangible goods to community well-being, make citizens more susceptible to the argument that we are consumers first and citizens second, in a digital world where the primary value of identity is to commercial interests who can use the information to target their particular product.

Corporations devote enormous resources to data mining: the art of finding patterns in data sets, using computational processes. Indeed, a 2013 *Globe and Mail* article in the Careers section had the title: “Hot Jobs, Crunch the Numbers: Data Analytics Specialists Mine Market Demand” (Galt, 2013: B1). Not only is this commercial information valuable for product marketing, it is valuable in and of itself to data-brokers, who frequently resell it to government. Information sharing between these two sectors is illustrated by the relationship of private airline companies to the federal government. The government sets the regulations, which force the companies to collect particular types of information before a passenger is allowed to get on an airplane. Airlines then pass on information to the government. Corporations are not the only ones mining data, however. Political parties use public data they receive from Elections Canada as a base from which to build a profile of voters from data attained from commercial sources. As such, the collection, retention and exchange of information do not occur on a one-way street; data flows in both directions through permeable institutional boundaries.

The market orientation of private-sector media systems controlling one particular form and flow of information further breaks down the distinctions between nation-states and private-sector entities, as well as distinctions among nation-states. As Thussu (2007) notes:

> Nationality scarcely matters in this market-oriented media ecology, as producers view the audience principally as consumers and not as citizens. This shift from a state-centric and national view of media to one defined by consumer interest and transnational markets has been a key factor in the expansion and acceleration of media flows: from North to South, from East to West, and from South to South, though their volume varies according to the size and value of the market. (12)

Media information that is decoupled from national identities in favour of a global consumer identity serves to reinforce the propensity of individuals to self-identify as a consumer as opposed to a citizen.
Once we start thinking of ourselves primarily in consumer terms (which brands do I want to identify with? Which ones will enhance my status? Do I post my location as “Fernie Alpine Resort” when I take a picture of myself skiing and post it on Facebook, or do I reject corporate branding on principle?), we have fewer expectations that the state will promote our interests as citizens. In turn, low expectations reinforce the tendency to think of ourselves as individuals as opposed to members of a collectivity. The state in the past has been the primary site for the definition of a political identity; the state, however, is in a very weakened position as ICTs have also facilitated the movement of global capital, which means that the state has to create favourable conditions for capital retention. In the end, combined with hollowing out, there is a vacuum. Who expresses our collective identity and for what purpose?

IDENTITY IN THE AGE OF INSECURITY

The preceding discussion might suggest that the power of the state is receding to the point that it has little influence on our collective lives. While the state has relinquished its role with respect to promoting the collective wellbeing of citizens through active engagement in activities that promote some degree of equality in social, economic, and political manners, it has embraced its role as protector of citizens. The scope of this role is greatly enhanced by ICTs that provide powerful new tools for surveillance. The emphasis on security can be conceived as one more example of the blurring of the public- and private-sector roles—“security” stripped down is a modified version of the private-sector compulsion to manage risks. In the public sector, however, risk management has resulted in an assault on civil liberties, particularly with respect to data management.

The passage of the U.S. Patriot Act is a milestone with respect to curtailing individual information privacy rights. Passed only six weeks after the events of 9/11, this Act gave the U.S. government sweeping powers with respect to gaining access to information. It contains provisions that allow the government to force companies to surrender information to the FBI; companies are prohibited from revealing that the privacy of the information in their control has been compromised. Once in the hands of government officials, there are no provisions in the Act that prohibit the dissemination of this information, or the use of the information for purposes other than for which it is collected. It was passed in great haste and is not subject to the usual checks that protect civil liberties.
The U.S. Patriot Act has caused great concern in other countries, as its effects bleed over national borders in the same manner as information flows. For example, any information collected by the City of Edmonton from candidates applying for jobs with the municipality are subject to provisions of the Patriot Act, as the information management company that handles employment screening (and thus candidate information) is based in the U.S. This type of information-sharing caused an uproar in B.C. a decade ago, when citizens there realized that the management of their medical information was to be outsourced to an American company (Stefanick, 2007). At a time when being HIV positive was a reason to be denied entry to the U.S., British Columbians demanded that their information be held in Canada because they worried that they would have no idea where it would end up. Would their medical information find its way to U.S. customs?

One thing 9/11 demonstrated to us is that fear can cause us to do things we might not otherwise agree to. Fairfield (2005) describes how Americans and their politicians succumbed to such fear when they abrogated civil liberties in order to give the state extraordinary powers. He notes “when politicians in the heat of the moment, resort to draconian measures, it falls to social critics and theorists to call such actions by their name rather than allow themselves to be swept up in hysteria” (45). Canada followed suit with its own antiterrorism legislation. It was not as draconian but still produced heated debate. In 2011, however, a significant change was made with little fanfare to PIPEDA, Canada’s privacy act covering private-sector entities. This provision replicates the U.S. Patriot Act in allowing companies to hand over personal information to authorities without a warrant. As in the U.S., Canadian companies can be forbidden to alert individuals that the privacy of their information has been breached (Tencer, 2011).

Since 2001, the blurring of private and public sectors is most evident in private security companies, and other companies whose products can be used for security. So, for example, Google is regularly asked by governments to provide user data, and as both the legal framework and the standards are evolving in this area, the guidelines determining what is properly private data and what should be shared with government are contested—contested not in the public sphere but in the backrooms where lawyers and lawsuits reign supreme. In the U.S., it was revealed that AT&T allowed the U.S. National Security Agency to monitor its customers. Lawsuits against the company ensued, and the U.S. government moved quickly to amend FISA to protect companies from liability in the course of complying with security agencies. More important, cloud computing
is now included. This is particularly problematic for nongovernmental organizations and some public sector institutions, many of which use commercial software and computing services in a bid to save money. Data monitoring by the U.S. government violates basic organizational autonomy, and in particular the autonomy of individuals within those organizations who might be deemed a security threat.

What is interesting about fear as a tool that enforces complacency at the loss of civil liberties is that it is not restricted to the governmental level, but has seeped into our personal lives. As a result, the first surveillance-complacent generation is growing up; they understand personal tracking as a given. Parents bemoan their wired youth who disappear into a virtual space of gaming and chat rooms where predators lurk. In an effort to exert their influence on their dependents, parents embrace security measures such as installing home surveillance systems (including nanny cams to watch their children or pets), monitoring their children’s social activity through social media, tracking their scholastic activity through software such as SchoolZone, and monitoring their physical movements through GPS-enabled cell phones. Children (and other social media users) inadvertently contribute to their own surveillance whenever they post to social media. There is little wonder that young adults currently have a difficult time growing up and out from under “helicopter” parents. And more important, given that all the information posted on social media sites is used to categorize people for marketing purposes, the implications for personal autonomy are substantial for a generation taught that giving over personal data for corporate use is nothing to fear, and, moreover, that surveillance is a small price to pay for protection from predators. The danger with individuals trading autonomy for security is the blurring of the public and private spheres. At the same time, we, as collections of individuals, are also inadvertently trading freedom of expression for security. History has taught us that suppression of civil liberties has dire democratic consequences; the next section explores this theme with respect to those who are best equipped to critique the current trajectory of government policy-making.

SOCIAL SCIENCE, POLITICAL DISCOURSE, AND THE PUBLIC INTEREST

Surveillance provides an important example of the blurring of the boundaries between public and private space, and between the consumer-citizen and corporate-government entities. With respect to legislatively sanctioned state surveillance, there is an absence of the voices of social scientists whom Fairfield calls
upon to speak up against the incursion of the state into private space. In Canada, under the Harper government, the voices of reflective reasoning that advocate for evidence-based policy making were stifled. At the federal level, there was a concentrated effort to prevent the dissemination of research results, both in the “soft” and “hard” sciences. At an international conference of scientists in 2012, scientists and journalists convened a panel entitled “Unmuzzling Government Scientists: How to Re-open the Discourse.” Journalists lamented that it has become just about impossible to get information from government scientists in a timely fashion because now they must go through many layers of bureaucratic approvals before they can speak with the media. As O’Hara observes: “If we’re talking about policy that’s informed by fact, if we’re asking people to be critical thinkers, if we’re asking people to engage in democratic process and to engage in democracy, it’s incumbent on all of that we make sure the process is transparent” (CBC News, 2012).

O’Hara’s concern is not limited to Canadian scientists. In 2013, foreign researchers participating in a decades-old collaboration with federal government scientists claimed that a new confidentiality agreement they were required to sign was unacceptable. In the words of a physical oceanographer at the University of Delaware: “I believe this is a disturbing political climate change . . . I feel that it threatens my academic freedom and potentially muzzles my ability to publish data and interpretation and talk [in a] timely [way] on science issues of potential public interest without government interference” (CBC News, 2013). This concern for the suppression of scientific knowledge has been raised by others who have felt the impact of new government policies: for instance, the cancellation of an important statistical tool (the long-form census), and classifying librarians and archivists making presentations to school classes and conferences as engaging in “high risk” activities (Munro, 2013).

At the provincial level, the government of Alberta provides a clear example of the globalized neoliberal “reform” of education that is achieved through slashing post-secondary funding (Barkawi, 2013). Done in the name of fiscal exigency, these dramatic and deep cuts to the postsecondary education sector in 2012 and 2013 were less about money and more about promoting research that lends itself to commercialization. The emphasis on economically profitable research inevitably stifles academic freedom and the curiosity-driven research that produces critical analysis of government policy. Shortly after the 2013 budget was announced, the government of Alberta sent all postsecondary institutions “mandate letters” that sought to eliminate duplications and inefficiencies within the
postsecondary system by encouraging institutions to cooperate. Ironically, this neoliberal government that supports competition in the economic sector is trying to create monopolies with respect to the production of ideas. What is more troubling, however, is the focus on those academic activities that promote the commercialization of research. Coupled with crippling cuts, Budget 2013 made postsecondary institutions more reliant on industry funding. Rather than producing citizens with critical thinking skills, this trajectory serves the short-term interests of business and the economy at the cost of an informed and critically educated populace.

These trends in education and knowledge dissemination are part of a larger reconstruction of the public sphere, both with respect to institutional structure and information flow. Structural change, new management practices, and information flows combine with heightened concerns for personal and national security to produce a profound reconfiguration of the state. This new, networked form is actually harder for an attentive public to scrutinize, particularly because of the fuzzy distinctions between public- and private-sector boundaries. The net result is the contraction of a public sphere in which ideas are contested in the course of debating the nature of a collective, political identity.

THE SECURITY STATE AND THE CITIZEN-CONSUMER

The contraction of the public sphere where political identity is contested is the result of three interrelated forces: the dramatic reconfiguration of the institutions and purpose of the state, the commodification of identity through digitization, and the subsequent blurring of the distinctions between the public and private sectors. These forces are fuelled by the ascendance of neoliberal discourse that puts a high premium on market-based activities and freedoms. Individuals are losing their identities as citizens of a geographically defined political community through their redefinition as individual consumers who identify with, and are identified by, commercial entities. This emphasis on the individual, and in particular the individual as consumer, is producing an increasingly truncated public debate in the ever-contracting sphere in which this debate can happen. A limited debate and a limited public sphere have grave implications for democracy; the expression of collective identity has shifted from public institutions to an atomistic aggregation of participation in market activities.

Yet while the rights and responsibilities of individuals as citizens are decreasing, so too are their rights as customers. The citizen-consumer produces a
mountain of data in the course of everyday life. This information is collected, retained, and exchanged between and among organizations. Individual identity is being commodified, providing an important fuel for the production process and helping companies to position themselves within the marketplace. But such an atomized identity is also fed back into the machinery of the state, to be used in its role as the guardian of collective security.

The terrible events of September 11, 2001 caused many Americans to willingly sacrifice control of their personal data in exchange for security, via the passage of the U.S. Patriot Act. Citizens of other states followed suit by supporting their own states’ legislative responses to the crisis. Because of the fluid nature of digital communications, the consequences of this draconian American legislation flow across national borders. Insecurity over personal safety has tumbled over into many other areas of life, feeding the propensity to use new surveillance technologies, from nanny cams to GPS tracking, in day-to-day life. As institutions increasingly scrutinize individual action, personal agency is constrained, particularly when deviance is seen as a threat to personal security. As Foucault has observed, the watched begin to identify with the watcher (1977: 202–3).

The rise of the security state is happening at the same time as the demise of the welfare state. The notion that the state gives expression to national citizenship through the provision of universal services and a social safety net has been discounted. Neoliberal ideology is systematically dismantling the form and function of the administrative state through downsizing activities and outsourcing services to the private and not-for-profit sectors. As a result of the blurring of sectors, the expression of collective identity is shifting from our public institutions to the aggregation of our participation in market activities as autonomous individuals. These market transactions are increasingly mediated through digital media that allow commercial entities to track and monitor our activities. Our commodified identities feed the market machine of the private sector, which in turn feeds the securitization machine in the public sector. The quest to manage security risks often entails that individuals give up important rights as citizens. Combined with the contraction of the public sphere, where important political issues such as relinquishing citizen rights are debated, the prospects for individual autonomy are chilling. The question arises as to who is watching the watchers.
REFERENCES


246 Democracy and Identity in the Digital Age
10.15215/aupress/9781771991292.01


