中国人权
HRIC
HUMAN RIGHTS IN CHINA

Between a Rock and a Hard Place: Human Rights Defenders in China

By Sharon Hom

An edited and expanded version of the remarks delivered at the
22nd EU-NGO Human Rights Forum: The Impact of New Technologies on Human Rights
("Setting the Scene" panel) December 9, 2020[1]

Sharon Hom, Executive Director, HRIC

E-Mail: Sharon.hom@hrichina.org
Website: https://www.hrichina.org

Introduction

Thank you to the European Commission, the European External Action Service (EEAS), and the Human Rights & Democracy Network (HRDN) for this opportunity to participate in this year's EU-NGO Forum on The Impact of New Technologies on Human Rights.[2] It is an honor to follow the high- level speakers—and it is very encouraging to hear the strong affirmation of the EU's ongoing commitment to supporting defenders on the frontlines. For the human rights defenders, civil society groups, and activists round the world, especially those in China, I hope this official demonstration of solidarity will give you hope. And though this expression is now banned in Hong Kong, like many others, I want to say: "Ga Yau," "add oil"!

On the eve of International Human Rights Day, this year's Forum is taking place at a particularly critical time for the international human rights system. As we celebrate the 75th anniversary of the founding of the United Nations, the international human rights system continues to evolve amid complex debates, in particular, regarding treaty body mechanisms, special procedures, and the participation of civil society. In the face of efforts to undermine and replace international standards and norms (led by China and other rights-restricting states), what is at stake is the integrity and effectiveness of a key normative platform and set of tools for human rights defenders.

The growing speed, scope, and depth of technological developments inevitably outstrip what our laws, our regulations, our ethical development, and our cultural norms can meaningfully and effectively grapple with.

Since the end of 2019, COVID-19 has been used as *the* health emergency rationale to restrict rights. China recently has published a position paper on a post-COVID-19 world order including proposals for 5G and data security.[3] These are important trends that we're seeing that are both using *and* exploiting COVID-19. As the world grapples with COVID-19, the largest and most serious global pandemic since last century, we cannot yet talk about "after" COVID-19, because we are still in the middle of it. Although there will be an "after" to the "now," I don't think any of us can expect a return to any kind of pre-COVID "normalcy," given the impact on millions of people around the world, on every sector, and on the way we work, study, and connect.[4]

Technology has played a key role in our adjustments in the COVID era, with both empowering and also negative impacts, the "dark side," as referenced by a number of the previous speakers. Governments, civil society groups, and individuals have all *ramped up their use of technology* and digital security tools. The growing speed, scope, and depth of technological developments inevitably outstrip what our laws, our regulations, our ethical development, and our cultural norms can meaningfully and effectively grapple with. Our technological future is indeed happening faster than we think,[5] and, in fact, what we thought was "new" technology may already be receding into technology-time history as we struggle to comprehend the extent and impact of algorithmic control over our lives. Even the builders of this brave new world of AI, big data, and enhanced biometric surveillance don't really fully understand what their powerful machines and algorithms are learning and what the full social impacts will or might be.[6]

(Clockwise from upper left: Heidi Hautala, VP, European Parliament; Sharon Hom; Giuseppe Abbamonte, Director for Media Policy, European Commission; Michael O'Flaherty, Director, European Union Agency for Fundamental Rights (FRA); Marie Arena, MEP and Chair of the EP Subcommittee on Human Rights; Jennifer Baker, panel moderator.)

The "Rock": Challenges Posed by an Authoritarian State

For more than three decades, my organization, Human Rights in China, has been working to support defenders and address the steep challenges that civil society faces in China—one of the most economically and politically powerful and influential state actors in the world. In her remarks during the High level panel, Alice Mogwe, President of the International Federation for Human Rights (FIDH), highlighted the detrimental impact of China's security policies, its deployment of AI , its extensive use of facial recognition cameras and predictive analytics, and their serious impacts on the peaceful exercise of rights by ethnic groups and human rights defenders—in fact, by all of China's 1.4 billion people.[7]

The party-state in China is deploying these technologies supported by a national security-cyber security-legal regime, a powerful police security apparatus, and a comprehensive and systematic ideology-enforcement machine that compels correct behavior and thinking (read Xi Jinping thought[8]) and loyalty to the Communist Party of China.[9] The online community is under all-encompassing electronic surveillance that is designed to ensure that citizens stay "trustworthy."[10] In addition, a national social credit system helps to incentivize desired social behavior.[11]

The authoritarian regime in China is not only weaponizing these new technologies and digital tools to target civil society and human rights defenders and to carry out targeted and massive surveillance and censorship—it is exporting its digital authoritarianism model, including through major infrastructure projects in the Belt and Road Initiative and along the Digital Silk Road.

The authoritarian regime in China is not only weaponizing these new technologies and digital tools to target civil society and human rights defenders and to carry out targeted and massive surveillance and censorship—it is exporting its digital authoritarianism model, including through major infrastructure projects in the Belt and Road Initiative and along the Digital Silk Road.[12] The demand for Chinese surveillance exports, unfortunately, continues to grow,[13] which growth also fuels market competition to provide surveillance technology. For EU member states and other Western democratic governments, there's always tension between economic and strategic interests on the one hand, and risks presented by exporting this technology, on the other, risks including rights-related impacts of end use products or dual-use technology.

In line with the China Dream to restore the nation to its rightful place in the world,[14] China has also announced quite transparently its ambitious goals and policies to be the global leader in the development of digital technologies, including AI, quantum computing, robotics, biometric surveillance, and other disruptive technologies.[15] China is also increasingly active in cyber governance and standard setting,[16] such as assuming leading positions in multilateral institutions, including those addressing Internet governance, technical standards setting, human rights, cyber security, and counter terrorism. China's state champions in the technology sector, the BAT (Baidu, Alibaba, Tencent), are also shaping the global digital architecture, and Chinese engineers are actively contributing to the development of new technical standards.[17]

In light of the focus of Western governments and business on privacy challenges in cyberspace, I want to point out the importance of distinguishing norm, context, and implementation practice. China's domestic laws in particular, the *Cybersecurity Law*[18] and implementing regulations, incorporate the language of international privacy norms, even including *General Data Protection Regulation* (GDPR) language, such as principles of informed consent, disclosure, and the scope of the information collected and subsequent use, and the principle of data minimization.[19] However, despite these formal normative provisions, these legal provisions need to be understood within the context of a regime that rejects rule of law and international human rights standards as ”Western concepts” inappropriate for China’s national conditions (*guoqing*).[20]

During the massive 2019 social protests in Hong Kong, the frontline activists and ordinary citizens used social media to mobilize, organize or participate in actions. With the help of technologists, they built online platforms for public opinion polling and primary elections, and used digital tools to document and raise awareness of the rampant misuse of violence by law enforcement.

Formal privacy protections need to also be viewed within the context of the Internet legal regime in China, in particular, the legal restrictions on the use of encrypted tools[21] and real name requirements,[22] both key to ensuring privacy and anonymity. In addition, the *Cybersecurity Law* requires mandatory local storage of data collected in China and approval before transmission of data abroad. For example, companies have to show a legitimate business purpose for transmitting those data.[23]

At the same time, while China is using these digital tools to target and censor, activists are also using the digital tools to mobilize, organize, protest, or take other social actions. LGBT activists, feminist activists, and legal advocates on the mainland have used and continue to use social media platforms to raise awareness of domestic violence, sexual harassment, gender discrimination, and attacks on lawyers and citizen journalists.[24] During the massive 2019 social protests in Hong Kong, the frontline activists and ordinary citizens used social media to mobilize, organize or participate in actions. With the help of technologists, they built online platforms for public opinion polling and primary elections, and used digital tools to document and raise awareness of the rampant misuse of violence by law enforcement. And digital tools were critical to countering the powerful alternative, fact-adverse Beijing narratives that were propagated so effectively to the international community by state-controlled media outlets. Yet, despite the resourcefulness of these activists, the arrests and harassment of peaceful protesters, along with the attack on the electoral system, in Hong Kong continue.[25] And the expansion of technological surveillance and monitoring tools—which are employed to support ongoing state repression of peaceful exercise of rights—heightened and created new risks for rights defenders and civil society actions.

And digital tools were critical to countering the powerful alternative, fact-adverse Beijing narratives that were propagated so effectively to the international community by state-controlled media outlets.

The “Hard Place”: Challenges Posed by Silicon Valley[26]

The misuse of technology that Marie Arena and Alice Mogwe have already signaled may not just be a problem of misuse of the technology by bad actors; it could also be misuse by design. In other words, it’s not just the dark side of the technology—it is a part of the design of the proprietary disruptive social media technologies.

In comparison to the Chinese digital authoritarian model, I want to add another layer to the references to the dominant business model that has already been signaled as presenting rights problem related to privacy and data collection, aggregation, and use. The misuse of technology that Marie Arena and Alice Mogwe have already signaled may not just be a problem of *misuse* of the technology by bad actors, it could also be *misuse by design*. In other words;it’s not just the *dark side* of the technology—it is a *part of the design* of the proprietary disruptive social media technologies. As Adrienne La France, executive editor of the *Atlantic*, underscores: “Today’s social networks, Facebook chief among them, were built to encourage the things that make them so harmful. It is in their very architecture."[27] In fact, a growing number of former Silicon Valley “princelings” have been speaking out, sharing their sobering reflections and disowning the consequences and impacts of what they built, if not what they built.[28]

Jaron Lanier, co-founder of virtual reality, computer engineer, and musician, has vociferously urged users to delete their social media accounts or, at the very least, stop using them in order to create space to explore other ways to connect with others and to (re)discover one’s autonomy. Ex-Googler Tristan Harris warns how technology hijacks people’s minds. They are both focusing on what Lanier terms BUMMER, the dominant business model of these giant technology companies: the “behaviors of users modified and made into an empire for rent.”[29] Neuroscience researchers have sounded the alarm of the algorithmic-induced addiction to social media that serves the goals of BUMMER—more growth and more engagement and clicks, then more revenue. Some critics have also pointed out that the term “users” is really only used in two industry sectors: drugs and the Internet.[30] It is interesting that developers of social media platforms or tools, when asked if their children were allowed to use these tools, responded that no, at least not until they were no longer children or teenagers. I think that should give us pause.[31]

However, I am not proposing a Luddite argument to the stop use of all new technologies, or arguing that these giant technology companies have not also made good contributions to expanding space for freedom of expression or access to more information. But as Yuval Noah Harari puts it, “[s]ince the corporations and entrepreneurs who lead the technological revolution naturally sing the praises of their creations, it falls to sociologists, philosophers, and historians . . . to sound the alarm and explain all the ways things can go terribly wrong.” I would add that it falls to human rights scholars, activists, policymakers, and all of us to exercise critical vigilance to examine the development, use, and impact of these technologies, and reimagine other more rights-empowering models.

Between a Rock and a Hard Place

With Mark Zuckerberg’s 2017 “Manifesto,” Facebook launched a massive experiment in social engineering to create an online connected community that has now grown to include over 1.69 billion Facebook users, all interacting online with an illusion of choice and autonomy. The vast amounts of data willingly given up and the algorithmic manipulation of behavior based on this data *are* the enormously profitable products being sold. But this online “community” is also plagued by misinformation, fake news, cyber bullying and trolling, conspiracy theories, and echo chambers amplifying and spreading all of this.

At the same time, the digital authoritarianism experiment underway in China is exercising control over 1.4 billion people, with over 800 million online. Instead of monetizing the enormous data collected via a comprehensive surveillance system, the authorities are deploying technological tools of surveillance to ensure the party-state’s ideological and social control. In addition to official control of expression online that contributes to self-censorship, there are also the water armies *(shuijun*), who flood the Internet with nationalistic views or manufactured views, and the online wolf warriors who engage in savage trolling and cyberbullying.

Both these models and social experiments present threats to democracy and to human dignity and autonomy, which are at the heart of human rights. Human rights defenders, as well as all users of social media or technology tools, are therefore trapped between a rock and a hard place—between the manipulation for profit of “surveillance capitalism”[32] and the economic and political constraints of party-state authoritarianism.

Human rights defenders, as well as all users of social media or technology tools, are trapped between a rock and a hard place—between the manipulation for profit of “surveillance capitalism” and the economic and political constraints of party-state authoritarianism.

In addition to the global challenges of equitable access and connectivity to the Internet and the threats of disinformation and so forth, there is a deeper existential threat presented by these two powerful universes, these powerful centers of technological gravity—that we can think of

There is a deeper existential threat presented by these two powerful centers of technological gravity—that we can think of as black holes. One black hole is sucking vast amounts of data about us, data that are disappearing into the "siren servers," the gargantuan cloud computing servers that serve concentrated Silicon Valley power and wealth. And the other black hole serves an authoritarian party-state.

as black holes. One black hole is sucking vast amounts of data about us, data that are disappearing into the "siren servers," the gargantuan cloud computing servers that serve concentrated Silicon Valley power and wealth.[33] And the other black hole serves an authoritarian party-state.

For those netizens outside the Great Firewall and those defenders in mainland China, who manage with great effort to climb over the Great Firewall, what kind of online community or communities do they log on to? Is it an uncensored free Internet? Or is it another online space with new echo chambers, flooded by an onslaught of more fake news, fake personas, disinformation, and conspiracy theories?[34] As highlighted already by the other speakers and the concept notes for the Forum, these are serious complex issues that require critical examination, creative approaches, and political will on the part of key stakeholders.[35]

So, What's to be Done?

Despite extensive and mounting international attention, serious human rights abuses and practices continue in China, including the forced incarceration and surveillance of millions of Uighurs,[36] repression of cultural and religious expression in Tibet, and attacks on lawyers, rights defenders, and journalists.[37] Hong Kong remains a frontline of human rights defense—and a test of China's respect for and compliance with its international obligations. The immediate and serious impacts of the sweeping *National Security Law* in Hong Kong, widely- and deeply-felt, include heavy police presence in public spaces, intimidation, harassment, and repression of group gatherings; and censorship and self-censorship both offline and online. The threat of criminal prosecution is now reaching beyond China's borders, chilling expression and academic freedom and inducing self-censorship.

While the human rights challenges remain daunting, there may now be growing political will to engage with China more effectively to protect human rights. The awareness of the deadly consequences of information control and censorship that contributed to the spread of the COVID-19 outbreak is also contributing to a *changing and increasingly negative perception of China in the international community* as reflected in a new 14-country Pew Research Center survey (October 2020).[38] Certainly, the shift in opinion about China and pushback against its influence abroad are not helpful to advancing China's ambitions to be a respected global leader. Perhaps the shifting geo-political fault lines can be leveraged as a constructive opening to move beyond engagement as usual.

As other Forum speakers have already highlighted, there may be an increasing realization beyond rhetoric that security, trade, and sustainable environment are interrelated, and effective policies must be developed within a human rights framework. First, beyond being addressed in siloed policy debates, human rights need to be at the forefront of and integrated into the totality of bilateral relations. As HRIC points out in our White Paper: “Too Soon To Concede The Future**,”** the *National Security Law* itself states that fundamental rights and freedoms must be protected, including those “under the Basic Law . . . and the provisions of the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights as applied to Hong Kong” (Art. 4), and requires adherence to the rule of law (Art. 5).[39] Cynical dismissals of these rights provisions that cite China’s lack of a rule of law miss critical opportunities and strategies to advance policies and interventions that might contribute to stronger defense of individual cases as well as needed legislative and systemic reforms.

But across a fast-moving present, is humane technology possible? How can we re-center human dignity and autonomy and choice in a meaningful way? What other business models might be explored? The Center for Human Technologies, set up by several of the former Silicon Valley tech developers and experts, is focusing on public education to raise awareness of the risks and harms of these technologies, supporting changes in the industry culture and informing policy choices.[40] But at the end of the day, should we continue to allow the private sector—the technology giants—to control the paradigm and dominate the way we think about the technology?

Each of us, in different capacities, needs to critically examine our relationship to, our use of, and the impact of new technologies, especially social media, and explore other ways of connecting, community building, and exercising our rights in meaningful, authentic ways.

We need to look beyond the narrow demographic of the former Silicon Valley princelings, and the *mea culpa* in hindsight, to support and empower a greater diversity of stakeholders. At the same time, a more inclusive coming-to-the-table of stakeholders is just a beginning. We need to also recognize that civil society, NGOs, and human rights defenders do not come to the table, any table, with equal economic, political, and discursive power. How do we include stakeholders not beholden to shareholder profit pressure at the policy table in a robust way? For example, how can the role and function of the open-source technology community be expanded and deepened? More systematic inclusion of the open source community would highlight the potential effectiveness of expanded and more stringent regulatory approaches, since giant tech companies can simply absorb the cost of regulation as part of doing business.

How can we integrate the expertise and insights of developers actively working as part of an Internet Freedom technology community? While still a community in progress (including developers, NGOs, and capacity builders), the IF community has adopted an approach based on a critical premise: the effective use of technology to promote and protect rights must be *by design*. The needs and perspectives of the users need to be integrated throughout the different stages in the process, including needs assessment, design, implementation, audits, evaluation and subsequent iterations of the technology solutions, tools, and approaches.

Finally, each of us, in different capacities, needs to critically examine our relationship to, our use of, and the impact of new technologies, especially social media, and explore other ways of connecting, community building, and exercising our rights in meaningful, authentic ways. As LaFrance urges: it's still not too late to repair the aspects of our society and culture that the social web has badly damaged.[41]

And One More Thing . . .

Since there were references to cats and cat memes earlier by other speakers, a word about cats. As everyone knows, cat memes dominate the Internet. A Google search of cat memes, produces 370,000 results in .53 seconds. Jaron Lanier begins his *Ten Arguments for Deleting your Social Media Accounts Right Now* this way: "Let's start with cats." After extolling the intelligence and independence of our feline companions, he suggests that "[c]ats on the Internet are our hopes and dreams for the future of people on the Internet." Hence, his book is about "how to be a cat," that is, how to remain autonomous in a world of constant surveillance and manipulation by algorithms "run by some of the richest corporations in history."[42] Indeed, with the hundreds of thousands of cat memes online, we will still never domesticate cats and own their narrative. As the fulltime caretaker of 13 rescued cats, I couldn't agree more. Let's learn to be cats online.

[1] For information on the Forum, see https://eu-ngo-forum.b2match.io/home; video (1:08:39-1:28:03; 2:01:35-2:04:49; 2:09:49-2:12:55; 2:22:03-2:22:56): https://eu-ngo-forum.b2match.io/page-381.The panel was moderated by Jennifer Baker. Other panelists, in order of speaking were: Giuseppe Abbamonte, Director for Media Policy, Directorate General for Communications Networks, Content and Technology, European Commission; Michael O'Flaherty, Director of the European Union Agency for Fundamental Rights (FRA); Marie Arena, Member of the European Parliament and Chair of the EP Subcommittee on Human Rights; Eliska Pirkova, Europe Policy Analyst, Access Now; and Heidi Hautala, Vice-President, European Parliament.

[2] As described on its homepage, https://eu-ngo-forum.b2match.io/: "[t]he EU-NGO Human Rights Forum will provide an essential platform to elaborate recommendations on how the EU can further foster human rights compliance in the digital sphere and seize the potential of new technologies to promote the protection of human rights for all. It will also represent an opportunity to create or strengthen international multistakeholder networks."

[3] "China Publishes Position Paper of the People's Republic of China On the 75th Anniversary of the United Nations," Ministry of Foreign Affairs of the People's Republic of China, September 10, 2020, https://www.fmprc.gov.cn/mfa_eng/wjbxw/t1814034.shtml; and "Global Initiative on Data Security," Ministry of Foreign Affairs of the People's Republic of China, September 8, 2020, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml.

[4] However, while the rest of the world suffers enormous human costs, China's tech giants and CEOs in a range of sectors have been doing really well during the year of COVID-19. Thanks to the pandemic, China's e-commerce, health care industries, food delivery services, vaccine developers, and PPE producers contributed to enormous increase in personal wealth. As recently reported in *Forbes*, the top 400 richest individuals in China include: Jack Ma, Alibaba founder (net worth $65.6 billion); Pony Ma, CEO of Tencent, (net worth $55.2 billion), and Wang Xing, CEO of Meituan-Dianping, a home delivery service (net worth $22.5 billion, after a quadruple increase during COVID-19). Russell Flannery, "China's 400 Richest 2020: Total Wealth Surges Amid Pandemic," *Forbes*, November 4, 2020, https://www.forbes.com/sites/russellflannery/2020/11/04/chinas-400-richest-2020--total-wealth-surges-amid-pandemic/?sh=749688db3d7a.

[5] See Diamandis, Peter H. and Kotler, Steven, *The Future Is Faster Than You Think: How Converging Technologies Are Transforming Business, Industries, and Our Lives*, Simon & Schuster Paperbacks, 2020. The convergence of independent lines of accelerating technology (e.g. AI) with other lines of technology (e,g, augmented reality) at an ever-increasing rate has turbo-boosted both the rate and scale of major transformations across all fields.

[6] AI programs are even learning beyond human capacity or guidance. Yuval Harari cites an example of Google's AlphaZero that used the latest machine learning principles to self-learn chess by playing against itself. It won twenty-eight games and tied seventy-two against the champion program, Stockfish8. "AlphaZero went from utter ignorance to creative mastery in four hours, without the help of any human guide." Harari, Yuval, 21 Lessons for the 21st Century, *Vintage*, 2019, p.44.

[7] EU-NGO Forum 2020, Plenary opening session (Alice Mogwe from 21:00 to 28:28), December 9, 2020, https://eu-ngo-forum.b2match.io/page-381. HRIC has been an active member of the FIDH for decades and appreciates Alice Mogwe for highlighting the China challenges in her high-level remarks.

[8] Xi Jinping Thought on Socialism with Chinese characteristics for a New Era, now enshrined in the State and Party Constitutions of China. Constitution of the Communist Party of China, October 24, 2017, http://www.xinhuanet.com//english/download/Constitution_of_the_Communist_Party_of_China.pdf.

[9] Ideological requirements also appear in multiple laws, including the National Security Law, the Cybersecurity Law, for example, Art. 6 of the Cybersecurity Law requires the state to promote "honest, healthy and civilized network conduct…[and] dissemination of core Socialist values." (Emphasis added.) 中华人民共和国网络安全法 (*Cybersecurity Law*), Cyberspace Administration of China, November 7, 2016, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm. Art. 13 of the Internet News Information Service Management regulations require that internet news services should persist in the direction of serving the people and serving Socialism, persist in the orientation *of correct public opinion*, play the role of public opinion supervisor, …" (Emphasis added.) Regulations on Administration of Internet News Information Services, The Press Office of the State Council and Ministry of Information Industry, September 25, 2005, https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn345en.pdf.

[10] Internet service providers are required to build user credit systems and provide different access to services and functions based upon user credit. For example, In the Post and Comment Provisions, Art. 9 service providers are

required to “carry out credit assessments of users’ conduct, “to blacklist “seriously untrustworthy” users and to prohibit users form re-registering once they have been blacklisted. 《互联网跟帖评论服务管理规定》Provisions on the Management of Internet Post Comments Services (issued 2017-8-25).

[11] “国务院关于印发社会信用体系建设规划纲要（2014—2020 年）的通知,” The State Council of the People’s Republic of China, (issued June 14, 2014), http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm. According to the *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020)”*[11] (issued June 14, 2014), the goal is “by 2020, basically having established fundamental laws, regulations and standard systems for social credit, basically having completed a credit investigation system covering the entire society with credit information and resource sharing at the basis, basically having completed credit supervision and management systems, having a relatively perfect credit service market system, and giving complete rein to mechanisms to encourage keeping trust and punish breaking trust.”“国务院关于印发社会信用体系建设规划纲要（2014—2020 年）的通知,” The State Council of the People’s Republic of China, (issued June 14, 2014), http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm.

[12] Kristin, Shi-Kupfer, and Mareike, Ohlberg, “China’s Digital Rise: Challenges for Europe,” MERICS, April 8, 2019, https://merics.org/sites/default/files/2020-06/MPOC_No.7_ChinasDigitalRise_web_final_2.pdf.

[13] Cook, Sarah, “China’s Ever-Expanding Surveillance State,” Freedom House, April 30, 2018, https://freedomhouse.org/article/chinas-ever-expanding-surveillance-state.

[14] Roger Creemers, “The Chinese Dream Infuses Socialism with Chinese Characteristics with New Energy,” China Copyright and Media, May 6, 2013, https://chinacopyrightandmedia.wordpress.com/2013/05/06/the-chinese-dream-infuses-socialism-with-chinese-characteristics-with-new-energy/.

[15] “到 2035 年我国将建成文化强国,” The State Council of the People’s Republic of China, November 3, 2020, http://www.gov.cn/zhengce/2020-11/03/content_5557091.htm; “Position Paper of the People's Republic of China On the 75th Anniversary of the United Nations,” Ministry of Foreign Affairs of the People’s Republic of China, September 10, 2020, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1813751.shtml; Stephen Chen, “China claims quantum leap with machine declared a million times greater than Google’s Sycamore,” South China Morning Post, September 11, 2020, https://www.scmp.com/news/china/science/article/3101219/china-claims-quantum-leap-machine-declared-million-times-greater.

[16] But for argument that there is a gap between China’s announced ambitions and the actual progress, see Naomi Wilson, “China Standards 2035 and the Plan for World Domination—Don’t Believe China’s Hype,” Council on Foreign Relations, June 3, 2020, https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype.

[17] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan and Elise Thomas, “Mapping China’s Technology Giants,” Australian Strategic Policy Institute International Cyber Policy Centre, Report No. 15, 2019, https://www.aspi.org.au/report/mapping-chinas-tech-giants.

[18] Cybersecurity Law, op. cit.

[19] ibid, Arts. 40 - 44.

[20] “国务院关于印发社会信用体系建设规划纲要（2014—2020 年）的通知,” The State Council of the People’s Republic of China, June 14, 2014, http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm.

[21] See e.g. MIIT, “Notice of Cleaning Up and regulating the Internet Access Service Market,” Cyberspace Administration of China, January 17, 2017, http://www.cac.gov.cn/2017-01/26/c_1120381529.htm.

[22] Cybersecurity Law, op. cit. Art. 24.

[23] Cybersecurity Law, op. cit. Art. 37.

[24] Shelly Banjo, and Lulu Yilun Chen, “Digital Dissidents Are Fighting China’s Censorship Machine,” *Bloomberg Business*, June 4, 2019, https://www.bloomberg.com/news/articles/2019-06-03/digital-dissidents-are-fighting-china-s-censorship-machine; Leta Hong Fincher, “China’s women movement has not only survived an intense crackdown, it’s grown,” *The Guardian*, March 7, 2019, https://www.theguardian.com/world/commentisfree/2019/mar/07/chinas-womens-movement-has-not-only-survived-an-intense-crackdown-its-grown; Suyin Haynes, “Author Leta Hong Fincher Shows Why the World Should Pay Attention to China’ Feminists,” *TIME*, November 14, 2018, https://time.com/5453927/china-feminist-five-big-brother-leta-hong-fincher-interview/.

[25] See “Dozens arrested during Hong Kong peaceful protest against national security laws,” *The Guardian*, June, 29, 2020, https://www.theguardian.com/world/2020/jun/29/dozens-arrested-during-hong-kong-peaceful-protest-against-national-security-laws; and Tony Cheung , Natalie Wong and Kimmy Chung, “Hong Kong leader delays legislative elections, asks Beijing to resolve legal questions, citing coronavirus pandemic dangers,” *South China Morning Post*, July 31, 2020, https://www.scmp.com/news/hong-kong/politics/article/3095461/hong-kong-legislative-council-elections-be-postponed.

[26] I am using Silicon Valley as short-hand to refer to the giant technology companies based in the U.S. and the enormous concentration of economic power they wield.

[27] Adrienne LaFrance, Facebook is a Doomsday Machine, *The Atlantic*, December 15, 2020, https://www.theatlantic.com/technology/archive/2020/12/facebook-doomsday-machine/617384/.

[28] "The Social Dilemma,” directed by Jeff Orlowski, *Exposure Labs, Argent Pictures and The Space Program*, Netflix, 2020, https://www.netflix.com/title/81254224.

[29] Jaron Lanier, Ten Arguments for Deleting Your Social Media Accounts Right Now, *Henry Holt and Company*, 2018.

[30] "The Social Dilemma,” op. cit.

[31] ibid.

[32] Shoshana Zuboff’s term, see Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, *Profile Books*, 2019.

[33] Ten Arguments for Deleting Your Social Media Accounts Right Now, op. cit.

[34] See Pew Research Centre article that 97% of tweets in the U.S came from 10% of users “National Politics on Twitter: Small Share of U.S. Adults Produce Majority of Tweets,” Pew Research Centre, October 23, 2019, https://www.pewresearch.org/politics/2019/10/23/national-politics-on-twitter-small-share-of-u-s-adults-produce-majority-of-tweets/; and that political debates have become less respectful, less fact-based, substantive, Adrian Shahbaz, “The Rise of Digital Authoritarianism: Fake news, data collection, and the challenge to democracy,” Freedom House, 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[35] EU-NGO Forum 2020, https://eu-ngo-forum.b2match.io/home; and “22nd EU-NGO Human Rights Forum - the impact of new technologies on human rights,” European Union External Action Service, December 11, 2020, https://eeas.europa.eu/headquarters/headquarters-homepage/90483/22nd-eu-ngo-human-rights-forum-impact-new-technologies-human-rights_tr.

[36] See e.g. "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass. Emile Dirks and James Lebold, Genomic Surveillance: Inside China's DNA Dragnet. Australian Strategic Policy Institute, International Cyber Policy Center, Policy Brief, Report No. 34/2020.

[37] "China Puts Rights Lawyers, Families, Under House Arrest on Human Rights Day," Radio Free Asia, December 10, 2020, https://www.rfa.org/english/news/china/arrest-12102020113601.html; "China crackdown on rights lawyers 'shocking': Rights expert," Aljazeera, December 16, 2020, https://www.aljazeera.com/news/2020/12/16/china-crackdown-on-rights-lawyers-shocking-un-expert; and Owen Churchill, "China is global leader in imprisoned journalists for a second consecutive year, watchdog group finds," *South China Morning Post*, December 15, 2020, https://www.scmp.com/news/china/society/article/3113942/china-global-leader-imprisoned-journalists-second-consecutive.

[38] The Pew survey revealed that an unfavorable opinion of China has increased significantly over the past year and that a majority of the people in all the countries surveyed, including Sweden, United Kingdom, Germany, the Netherlands, and the United States now holds a negative view of China. This represents the highest points of unfavourability toward China in more than a decade since the topic has been surveyed. Laura Silver, Kat Devlin, and Christine Huang, "Unfavorable Views of China Reach Historic Highs in Many Countries," Pew Research Center, October 6, 2020, https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/.

[39] "Too Soon to Concede the Future: The Implementation of The National Security Law for Hong Kong--An HRIC White Paper," Human Rights in China, October 16, 2020, https://www.hrichina.org/en/press-work/press-release/too-soon-concede-future-implementation-national-security-law-hong-kong-hric.

[40] The Center for Humane Technologies, https://www.humanetech.com/.

[41] Facebook is a Doomsday Machine, op. cit.

[42] Ten Arguments for Deleting Your Social Media Accounts Right Now, op. cit. p.2