LOOKING AHEAD

Rob Faris & Rebekah Heacock

The essays collected in this report echo a familiar narrative about Internet and society: digital technologies enable new forms of human interaction that disrupt existing political, social, and economic systems. Some of this disruption is good, and some bad. Public institutions, particularly legislative and formal regulatory mechanisms, have struggled to keep up with the rapid pace of change; companies and citizens have proven to be far more nimble in leveraging the affordances of digital communication and exploiting new opportunities. Although this narrative glosses over many important details—some of which are addressed earlier in this report—as a general premise, it tends to hold true. The ongoing legislative efforts around the world to create a coherent and enforceable framework for regulating online activity have shown modest success; meanwhile, private ordering plays a major role in digital affairs.

Many of the concerns over Internet policy and practice over the past two decades have focused on the nature and scale of content regulations by governments, such as the blocking of websites and social media platforms, and the appropriateness of different legal mechanisms for regulating online activity. This debate shows no signs of abating. Political pressure for restricting online content continues to be powerful, whether from civil society concerned with harmful activity online or from governments that are intent on consolidating power, though strong coalitions have emerged to resist proposals for greater Internet controls. In countries with a reliable adherence to the rule of law and robust civil liberties protections, the past two decades of debates over controlling Internet activity have commonly resulted in an uncomfortable balance of speech protections that leave much harmful speech unimpeded and fail to fully address security concerns. In more repressive environments, civil society activity has been suppressed without evidence of any corollary gains in terms of security or reduction of harmful speech.

Revelations regarding state surveillance have shifted the political landscape over the past year, and questions regarding the ramifications of and responses to this surveillance are likely to dominate Internet policy discussions into the foreseeable future, along with related questions of security and privacy. We appear to be entering a new stage in the debates over Internet policy based on the awkward realization that democratic governments that have promoted an open Internet also have been engaged in extensive surveillance, outside of the public scrutiny and with few political constraints, and that these surveillance programs likely represent a serious threat to the open Internet. This may mark the beginning of a major rethinking of the familiar narratives and allegiances in the debate over maintaining an open and connected Internet, with the United States at the center of the controversy. Although it is too soon to understand the full implications of these changes, they appear to have introduced a crisis of trust in the evolving Internet governance institutions and a growing rejection of the status quo and current distribution of power. Governments around the world have reacted to the surveillance revelations with a strong call to reduce the influence of the United States in managing the core infrastructure of the Internet. This provides political support to those countries that have pushed for a greater role for the ITU in Internet governance. The signatories of the Montevideo Statement on the Future of Internet Cooperation, including ICANN, ISOC, IETF, W3C, and several registries, called

for "accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing," which implies a lesser US role in these matters, although without suggesting an increase in the role of the ITU.

A growing fear is that failing to strike a new deal on state surveillance may lead to greater Balkanization if countries use this as a rationale for erecting greater walls around their sovereign space. More scrutiny is already being paid to international data flows and routing patterns, and the location of servers and data hosting will likely garner even more attention in the coming months.

The general consensus is that the surveillance and information acquisition capabilities of governments are outpacing commercial and civil society efforts to secure personal communication online. This is true of the United States, China, Russia, and every other country that invests in state surveillance. A central question for the coming years will be whether a new bargain can be reached over the extent, means, and governance of state surveillance, both within and across national borders. As in prior policy questions, this plays out in both the political and technological realms. The political questions center on the viability of legal and institutional mechanisms to limit state surveillance. The veil of secrecy that ensconces state surveillance forms a formidable obstacle to attempts to limit the scope of government activity and promote transparency and accountability.

The battles over surveillance are being waged not only at the political and legal level but also by technologists, some working to better secure digital communication networks against unwanted snooping, and others cracking into these networks. Rather than seeking to define rules and regulations through legal and political channels, this battle is less constrained by laws and political processes, is more adversarial in nature, and is taking place largely out of public view—through tapping into submarine cables, gathering up telephone records, and hacking into private communication channels. Reforming the political and governance structures that operate state surveillance programs can and should be part of any solution. However, if the lessons of the past carry into the future, it will be the advances in the technologies of privacy and surveillance that define the limits of surveillance. An open question is whether surveillance-resistant tools are developed and deployed that will restore a widely accepted balance between state surveillance and private communication. Technology companies have a strong incentive to improve the sense of security among their users and to restore faith in their commitment to protect users from excessive surveillance. There is also renewed impetus to develop non-commercial and open source tools to secure online security and privacy.

Traditionally, cybersecurity and surveillance have not been strongly linked in policy discussions, and have been often presented as complementary: the notion that spying on one's enemies will help in securing digital networks from attack. This logic is inverted when a country turns the attention of its surveillance program to its own citizens. The technologies and tools that help to secure companies and citizens from unauthorized intrusions and cyberattacks also make state surveillance more difficult, and efforts to diminish these security measures make citizens and corporations more vulnerable to malicious attacks. Although far from a foregone conclusion, the current prominence of state surveillance issues could shift the framing of national debates around cybersecurity from a narrative of warring cyber armies to more broadly securing personal communication on digital networks from all potential attackers.

Protecting privacy online, whether from governments, companies, or other users, is of growing concern, and state surveillance is compounding a growing uneasiness regarding the acquisition, use, and distribution of personal information by private sector companies. Moreover, the ability of the state to collect information on people is supported by private sector data collection and the willingness of users to share information in private, semi-public, and public spaces online. This is a structural issue that runs deep into economic and social foundations of the Internet. A vast number of Internet users have offered up personal information to companies in quasi-consensual relationships in exchange for free access to social media, social networking, search, email, mobile applications, and a host of other online services. The monetization of this data in turn finances and maintains the Internet that entertains and enthralls these users. Crafting a new bargain over privacy and individual data seems both overdue and somehow more difficult by the minute. Any deal must work within or around the market and technological structures that define today's digital infrastructure. One question is whether Internet users may be willing to pay for more of the services they use in exchange for greater privacy protections. An alternative question is whether stronger legal mandates for protecting privacy online will imperil innovation in online consumer services.

Potentially lost in the debates over privacy, security, and surveillance, is the fact that access to information plays a critical role in human development, governance, and economic growth across all sectors, including health, education, energy, agriculture, and transportation. As the actions of governments, companies, and citizens shift the balance of privacy, surveillance, and security online, whether by technological, political, legal, or market-based means, important public policy questions lie in the balance.