Written Submission from Amnesty International UK (TFP0005)

Technology and the Future of UK Foreign Policy

** This submission focuses on the human rights dimension of technology and some of the measures required to ensure that technology does not undermine human rights with regard to the FCDO's role in promoting the UK's foreign relations and international obligations*

Amnesty International United Kingdom Section
The Human Rights Action Centre, 17-25 New Inn Yard, London EC2A 3EA
Contacts for further information: Peter.Frankental@amnesty.org.uk; or advocacyteam@amnesty.org.uk

www.amnesty.org.uk

Amnesty International UK

Amnesty International UK is a national section of a global movement of over seven million people who campaign for every person to enjoy all rights enshrined in the Universal Declaration of Human Rights and other international human rights standards. We represent more than 670,000 supporters in the United Kingdom. We are independent of any government, political ideology, economic interest or religion.

Summary

1. Recent advances in digital communications technology – and in particular social media and the spread of the smartphone – have revolutionized the practice of human rights. Victims of, and witnesses to, human rights abuses can now document their experiences and share them directly with the world. This information, when verified, can then contribute to broader human rights documentation and accountability mechanisms.[1]

2. New technologies however are also providing governments with increasingly powerful tools to supress dissent, undermine freedom of expression and intimidate human rights defenders. This has led to a convergence of interests between technology companies seeking to expand markets for their products and governments that are either indifferent to the human rights impacts of such technologies or that actively seek to use them to violate human rights. The outcome has been increased levels of harassment faced by individuals and organisations who monitor and expose human rights violations. This is closing down civic space across the world and undermining the capacity of human rights defenders to hold governments accountable for their failure to respect and protect human rights.

3. While governments bear the primary responsibility for allowing such a situation to arise, technology companies are part of the problem. Their business models and strategies are often incompatible with human rights.[2] The influence that FCDO can bring to bear on these companies through its engagement with them is limited because of the extent to which these companies are driven by financial markets. Technology companies may be mindful of the concerns of consumers of their products and other stakeholders, but this is unlikely to lead to the responsible development and use of data and of information technologies. The balance of incentives favours the continuing propagation of human rights abuses by these companies and by the governments who use their products.

4. By the same token, the FCDO's ability to engage with private companies to encourage internationally accepted norms for the use of social media is constrained by the fact that these companies operate transnationally and adopt strategies and business models that are global in their scope and impacts. Such companies are unlikely to be influenced by representations from FCDO except in situations where there is some threat to their commercial interests if they fail to improve their conduct.

[1] See for example Amnesty International's digital verification collaboration with the University of Essex https://www.essex.ac.uk/research-projects/digital-verification-unit and its Citizen Evidence Lab https://citizenevidence.org

[2] https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF

5. What is required is much more effective oversight and regulation of the activities of technology companies to ensure that they conform to international norms in the sphere of human rights. Criminal law and civil law should reflect this to enable offending companies to be held accountable and those harmed to access remedy.

6. There is currently a hiatus at all levels – international, regional and national – in the development and implementation of rules and regulations relating to the human rights impacts of information technologies. Governments are reluctant to act against the interests of companies domiciled within their jurisdiction if such action would put them at a competitive disadvantage, compromise inward investment or affect their export markets.

Recommendations

7. The FCDO should promote a global moratorium on the export of surveillance technology until there is a proper human rights regulatory framework in place. This is something that the UN Special Rapporteur on Freedom of Opinion and Expression has called for.[3] Such a moratorium should include the use, development, production, sale, and export of facial recognition technology for identification purposes by both state agencies and private sector actors, with particular regard to human rights violations arising from use of this technology.

8. The FCDO should support its missions abroad to understand and monitor use of these technologies, especially where they are linked to British companies. A human rights specialist should be included on trade delegations to ensure that trade and investment opportunities that are being promoted address the human rights impacts associated with these technologies.

9. The FCDO should take a more proactive approach to addressing the threats to human rights defenders arising from surveillance technology, raising issues with host governments at an early stage, speaking out when these technologies are being misused, and publicly supporting human rights defenders who are being targeted by them.

10. The FCDO should ensure consistency and coherence of government policy relating to the human rights impacts of surveillance technologies globally in spheres such as the granting of export licences, the promotion of business opportunities and invitations to trade fairs.[4] There should be a joined-up approach to these issues across Departments, particularly the Department for International Trade, the Home Office and the Department for Business, Energy & Industrial Strategy.

11. The FCDO should support a new law to hold companies to account when they fail to prevent human rights abuses as recommended in 2017 by Parliament's Joint Committee on Human Rights[5] and confirmed as legally feasible in 2020 by the British Institute of International and Comparative Law.[6] Such a 'corporate duty to prevent' law should be

[3] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736
[4] https://www.amnesty.org.uk/press-releases/uk-home-office-should-withdraw-trade-fair-invite-israeli-spyware-firm
[5] Recommendation 24, p73, https://publications.parliament.uk/pa/jt201617/jtselect/jtrights/443/443.pdf

modelled on the civil and criminal duties to prevent tax evasion and bribery found in the Criminal Finances Act 2017 and the Bribery Act 2010. This law should mandate companies, including those in the field of surveillance technology, to undertake human rights due diligence to identify and prevent harm arising from their operations and products.[7]

Q1 and Q2 Technologies that are shifting power in ways that are incompatible with the protection of human rights

Internet shutdowns

12. Shutting down the internet is a tactic of repression being used more and more by governments to limit Freedom of Expression and mask human rights violations. Shutdowns are increasingly employed to hide dissent, repression, and popular protest.

13. Amnesty has documented the killings by Iranian Security Services of 304 people during the five days of protests that swept the country in November 2019.[8] More than two thirds of the deaths verified by Amnesty took place within 48 hours of the internet shutdown, which began a day after protests broke out on November 15, 2019, in response to a sudden hike in fuel prices. Security forces used lethal force unlawfully against protesters and bystanders, many of whom were shot in the head or torso. Not only did cutting off the internet prevent people from sharing evidence of violence on social media or messaging services during the crackdown, it also had an inhibiting effect afterwards. Although internet access was restored, many people were still too afraid to post footage of what happened online.

14. The internet shutdown in Iran made it difficult to document the severe human rights violations that happened during that period. Under international law, governments are required not to block or hinder internet connectivity in relation to peaceful assemblies. Any restrictions on freedom of expression should be legal, necessary, proportionate and timebound.

15. Internet shutdowns are becoming particularly prevalent. Ethiopia blocked access to the internet for more than two weeks in July 2020 to supress unrest after protests erupted over the death of a popular singer.[9] The Indian government is one of the most frequent users of shutdowns in the world, blocking access for months at a time in the region of Jammu and Kashmir.[10] Over the last five years, Chadian authorities have deliberately restricted the internet at important moments of political dispute, amounting to two and a half years in total of shutdowns and disruptions.[11]

---

[6] https://www.biicl.org/publications/a-uk-failure-to-prevent-mechanism-for-corporate-human-rights-harms
[7] https://corporatejusticecoalition.org/wp-content/uploads/2020/04/Duty-to-prevent_principal-elements_FINAL.pdf
[8] https://iran-shutdown.amnesty.org/
[9] https://www.amnesty.org/en/latest/news/2020/06/ethiopia-popular-musicians-killing-must-be-fully-investigated/
[10] https://www.amnesty.org/en/latest/news/2020/03/mitigate-risks-of-covid-19-for-jammu-and-kashmir-by-immediately-restoring-full-access-to-internet-services/
[11] https://www.amnesty.org/en/latest/news/2021/04/tchad-les-coupures-internet-une-entrave-la-liberte-dexpression

Censorship and blocking of content

16. The blocking of internet content has been another means by which governments have restricted Freedom of Expression. In August 2019, a court in Ankara blocked scores of web addresses without any justification as to why this was necessary or proportionate.[12] One of those targeted includes Bianet.org, an independent news portal in Turkey that was continuing to report on human rights abuses throughout the media crackdown.

17. Many countries adopt laws that allow the blocking of websites on grounds of protecting the right to life and security of people and property, national security and public order, prevention of crimes or protection of general health, or on the request of relevant ministries or officials. However, in some cases these grounds become a pretext for censoring journalism and suppressing dissent.

18. Cyber-censorship is now a global phenomenon, and it is not limited to websites being blocked. In 2016 Amnesty documented 55 countries where people were arrested just for what they said online. Many Governments are using sophisticated new technologies to silence, spy on, harass and track critical voices.

19. Mass surveillance is also a form of censorship, since many activists self-censor when they know that the authorities are listening in to all their communications. In Belarus, an Amnesty International investigation showed how round-the-clock, unchecked surveillance has a debilitating effect on free speech and dissent. Amnesty International has also uncovered well-orchestrated troll campaigns in Mexico to track and harass particular individuals and journalists through platforms like Twitter, and documented cyber attacks on activists in Qatar and Nepal.

Use of surveillance spyware to track and monitor human rights defenders

20. Digital attacks on activists' phones or computers are not simply about gaining access to information. They are about control and intimidation, always forming part of a wider story of repression and human rights abuses. Amnesty's investigations have revealed sophisticated spyware attacks against activists in countries including Morocco, Egypt, Azerbaijan, India, Uzbekistan, Qatar, Mexico, and Pakistan.[13]

21. Cyberattacks range from cutting-edge infiltration of mobile phones to less sophisticated phishing campaigns. Among the biggest new challenges are "network injections", used to deliver advanced spyware, such as NSO Group's Pegasus.[14]

22. A network injection redirects a device's web browser to a malicious website, without requiring any action by the victim. The malicious website installs Pegasus, leaving little trace, enabling the attacker to silently access a phone's messages, emails, media, location, microphone, camera, calls and contacts.

---

[12] https://www.amnesty.org.uk/press-releases/turkey-136-social-media-and-news-sites-blocked-suffocating-crackdown-freedom

[13] https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/

[14] https://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/ See also Rights Groups Open Letter: NSO Group Continues to Fail in Human Rights, 27 April 2021 https://www.amnesty.org/en/documents/doc10/4036/2021/en/

23. Vietnamese activists have been targeted by hacking group Ocean Lotus, highlighting an intensifying assault on freedom of expression online. Amnesty has called upon the Vietnamese government to carry out an independent investigation into these digital attacks.[15]

24. Amnesty has conducted research into the surveillance capacity of the Government of South Sudan and the impact of its abusive deployment without safeguards.[16] Digital and physical surveillance have created a pervasive climate of fear and self-censorship. While many human rights defenders continue to courageously work within the limits of this repressive environment, exercising their right to free speech is fraught with danger.

Facial Recognition

25. Amnesty International has been drawing attention to the human rights risks arising from Facial Recognition Technology (FRT), a term that is used to describe digital applications that perform a specific task using a human face to verify or identify an individual.[17] FRT is one of numerous biometric technologies being deployed increasingly by states and commercial entities for a wide range of purposes including the cracking down on peaceful protest.[18]

26. Facial recognition technologies pose a direct threat to the enjoyment of the rights to privacy and peaceful assembly, among other rights. It can create a chilling effect and seriously deter such forms of peaceful dissent for the foreseeable future.

27. For example, law enforcement authorities have used facial recognition technologies to track down protestors, by using images captured through CCTV and other video surveillance devices and running them through facial recognition software to perform face analysis or search for potential face matches against a designated database. The software, which has higher rates of false positives amongst persons of colour,[19] also augments existing discriminatory practices within law enforcement agencies, as evidenced by the Metropolitan Police's use of the Gangs Matrix.[20]

28. Through targeting protesters from marginalized communities, including persons of colour, FRT undermines the right to equality and non-discrimination. This is especially relevant in the current context of global protests for racial justice.

---

[15] https://www.amnesty.org/en/latest/news/2021/02/viet-nam-hacking-group-targets-activist/
[16] https://www.amnesty.org/download/Documents/AFR6535772021ENGLISH.pdf
[17] https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/
[18] https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/
[19] ACLU tested amazon's facial recognition, which falsely matched members of congress with mugshots: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
[20] https://www.amnesty.org.uk/trapped-gangs-matrix

29. Any interference with the right to privacy must always be legitimate, necessary, and proportionate; FRT that scans and captures data from all faces within its radius is not necessary or proportionate in most circumstances.

30. Amnesty International is calling for a ban on the use, development, production, sale, and export of facial recognition technology for identification purposes by both state agencies and private sector actors, with particular regard to the human rights violations arising from use of this technology.

Smart Cities

31. Smart cities have become increasingly popular in urban planning over the past decade. The industry is growing rapidly, with smart city solutions being implemented across the world and increasingly in emerging markets - often with the backing of the United Nations through initiatives such as the 'United Smart Cities' programme.[21]

32. The aggregation of data collected through smart city sensors and cameras, found on rubbish bins, traffic lights, streetlights, manhole covers, CCTV and 'free' WI-FI can create an increasingly pervasive surveillance system, threatening privacy, freedom of expression and opinion, peaceful assembly, while also fueling discrimination.[22]

33. As cities collect larger amounts of personal data on residents, often without their knowledge or consent, the right to privacy in public spaces becomes more effectively eroded. Smartphones exacerbate data collection by sharing, for example, geo-location data and digital interactions with mobile applications and WI-FI providers, who are, in turn, able to share data with other service providers. Accordingly, the increasingly interconnected and digital nature of city services means that the very act of being in public spaces engenders data sharing.

34. Such infrastructure can provide state law enforcement and security agencies with the tools to intrusively track and target ethnic minorities or other protected groups. In China, smart cities in Xinjiang Uighur Autonomous Region (XUAR) already form part of the state authorities' systematic surveillance and repression of Muslim ethnic groups in the region. Facial and gait recognition, coupled with CCTV outside mosques, and powered by new artificial intelligence (AI) and analytics technology, enables authorities in XUAR to maintain a "digital police state".[23]

35. In many cases, governments have limited control over this technology as they are delivered through private-public partnerships, which are often bound by confidentiality agreements imposed for reasons relevant to the proprietary nature of the technology. This clearly makes it hard for citizens to scrutinise the systems being fitted to their cities and used by and on them. The opaqueness of these closed source proprietary models raises serious concerns over accountability and transparency.

---

[21] https://sustainabledevelopment.un.org/partnership/?p=10009

[22] https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/

[23] https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/

36. Human rights must be put at the centre of development plans for smart cities to ensure freedoms are protected. Civil servants should have a deep understanding of the technologies they are contracting out to the private sector and enforce public procurement specifications that protect against abusive or wrongful use of the technologies. Technology needs to have safeguards built in to ensure that its use is consistent with human rights standards. Ultimately, people whose rights will be affected by these technologies should have control over whether and how these new technologies are used through meaningful public oversight, consultation, and control.

Business Models of Tech Companies

37. In 2019 Amnesty launched a report on how the surveillance-based business model of companies like Facebook and Google undermines fundamental rights, including the right to privacy and freedom of expression.[24]

38. Google and Facebook have established dominance over the primary channels that most of the world – outside of China – relies on to realize their rights online. The various platforms they own – including Facebook, Instagram, Google Search, YouTube and WhatsApp – facilitate the ways people seek and share information, engage in debate and participate in society. Google's Android also underpins most of the world's smartphones.

39. The tech giants offer these services to billions without charging users a fee. Instead, individuals pay for the services with their intimate personal data, being constantly tracked across the web and in the physical world as well, for example, through connected devices.

40. While the internet is vital for people to enjoy many of their rights, most people have no meaningful choice but to access this public space on terms dictated by Facebook and Google.

41. This extraction and analysis of people's personal data on such an unprecedented scale is incompatible with every element of the right to privacy, including the freedom from intrusion into our private lives, the right to control information about ourselves, and the right to a space in which we can freely express our identities. Children have also become targets of surveillance marketing.[25]

Q6 Building resilience of civil society to the threats posed by new technologies

42. Human rights defenders (HRDs) are in the frontline of exposing the adverse impacts of new technologies, while at the same time being amongst their targets.

43. FCDO recognizes that human rights defenders are an essential part of its foreign policy and it has a vital role to play in supporting human rights defenders whether they are

[24] https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF

[25] See for example Amnesty International, *Facebook building Instagram platform for children under 13, 19 March 2021, https://www.amnesty.org/en/latest/news/2021/03/facebook-building-new-instagram-for-children-under-13/*

campaigners, journalists, union activists, politicians, lawyers, teachers or others.[26] These are the people who are speaking truth to power, who are fighting for progressive change, for freedom, for responsible business, and who seek to hold those in power to account.

44. However, HRDs often face extreme risk as a result. These risks have worsened in recent years and it is no coincidence that the unprecedented surge in repression faced by HRDs and civil society organisations, in every region of the world, is taking place against a backdrop of surveillance technologies that support authoritarianism and the suppression of dissent. [27] Human rights defenders are the canaries in the mine, with attacks against them foretelling increasingly repressive and regressive regimes, whilst also being the most important partners for exposing and opposing current abuses of power.

45. Amnesty International has documented a global trend of the use of new technologies to interfere with the right to freedom of association and to hamper the work of civil society organizations, criminalising legitimate human rights activities and using social and state media to smear human rights defenders. Surveillance technology and the manipulation of social media are key elements in this approach.

46. FCDO does some good work to support human rights defenders, but that work is inconsistent, largely reactive and behind closed doors, even when human rights defenders have consented to and appealed to foreign governments for public support.

47. In February 2021 Amnesty International UK and the Centre for Applied Human Rights, working with several partner organisations, published a report, "*On the Human Rights Frontline – How the UK can defend the defenders*", which demonstrates the need for a UK government strategy to improve support and protection for HRDs and civil society space.[28]

May 2021

[26] UK Government Policy Paper: UK support for human rights defenders, July 2019 https://www.gov.uk/government/publications/uk-support-for-human-rights-defenders

[27] https://www.amnesty.org/en/latest/research/2019/08/a-dangerous-alliance-governments-collaborate-with-surveillance-companies-to-shrink-the-space-for-human-rights-work/

[28] https://www.amnesty.org.uk/onthehumanrightsfrontline