Computing as Oppression: Authoritarian Technology Poses a Worldwide Threat

DOUGLAS SCHULER, The Evergreen State College and The Public Sphere Project

The advent and ubiquity of interconnected digital computer systems provides a cornucopia of opportunities for enabling oppression. While commercial (legitimate and criminal) enterprises use these for questionable purposes, big governmental systems, generally with industry cooperation, pose substantial threats to freedom and democracy and to collective problem-solving abilities (civic intelligence) worldwide. The government of China has established a startlingly pervasive network of surveillance, censorship, and incarceration for social control and is now expanding that system domestically while making the tools within that system available worldwide. While there are other perpetrators, including the United States, China's approach is further advanced and has fewer constraints than those found in more democratic states. The new evolving control/surveillance infrastructure based substantially on technological advances presents ethical and practical dilemmas for computer professionals and their associations. The preamble of the ACM Code of Ethics and Professional Conduct states that in order to act responsibly, computing professionals "should reflect upon the wider impacts of their work, consistently supporting the public good." This commentary intends to point out the urgency of these issues, contribute to the wider discussion, and encourage social responsibility within the profession.

CCS Concepts: • **Social and professional topics → Government technology policy**;

Additional Key Words and Phrases: Social control, surveillance, professional associations, democracy, civic intelligence

ACM Reference format:
Douglas Schuler. 2022. Computing as Oppression: Authoritarian Technology Poses a Worldwide Threat. *Digit. Gov. Res. Pract.* 3, 4, Article 29 (December 2022), 11 pages.
https://doi.org/10.1145/3568400

1 INTRODUCTION

Computer professionals cannot undue all the damage that has been done with their technology nor prevent all the damage that is to come. Nevertheless, not only because they have enacted these systems but also because they understand them better than most, computer professionals must assume more responsibility. For starters, computer professionals must help promote public understanding of these systems, both challenges and opportunities, and be part of the discussion on what ought to be done going forward, including finding ways to confront powerful entities. Unfortunately, current approaches to slowing down, stopping, or otherwise mediating these dangerous trajectories are generally failing to achieve positive results. While China presents an especially significant set of issues, versions of those issues can be found anywhere.

Author's address: D. Schuler, The Evergreen State College and The Public Sphere Project; email: douglas@publicsphereproject.org.

2639-0175/2022/12-ART29 $15.00
https://doi.org/10.1145/3568400

The Association for Computing Machinery (ACM), the world's largest computing society, must shoulder at least some of the responsibility of providing ethical leadership regarding negative uses of computing. Because of the broad technological claims and aspirations and the nature of China itself — its influence, economic strength, and political practices — this special issue of the ACM's journal *Digital Government: Research and Practice* dedicated to New Directions in Chinese Governance presents a direct challenge to this responsibility. Unfortunately, while the special issue potentially will provide an important window into a new era of technologically focused systems of governance, many issues in relation to social responsibility were missing in the call for commentary [1] and might not have been discussed in response. The relevant issues such as participation in governance, inclusion, and public supervision of government that were mentioned in the call, seemed to be out of place with its technocratic focus. Moreover, those features are likely to be unpopular with the Chinese government and, hence, unlikely to be realized.

More broadly, the challenges that the Chinese government and other authoritarian governments are presenting to computing professionals, associations of computing professionals, policy makers, and citizens are immense. There is nothing less at stake than how the world is governed in the future and what sort of social orders and disorders we construct via our incredibly powerful digital capabilities.

2 SOME BACKGROUND

This commentary focuses on the spread of oppressive technology that is sanctioned by the Chinese government. In doing so, a number of other relevant threads are also discussed, including the role of computing professionals and associations of computing professionals. Although parts of this commentary are written in the first person, I have endeavored to keep emotion out this as well as personal feelings. However, as a relevant aside, I would suggest that the "personal feelings" I might have — and emotions generally — are natural and are likely shared by vast numbers of people who are anxious about the seeming inevitability of computer misuse. The first part of this commentary relates my experiences bringing it into being, since that is relevant to the issues at hand.

My discomfort with this project began with the call for contributions, which seemed to celebrate digital technology as a sort of panacea. It also sidestepped the sustained disregard of human rights and democratic principles on the part of the Chinese government. At that point, I wrote a letter to the editor of *Communications of the ACM* (*CACM*), the flagship periodical of the Association for Computing Machinery (the professional organization that sponsors this journal — *Digital Government: Research and Practice*). Soon afterwards, the editors-in-chief of this journal contacted me and demonstrated their desire for multiple perspectives, including their receptiveness to the airing of criticism of new and emerging their digital governance. For this reason, I want to express my gratitude to people within *CACM* and to the editors of this journal for their encouragement.

While some commitment is implicitly made in the call to fairness regarding potential criticism through the reviewing process, the invitation to "international colleagues" (which I took to mean colleagues who are not Chinese citizens living in China) in the call to submit "commentaries" suggested to me that "international colleagues" were not expected to submit "regular special issue papers." This would have suggested that Chinese nationals would constitute the sole eligible contributors, which would raise serious questions regarding the openness of the call. I was assured by the journal editors that this was not the case. However, while I am content with writing a commentary (because my career did not depend on ranking), I do wonder whether critiques are somehow by their nature unsuitable grist for the academic mill (such as this journal) perhaps because they are not necessarily theoretical. If that is the case, explicitly or implicitly, the scholarly world, especially in regards to implications of computing and society, is not fulfilling its obligations.

Discussions about the use of computing in society are often one-sided, with the commercial community and the technical community basically joining forces with the message asserting that computing is invariably a social good. That often unspoken assumption causes great harm to discussions about computing in society because computing seems to cause, or at least enable, a disparate set of negative effects, including the explosion of wealth disparity worldwide. More to the point of this topic, moving democratic practices and infrastructure into digital realms has always been problematic [2]. The computing community needs to play a special and difficult role here, especially in not overselling technological "solutions" or ignoring potential and actual risks. However, rather than highlighting the dangers of these advanced technologies or calling for more scrutiny, the call for participation suggests an almost inevitable future built upon technological solutions.

To my mind, especially in a journal devoted to the use of computing within governmental systems, calls for papers should explicitly state that critiques relating to computing in society are encouraged and that they would not be prejudged as unacceptable. If critique is not explicitly requested and the frame of computing as an unqualified social good is tacitly reinforced, then both contributors and reviewers — and, ultimately, readers— are less likely to gain a more realistic and multifaceted view. While this outcome is not certain, the readers may then go on to design systems that are critically flawed or take part in decision-making that helps bring these flawed systems into public use unaware of the critical perspectives. In this regard, arguably, this journal has the additional responsibility to help promote social good, with the obvious caveat that this does not excuse faulty reasoning, sloppy scholarship, or propagandizing within the journal.

3 REFLECTING ON THE CALL FOR PAPERS

The introduction to the call for papers raises several dubious and somewhat ominous points. The first sentence states that "The in-depth application of emerging technologies such as the Internet, big data, and artificial intelligence (AI) is bringing about a new round of digital government advancement." This by itself may not be a big problem. However, thinking about a system of governance, especially one that is presumed to have at least some democratic characteristics, as basically an engineering project that will make the system more advanced and more modern (as we see below) is a flawed assumption. And if "advancement" (and "modernization") just means doing what is being done already, only faster and to more people, then the call, at least in this case, is implicitly describing computing technology whose primary goals are reducing freedom and democracy.

Later we see that: "Data intelligence technology integrates government affairs data, promotes the digital transformation of governments at all levels, and realizes precision social governance." And: "The outbreak of COVID-19 in 2020 has strengthened the Chinese government's embrace of "using big data to improve and modernize national governance," and has advanced the development of digital government in a more comprehensive, systematic, and precise manner." The idea of precision in both statements stands out because of its implications: that the system can be entirely accurate (no false negatives or positives) and that it can (will?) be *precisely* tailored to meet particular circumstances — two somewhat dubious assumptions. The combination of comprehensive, systematic, and precise suggests that the systems they develop are likely to be less transparent (in the code and in practice) and more resistant to understanding, let alone criticism. And while the topics section explicitly lists "Political participation of cyber groups" (but not, for example, ethnic groups), "Public supervision of the process of government," and "Rule of law, representation, and participatory engagement of diverse voices," one gets the general impression that the call is seeking technological achievements and designs rather than critical explorations.

Finally, within the list of positive tech-induced outcomes, the assertion that "the system also creates new opportunities, and environments for the development of democratic politics" seems to be out of place. Of course there are likely to be opportunities, but *having* opportunities is not the same as providing them. And given the government's mass surveillance over Weibo, WeChat, and other online media that Chinese citizens are allowed to access, whatever opportunities that are created through their new systems are undoubtedly going to be carefully crafted to preclude citizen independence, privacy, or prerogative.

4 WHY CHINA? NOT ONLY CHINA

Democracy around the world, as seen through a variety of measures, is threatened [3]. Many of the world's leaders and political parties are devoting substantial energy towards oppressing one or more groups of people rather than governing and working to address shared problems. People are losing their faith in democracy's ability to address shared problems at the same time that they are being inundated with fake news — information often in the form of deranged conspiracies — that is manufactured with the intent of confusing and deceiving. Although China is not the only player on the world stage whose commitment to democracy seems largely rhetorical, China's economic might, technological influence, and worldwide stature certainly mark it as a country of particular concern.

Current events in China seem to argue strongly against any hope for increasing democratization. One example of this was the government destruction of *Apple Daily*, the Hong Kong–based periodical that was critical of the Chinese government, with national security police [4]. The government also dismantled democratic institutions in Hong Kong, arrested Democratic party politicians and activists on national security charges, and required that all candidates must be vetted by the state before they are allowed to run for office [5].

The near absolute power of the Chinese state may surprise citizens living in relatively free societies. In 2017, for example, the government went so far as to ban the image of Winnie the Pooh from social media because a photo of Chinese President Xi Jinping and US President Barack Obama was being posted adjacent to an illustration of Pooh and Eeyore on social media, portraying the Chinese president in an unsanctioned way [6]. In a much more sweeping and significant move, the Chinese government recently declared that the maximum number of hours that people under 18 years of age are allowed to spend playing online video games per week is three (doled out in three one-hour sessions) [7]. Regardless of whether that might in fact be a good thing, this declaration was simply imposed without any public dialogue. In a similar fashion, a few weeks later, television shows and competitions that portrayed men as being too effeminate in the eyes of the authorities were banned [8], a practice which has accelerated since this paper was first submitted [9].

5 SOCIAL DISCREDIT

The governmental systems discussed in the call for papers are also likely to be connected to China's wide-ranging Social Credit system that is being developed by the PRC and "social-media conglomerates such as Alibaba and Tencent to build an Orwellian-sounding Social Credit System that will rank citizens' and businesses' reputations based on their purchases, movements, and public communications" [10]. This system, which had its origins in banking and financial credit ratings, has expanded its horizons considerably. It maintains data on millions of citizens and businesses related to financial dealings as well as prosaic infractions such as playing loud music, parking bicycles in unsanctioned ways, or jaywalking. Low scores invite punishments, which are meted out algorithmically, ranging from throttling Internet speeds to restricting access to jobs, travel, and credit [10]. The system is integrated with Skynet, a vast surveillance system across China incorporating facial recognition, big data, and AI. Furthermore, according to Ron Deibert of the Citizen Lab, which monitors antidemocratic use of technology, "Companies operating in the PRC must comply with China's 2016 cybersecurity law, which requires them to police their networks, silently censor private chats and public posts, and share user data whenever PRC authorities demand it" [10].

In addition to the everyday censorship and surveillance of its citizens by the Chinese state, the government has been systematically oppressing an entire ethnic group, the 12 million Uyghurs in Western China who are being singled out for abuse, undergoing constant surveillance (described by critics as being "turbocharged by technology" [12]) and forced resettlement to re-education centers. Estimates of the numbers of people held in these centers are generally around 1 million people [12]. The forced Sinicization of this Muslim population, redolent of "conversion therapy" that has been imposed on gay people, is part of their "Strike Hard Policy," which is ongoing [13]. These are — as are other egregious actions — legitimized on the basis of national security, a fairly common approach in illiberal and authoritarian countries that is inimical to human rights considerations. The humanitarian group Human Rights Watch has extensively studied Chinese use of high-tech against the Uyghurs [13]:

> "Efforts to monitor Uyghurs include the use of modern, and often cutting-edge, surveillance and biometric technologies. Human Rights Watch has documented the Xinjiang authorities' directive to

> authorities to collect biometrics, including DNA samples, fingerprints, iris scans, and blood types of all residents between the age of 12 and 65 [14]. These biometrics, as well as "voice samples," are collected as part of the passport application process; in addition, DNA and blood types are being collected through a free annual physical exams program."

Recently, in fact, scientific papers based on this unethical gathering of personal data have been retracted from scientific journals [15]. The government also censors all critical discussions in China concerning the state's policies towards minorities in Xinjiang [14] and prohibits international journalists and many others from visiting Xinjiang.

6 EXPORTING OPPRESSION

While the techno-authoritarian infrastructure within China is vast, what is made in China does not necessarily stay in China. The Chinese government is at the forefront of surveillance and control systems, which will be sought — and bought — by authoritarian governments around the world struggling to maintain and extend their dominance over their citizens. In terms of revenue, the Chinese are the most successful vendors, but they do have competition. The United States is not far behind. Technology that is antithetical to democracy and human rights is in high demand [16].

China and other countries are using and developing facial recognition technology, mobile hacking tools, cameras, and AI as elements in surveillance infrastructures. Social media surveillance data used to influence elections, social media bots used to sow misinformation and confusion, and mobile phone scanners that allow government to intercept citizens' private communications and locations are all popular. New laws are being enacted to ensure that no one eludes the state's surveillance complex, including compulsory registration of mobile phone SIM cards and laws requiring mobile phone and Internet companies to save all mobile communication data [11, 16, 17]. And speaking of infrastructure, states sometimes may want to shut down the bits of infrastructure that are not working for them, using "technologies to enable internet shutdowns in specific districts and of particular platforms" [16].

While it is true that there is overreach and problematic behavior in and by other governments, China seems to be in a league of its own. Four main factors contribute to China's formidable production of worrisome tech: (1) a trained, advanced, sizable, and well-resourced workforce; (2) economic demand for the products from the vast Chinese state; (3) a willingness to quickly incorporate new research into large-scale surveillance systems; and (4) central authority with no barriers posed by democratic processes. This has enabled them to move quickly into a more threatening space in which *active* systems are employed. Robots equipped with stun guns navigate their own path down designated routes to police parks and other public places [18]. In other places in China, robots amble through train stations looking for suspects using face recognition software while also answering travelers' questions. In addition, "in the central metropolis of Wuhan, the Ministry of Public Security has teamed up with tech giant Tencent to develop a fully automated police station driven by the latter's AI technology" [18]. It is not difficult to imagine this as the early stages of a juggernaut beyond anybody's control: the coupling of mobility, autonomy, ubiquity, and weaponry in a digital policing context has nightmare written all over it. At the same time, in China, the relationship between the state and its citizens is determined solely by the state. The government owns the digital records of all Chinese citizens. Given China's harsh handling of dissent and its assumptions of infallibility and inalienable right, more ominous shadows are being cast on the current digital government enterprise. It suggests that computing technology will enable them to do what they are already doing but faster, with a broader coverage, and — less oversight.

7 DEMOCRACY?

The call for papers does not claim that China is a democracy or even that it strives to be one, while the Chinese government itself asserts that it is one [19, 20]. It does, however, state that China's new digital government trends create "new opportunities, and environments for the development of democratic politics," which raises some significant questions. What forms would these opportunities and environments take? And how realistic are those outcomes given the current state of affairs and the trajectory that the Chinese government is taking?

The roles of government and citizens in democratic societies, however imperfectly they are enacted in practice, have some clear, base-level functions. All citizens must have certain rights that protect them from government overreach and enable them to participate in the affairs of the country. By using the first 10 articles in the US Constitution (the Bill of Rights) as a rough set of democracy indicators, China fails in most of them, including freedom of religion, free speech, free press, freedom to assemble, free to be secure in one's home, the right to a speedy and public trial, as well as protection from cruel and unusual punishment. In addition to failing normative and procedural features of democratic governance, these failures violate the United Nations Declaration of Human Rights as well as China's Constitution and treaties to which they are signatories [21].

Moreover, per the Bill of Rights, the citizenry (with the assistance of independent media and governmental cross-checks) is expected to keep the power of government in check. The degradation of these safeguards at the hands of authoritarian governments is increasingly common: the previous president of the United States, for example, employed various approaches with the aim of remaining in power after losing the 2020 election, including dubious employee hirings and firings in key positions, and is still making false accusations about the election. To counter these assaults and to help ensure democracy going forward, the rights of the citizens must be encoded in law and protected by the state. Additionally, to perform democratic duties, citizens must have the intellectual (and many other) resources, individual and group skills (such as being able to work together effectively), and the ability to put issues and proposals on the agenda. They must have sufficient collective efficacy or civic intelligence [22] to perform the duties of citizens. Unfortunately, that important capability is singled out for special attention by the Chinese government; it is monitored and systematically undermined. In the case of social media in China, for example, it seems that while posts critical of local government officials are often not censored, posts that endorse any type of collective action, even if *supportive* of the government, are generally disappeared by the censors [23], suggesting that *any* type of independence of thought and action is discouraged. It does not stop there, however: censorship prevents people from consuming or providing information that the state deems unacceptable but it actively decides what information its citizens *should* see as well. For example, when Russia invaded Ukraine in March 2022, Chinese officials echoed stories from Russian state media, including fabrications that Ukrainian President Zelenskyy had fled Kyiv. This was posted to the Twitter-like Weibo site "that was viewed 510 million times and used by 163 media outlets in the country" [24].

Governance in China currently is based predominantly on severely limiting the autonomy of its citizens. This work depends to a large degree on surveillance of posts on social media, telephone calls, and actions in public settings, with special attention paid to specific ethnic groups. But, as Tony Roberts points out, "All surveillance is a violation of human rights" [16] and clearly degrades democracy in the process. He goes on to say that "Surveillance of political opponents, journalists, judges or peaceful campaigners is illegal whoever it is carried out by" and suggests that "selling of spy technologies to violate citizens' rights" should therefore also be made illegal. Transparency, although not mentioned in the call, is also critical for democratic systems. However, in the Chinese social credit system, for example, opacity is legally enforced: "The algorithms that derive the credit scores are trade secrets, prohibiting forms of testing that can determine how they work." Moreover, China (and other authoritarian countries worldwide) are also prohibiting, capturing, or otherwise diluting the independence, access, and influence of the variety of institutions or infrastructures that help maintain democracies. The seizure of the *Apple Daily* newspaper in Hong Kong mentioned earlier is a prime example [4].

8 RESPONSIBILITY AND BIG PLAYERS

How big a problem is this? By any measure, it is enormous. In terms of scale, rate of change, novelty, and lack of theoretical and practical tools for understanding it and dealing with it, it makes the idea of a "wicked problem" seem trivial [25]. The magnitude of the problem, however, should provide clues as to how to address it.

China's aims are audacious, unprecedentedly vast, and, as mentioned earlier, it is not the only player engaging in these problematic enterprises. Yet what would deter them? While the use of systems that are at odds with democracy and human rights generally seems to be increasing, the ability of various players within China and on the broader world stage to address the situation in China seems to be out of reach. Commentators such as Andrew Chien, writing in *Communications of the ACM* recently, shared that view: "Scenes of the violent assault of HK Polytechnic University and suppression of all HK opposition press have extinguished any hope China might evolve to tolerate diverse political thought and multiparty politics" [26]. President Xi strengthened that view speaking at the CCP Centenary in July 2021, stating that "foreign forces" that attempted to interfere in China's internal affairs would see "heads bashed bloody against a Great Wall of steel" [27].

China's influence on the world, of course, is outsized. Its population, gross national product, and environmental impact are enormous. China has been selling surveillance technology to countries all around the world, including some of least democratic: Zimbabwe, Egypt, Sri Lanka, Myanmar, Cambodia, Kenya, Nigeria, the Philippines, Malaysia, and Venezuela [28]. Also, at the same time that China's surveillance technology is spreading, its intentional geopolitical influence is growing, for example, through its Belt and Road Initiative, a global infrastructure development strategy to invest in nearly 70 countries and international organizations [29]. Often, this includes telecommunications infrastructure, which opens up opportunities for Chinese intelligence gathering [28]. The Chinese government is also, of course, largely out of reach. The levers of influence are unknown and uncertain for insiders and outsiders alike.

While China's approach to censoring social media has been called "the largest selective suppression of human communication in the recorded history of any country" [23], it is, in fact, the entire antidemocratic trajectory (of which censorship of social media is just one part) that needs consideration. Contrary to the idea that China will become more democratic is the idea implicit in the call for papers that China is building the largest, if not the first, *algocracy*, government by algorithm, in the world. (The fact that the system will undoubtedly not operate with precision and will be plagued with bugs, as well as false negatives and false positives, only compounds the problems.)

Any advancement in technology that furthers democratization in China is welcome. This could be demonstrated in many ways, including more transparency, support for independent media and judiciary, and free and fair elections. An important factor, often not mentioned, is the desire and will of people, specifically the Chinese citizenry and members of the Chinese government, to achieve those factors. Currently, the Chinese government is set on a path to prevent any of these factors from occurring and is working to dilute their development in its citizenry.

Invoking destiny or "emergence" when it comes to democratization or other types of positive social change is not a valid explanation. Fundamentally, social change depends on actual human actors and what they do with the cards they have been dealt. Although individuals can make a tremendous difference, it will come down to their collective efficacy for change to occur. One counter to the pessimism expressed here is the collective action in Hong Kong for democratization, where large numbers of people were willing to agitate for democracy and had enough of a shared vision that allowed them to become quite well organized very quickly. In the end, however, their efforts were crushed — and, in any case, Hong Kong itself is an anomaly in relation to the rest of China.

9 WHAT IS TO BE DONE?

The magnitude of this breach in human rights clearly calls for reasoned resistance. No one group is capable of developing the monumental response that would be required. However, although the response would need to come from many places, some parties are more obligated to stand up. The community of computer professionals, as the technological core of these abuses, certainly is one such party. In some cases, small groups of computer professionals have made large impacts. Within Google, for example, in August 2018, employees protested Google's work on Dragonfly, a search engine based on China's ongoing censorship of online content, a project that was eventually terminated [30]. While that sort of protest is uncommon in the United States, it seems even less likely within China. It is unclear how intentional, bottom-up change can be furthered within China when all avenues for independent action are closed.

The ability of professional societies to temper these forces is an open question. Quite possibly, their successes would be limited and infrequent. The Division of Information and Electronic Engineering within the Chinese Academy of Engineering is more focused on the production of innovative technological products than examining uses of technology in the social sphere. At the same time, for professional groups such as the ACM, it should be more a matter of *how* rather than *whether*.

The ACM's Code of Ethics and Professional Conduct [31] can be a useful grounding for this work by providing principles of ethical behavior of computer professionals both in diagnosing existing systems and in anticipating abuse in those being designed and deployed. The Code seems to focus on the individual computing professional although it does state that it addresses professionals acting individually and collectively. It is an important document but it does not explicitly address crucial issues relating to the actions of companies, governmental entities, or rogue informal or quasi-governmental groups (such as China's Wolf Warriors). Nor does it address what could or should be done to ensure that those entities act ethically.

One exercise would be to see how the Code in its current form could be extended to address ethical issues as they pertain to collective entities that are almost always the producers and beneficiaries of using computing in unethical ways. One principle, for example, in the Code (Section 1) states that "a computing professional should contribute to society and to human well-being, acknowledging that all people are stakeholders in computing." It specifically stipulates (1.1) that "When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority." The fact that technology is being used to oppress 12 million Uyghurs in China starkly points out this violation. The Code can be interpreted to assert that not only should the Uyghurs not be oppressed but that their concerns should be prioritized, a perspective not likely to be adopted. Also, looking at China's recent attacks on "sissy men," male celebrities that are not perceived as masculine enough, reveals that other groups besides ethnic minorities can become subject to discrimination. If that new practice becomes embedded digitally — for example, finding earrings on male celebrities via facial recognition software — it would be a clear violation of the Code.

While the Chinese government appears to violate many of the ACM principles, 3.7 is especially pertinent: "Recognize and take special care of systems that become integrated into the infrastructure of society." These systems, of course, are intended to be integrated into the infrastructure in unprecedented ways, both in breadth of people affected and to the depth of the integration into people's lives. Likewise, Section 2.5 in the Code states the obligation to "Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks." This appears to have been violated, although these calculations may easily have been done under secrecy, using a definition of risk that might not pass United Nations human rights criteria.

The ACM, of course, does not have the authority or resources to enforce ethical guidelines. The ACM does have the limited but critical responsibility to raise the alarm and, somewhat paradoxically, provide opportunities for critics of computing in society to make their voices heard. The ACM and other professional societies must establish clear norms upon which policy can be enacted that they must abide by even in the face of opposition from powerful state and commercial entities. The association also, in my opinion, has the responsibility to help with public education, especially about the role that computers play in society — and not just for budding computer scientists. Also, lest I seem unduly pessimistic about the future, I suggest that the ACM help sponsor broad prizes for social innovation — not only in technical research — and encourage and support civic technology, anticipatory education, citizen science, and the like, plus help develop and support broad opportunities for careers in the application of computers for the public good.

10 CONCLUSIONS

Many of the trends we see in China are unsettling. Here are three implications that directly threaten the idea and the realization of democracy, not just in China but also on a global scale. The first is that the Chinese people are being prevented by their government from taking part in any governance on important issues of concern. This diminishes their civic intelligence and, likely, their ability to participate effectively if and when democratic opportunities arise. (However, we can also be surprised in this regard when resilience and resistance arise in unlikely and precarious situations.) The second is that the technology that the Chinese government is developing (and they are not the only ones) will continue to be used in other settings by other authoritarian governments. This makes democracy less likely worldwide, leaving the world a more dangerous and capricious place. The third is that this race towards a ubiquitous super-surveillance dystopia is not only an abysmal goal but a tremendous waste of human resources. This casts the whole human experiment in a very dim light.

One of the more inconvenient fruits of our labor as computer professionals is enabling oppression at scale. Computing is at the core of some of the world's most inhumane systems and advanced technology, including mass surveillance and recognition systems that promise less transparency as well as the wholesale removal of human oversight from a complex web of automated decision-making that comprise all of the components of a governmental system.

At some point, especially considering the spread of these oppressive systems, it might not matter who is directing them, whether it is the Chinese government, other large countries, tech behemoths, renegade hacker bands, or AI bots adrift in the Internet of Things. The panoply of technology that can be used to degrade democracy is awesome. It certainly demonstrates a concerted degree of creativity and intelligence as well as a seemingly unquenchable thirst for power at the top and, at all levels, a certain ethical ambiguity when money is at stake.

The preamble of the ACM's Code of Ethics and Professional Conduct begins with a truism: "Computing professionals' actions change the world." These changes, many of which are quite ominous, are more apparent with each passing day. As the group most responsible for the development and deployment of technology, both for good purposes and bad, and as the group with the most thorough understanding of the technology, computer professionals have critical roles to play in relation to software systems, especially those with potential for great harm. Much damage has been done already. Because the processes that have caused the damage have been institutionalized, we expect more damage as time goes on. Computer professionals must acknowledge that their work has consequences and that they, too, are members of the larger community. This means encouraging public understanding of these systems, both for good and bad, and taking part in discussing and developing new options for moving forward. While this commentary focuses on China, systems that enrich the already powerful at the expense of the less powerful are being rolled out worldwide at an alarming pace.

The hopes that we may have for our vexing species rest on the possibility that we might against all odds face up to the reality of our challenges and the necessity of living together. This would in all likelihood mean pressuring powerful well-resourced governments and corporations (as well as less powerful and less well-resourced entities) to play significant — and intentionally positive — roles in climate change mediation, environmental protection, mutual assistance, and education, for example. It also would mean mounting a rigorous and dedicated defense and reimagining of democracy. Ideally, democracy is the arena in which we collectively have the potential to do the right thing. However, democracy also requires rules that can prevent overreach of the most powerful. It means a broad commitment to the common good.

Although I am not speaking on behalf of SIGCAS, the ACM's Special Interest Group on Computers and Society, as Chair I am obligated to formally protest the development of the largest system of social control the world has ever known. The ACM should advance computing as a science and a profession, not as an engine of oppression.

REFERENCES

[1] ——. 2021. Call for papers. *ACM DGOV. Undated.* Retrieved October 19, 2022 from https://dl.acm.org/pb-assets/Special%20Issue%20on%20New%20Trends%20of%20Building%20Digital%20Government%20in%20China-v3-1619536933927.pdf.

[2] Douglas Schuler. 2020. Can technology support democracy? *Digital Government: Research and Practice* 1, 1 (2020), 1–14. https://doi.org/10.1145/3352462

[3] Yascha Mounk. 2021. Democracy on the Defense: Turning Back the Authoritarian Tide. *Foreign Affairs.* 100, 163. https://www.foreignaffairs.c,7om/articles/united-states/2021-02-16/democracy-defense.

[4] Helen Davidson. 2021. Hong Kong's Apple Daily, symbol of pro-democracy movement, to close. *The Guardian*. 2021. Retrieved October 19, 2022 from https://www.theguardian.com/world/2021/jun/23/hong-kong-apple-daily-symbol-of-pro-democracy-movement-to-close.

[5] ——. 2021. National security law: Hong Kong rounds up 53 pro-democracy activists. *BBC News*. January 6, 2021. Retrieved October 19, 2022 from https://www.bbc.com/news/world-asia-china-55555299.

[6] Stephen McDonell. 2017. Why China censors banned Winnie the Pooh. *BBC News*, Beijing. July 17, 2017. Retrieved October 19, 2022 from https://www.bbc.com/news/blogs-china-blog-40627855.

[7] Brenda Goh. 2021. Three hours a week: Play time's over for China's young video gamers. *Reuters*. August 31, 2021. Retrieved October 19, 2022 from https://www.reuters.com/world/china/china-rolls-out-new-rules-minors-online-gaming-xinhua-2021-08-30/.

[8] Lily Kuo. 2021. Xi Jinping's crackdown on everything is remaking Chinese society. *New York Times*. September 9, 2021. Retrieved October 19, 2022 from https://www.washingtonpost.com/world/asia_pacific/china-crackdown-tech-celebrities-xi/2021/09/09/b4c2409c-0c66-11ec-a7c8-61bb7b3bf628_story.html.

[9] Elizabeth Economy. 2022. Xi Jinping's New World Order: Can China Remake the International System? *Foreign Affairs*. 101, 52.

[10] Ronald Deibert. 2019. The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy*. 30, 1 (2019), 53–67.

[11] Scilla Alecci. 2020. Uighur repression 'turbocharged by technology,' confidential documents show. *International Consortium of Independent Journalists*. December 14, 2020. Retrieved October 19, 2022 from https://www.icij.org/investigations/china-cables/uighur-repression-turbocharged-by-technology-confidential-documents-show/.

[12] ——. 2021. Who are the Uyghurs and why is China being accused of genocide? BBC News. June 21, 2021. Retrieved October 19, 2022 from https://www.bbc.com/news/world-asia-china-22278037.

[13] ——. 2018. "Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims. *Human Rights Watch*. September 9, 2018. Retrieved October 19, 2022 from https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

[14] ——. 2017. "China: Minority Region Collects DNA from Millions," *Human Rights Watch*. December 13, 2017. Retrieved October 19, 2022 from https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions. Cited in [12].

[15] Dennis Normile. 2021. Genetic papers containing data from China's ethnic minorities draw fire. *Science*. 373, 6556 (2021), 727–728. Retrieved October 19, 2022 from https://www.science.org/content/article/genetic-papers-containing-data-china-s-ethnic-minorities-draw-fire.

[16] Tony Roberts. 2021. State surveillance of citizens reaches far beyond Pegasus. *Institute for Development Studies*. July 23, 2021. Retrieved October 19, 2022 from https://www.ids.ac.uk/opinions/state-surveillance-of-citizens-reaches-far-beyond-pegasus/.

[17] Lily Kuo. 2019. China brings in mandatory facial recognition for mobile phone users. *The Guardian*. December 2, 2019. Retrieved October 19, 2022 from https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users.

[18] Ben Halder. 2018. China Turns to Robotic Policing. *Ozy*. May 30, 2018. https://www.ozy.com/around-the-world/china-turns-to-robotic-policing/86559/.

[19] Keith Bradsher and Steven Lee Myers. 2021. Ahead of Biden's Democracy Summit, China Says: We're Also a Democracy. *New York Times*. Dec. 7, 2021. Retrieved October 19, 2022 from https://www.nytimes.com/2021/12/07/world/asia/china-biden-democracy-summit.html.

[20] ——. 2021. Full Text: China: A Democracy that Works. *The State Council Information Office of the People's Republic of China*. December 4, 2021. Retrieved October 19, 2022 from http://www.news.cn/english/2021-12/04/c_1310351231.htm.

[21] Giavanna O'Connell. 2020. How China is Violating Human Rights Treaties and Iits Oown Constitution in Xinjiang. *Just Security*. August 19, 2020. Retrieved October 19, 2022 from https://www.justsecurity.org/72074/how-china-is-violating-human-rights-treaties-and-its-own-constitution-in-xinjiang/.

[22] Douglas Schuler. 2001. Cultivating society's civic intelligence: Patterns for a new 'world brain'. *Inf. Commun. Soc. Information, Communication & Society* 4, 2 (2001), 157–181.

[23] Gary King, Jennifer Pan, Margaret E. Roberts. 2014. Reverse-engineering censorship in China: Randomized experimentation and participant observation. *Science*. August 22, 2014.

[24] Li Yuan. 2022. How China Embraces Russian Propaganda and Its Version of the War. *New York Times*. March 4, 2022. Retrieved October 19, 2022 from https://www.nytimes.com/2022/03/04/business/china-russia-ukraine-disinformation.html.

[25] Douglas Schuler. 2021. On Beyond Wicked: Exploring the Uses of "Wicked Problems." Douglas Schuler. Workshop on Computing within Limits. Retrieved October 19, 2022 from https://computingwithinlimits.org/2021/papers/limits21-schuler.pdf.

[26] Andrew A. Chien. 2022. Is the Global Computing Community Irrevocably Divided? *Communications of the ACM* 65, 1, Page 5. https://m-cacm.acm.org/magazines/2021/1/249440-2021-computings-divided-future/fulltext.

[27] David Crawshaw and Alicia Chen. 2021. 'Heads bashed bloody': China's Xi marks Communist Party centenary with strong words for adversaries. *Washington Post*. July 1, 2021. Retrieved October 19, 2022 from https://www.washingtonpost.com/world/asia_pacific/china-party-heads-bashed-xi/2021/07/01/277c8f0c-da3f-11eb-8c87-ad6f27918c78_story.html.

[28] Adrian Shahbaz. 2018. The Rise of Digital Authoritarianism. *Freedom House*. Retrieved October 19, 2022 from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[29] Wikipedia. Belt and Road. Retrieved October 1, 2021 from https://en.wikipedia.org/wiki/Belt_and_Road_Initiative.

[30] Caroline O'Donovan. 2018. Google employees are organizing to protest the company's secret, censored search engine for China. *Buzzfeed News*. August 17, 2018. Retrieved October 19, 2022 from https://www.buzzfeednews.com/article/carolineodonovan/google-dragonfly-maven-employee-protest-demands.

[31] ACM Code 2018 Task Force. 2018. ACM Code of Ethics. Association for Computing Machinery. June 22, 2018. Retrieved October 19, 2022 from https://www.acm.org/code-of-ethics.

Received 3 November 2021; revised 8 March 2022; accepted 13 October 2022