ADVANCING HUMAN-RIGHTS-BY-DESIGN IN THE DUAL-USE TECHNOLOGY INDUSTRY

Jonathon Penney, Sarah McKune,
Lex Gill, and Ronald J. Deibert

It is no secret that technology companies have greased the wheels for human rights abuses around the world backed by a global web of private sector support and investment that has yielded significant financial returns. In April 2018, Citizen Lab published research analyzing the use of Internet filtering technology in ten countries of interest: Afghanistan, Bahrain, India, Kuwait, Pakistan, Qatar, Somalia, Sudan, United Arab Emirates, and Yemen.[1] In these countries, technology produced by a company called Netsweeper is implemented by national-level, consumer-facing Internet Service Providers (ISPs) to filter online content. Choices made by Netsweeper have a significant impact on the types of websites that users in a given country can ultimately access.

Citizen Lab researchers demonstrated through a variety of technical methods that Netsweeper's technology facilitates the blocking of digital speech protected by international human rights law—from religious content in Bahrain and political campaigns in the UAE to media websites in Yemen. News concerning Rohingya refugees was censored, information about violence against national religious minority populations blocked, and websites—from the World Health Organization to the Christian Science Monitor—were miscategorized as "Pornography" using Netsweeper's filtering tools. Pre-set categories curated by Netsweeper itself (including an "Alternative Lifestyles" category) also facilitated the miscategorization and censorship of content from LGBTQ2+ civil rights and advocacy organizations, HIV/AIDS health resources, and media and cultural groups. Netsweeper's filtering system can even be configured so that every website originating from an entire specified country can be blocked all at once.

Journal of International Affairs, Vol. 71, No. 2.

Citizen Lab concluded that these uses of Netsweeper's technology were likely contrary to international human rights law.[2] They appeared to constitute impermissible restrictions on, among other rights, freedom of opinion and expression, minority rights, and protections against discrimination enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Yet Netsweeper is not an outlier. It is merely one example, operating within a complex cyber security industry increasingly financed by specialized and powerful investment firms.[4] Products like Netsweeper's Internet filtering systems are often referred to as "dual use." While they may serve legitimate societal objectives in some cases, they are also used to undermine human rights like freedom of expression and privacy. Citizen Lab research has repeatedly exposed the ways in which deep packet inspection (DPI) technology and Internet filtering software—services offered by technology companies like Sandvine and Netsweeper—can be used to censor speech and threaten freedom of expression online.[5] Research has also revealed the widespread abuse of dual-use technology in the form of malicious software, spyware, and hacking tools (like those developed by private sector security and intelligence firms, including FinFisher, Hacking Team, and NSO Group) governments with problematic human rights records use to target civil society.[6] As surveillance technology is propagated and normalized, it has crept into ordinary commercial markets, putting tools or techniques designed for use by intelligence and law enforcement into the hands of ordinary criminal actors and abusive spouses alike.[7]

These business practices would not be possible without private sector financial and investment firms bankrolling them. For example, Francisco Partners is a global private equity firm specialized in the technology sector.[8] Its portfolio companies have included Blue Coat (since acquired by Symantec), a manufacturer of dual-use technology deployed in countries with deeply problematic human rights records including Iran, Syria, and Sudan, subject to sanctions by the United States government.[9] Sandvine—a company whose PacketLogic devices were apparently used to surreptitiously inject malicious and dubious redirects for users in Turkey, Syria, and Egypt—is currently a member of the Francisco Partners family.[10] And Francisco Partners has long been the controlling shareholder in an Israeli cyber-arms dealer called NSO Group.[11] The NSO Group spyware can be directly linked to the illegal surveillance of human rights activists, journalists, and lawyers from the UAE to Mexico.[12,13]

Emerging markets for the sale of filtering, hacking, and targeted surveil-

lance technologies, especially to repressive and authoritarian states, raise serious human rights concerns. Yet, when researchers, human rights activists, and civil society groups raise concerns and call on these companies to change course, these concerns are frequently met with vague statements, denial, and silence.[14] While the investment firms financing these business practices often pay lip service to corporate social responsibility, in practice they have done little to enforce respect for human rights.[15,16]

Investors can no longer turn a blind eye. There is now a worldwide market in the billions of dollars for companies that are prepared to facilitate mass censorship and surveillance. Cleaning it up will require action by all stakeholders in the cyber security industry, including governments, businesses, employees and their shareholders, industry associations, private investment firms, incubators, and accelerators funding it all.

International human rights law, at present, does not explicitly require states to police business activities outside their national jurisdiction; however, states do have a general duty to ensure that businesses over which they have jurisdiction respect human rights.[17] In Citizen Lab's Planet Netsweeper report, researchers set out a range of concrete recommendations based on these obligations.[18] For national governments, particularly those such as the Canadian government that have funded and supported dual-use technology companies, the report recommends tying the ability to receive financial support (such as research and development grants) to clear prohibitions on illegal and unethical business practices abroad.[19] It also recommends restricting government procurement of dual-use technology to companies with clean human rights records; mandating stronger corporate transparency; and empowering agencies tasked with investigating Canadian businesses involved in human rights abuses abroad. Researchers further recommend enacting legislative measures to make it easier for foreign human rights victims to seek redress in domestic courts. They also suggest following Europe's lead in requiring stronger human rights considerations in export controls and licensing decision-making. Also, following Europe's approach in proposing broad whistleblower protections can empower employees tasked with developing or operationalizing rights-infringing technologies.[20] Businesses have international human rights responsibilities as well.[21] For companies like Netsweeper—and their corporate leadership—this requires at minimum establishing human rights due diligence processes; transparency about corporate social responsibility and human rights policies and practices; and measures to remediate adverse human rights impacts caused by their business activities.

But businesses can do far more than these basic measures. They could adopt a "human-rights-by-design" principle whereby they commit to designing tools, technologies, and services to respect human rights by default, rather than permit abuse or exploitation as part of their business model. The "privacy-by-design" concept has gained currency today thanks in part to the European Union General Data Protection Regulation (GDPR), which requires it.[22] The overarching principle is that companies must design products and services with the default assumption that they protect privacy, data, and information of data subjects. A similar human-rights-by-design paradigm, for example, would prevent filtering companies from designing their technology with features that enable large-scale, indiscriminate, or inherently disproportionate censorship capabilities—like the Netsweeper feature that allows an ISP to block entire country top level domains (TLDs). DPI devices and systems could be configured to protect against the ability of operators to inject spyware in network traffic or redirect users to malicious code rather than facilitate it. And algorithms incorporated into the design of communications and storage platforms could account for human rights considerations in addition to business objectives. Companies could also join multi-stakeholder efforts like the Global Network Initiative (GNI), through which technology companies (including Google, Microsoft, and Yahoo) have taken the first step toward principles like transparency, privacy, and freedom of expression, as well as to self-reporting requirements and independent compliance assessments.[23]

Technologists and industry associations also have essential roles to play as guardians of business ethics. For better or worse, the rights impacts of advanced technologies will reflect individual human decisions. In the spring of 2018, for example, over 4,000 Google employees signed a letter condemning the company's involvement with Project Maven, a U.S. military effort to combine machine learning and drone surveillance.[24] As a result of their advocacy, the Pentagon contract will not be renewed—and Google has now adopted a series of principles to govern the company's research and development activities in the field of artificial intelligence.[25] The list of principles also includes an explicit list of "applications we will not pursue," restricting the development of weapons, mass surveillance tools, and other "technologies whose purpose contravenes widely accepted principles of international law and human rights."[26] Similarly, engineers and other employees at cyber security firms, with the support of industry and professional associations, can draw on (and update) existing models like the IEEE Computer Society's Engineer's Code of Ethics to establish cyber security

ethical codes and standards.[27] This, combined with greater whistleblower protections, provide a framework for greater employee responsibility for ethical business practice and design principles.

A culture shift is required to fully address the human rights challenges in current cyber security industry practices. What that shift will look like is ultimately the responsibility of each of the stakeholders involved in the dual-use technology ecosystem. The first step is dialogue, to identify problems and gaps, and begin the process of developing rights-based benchmarks for industry.[28]

Jonathon Penney *is Citizen Lab's 2011 Google Policy Fellow. He is currently a pursuing a doctorate in information and communication sciences at Oxford University. Before Oxford, Jonathon spent time studying and researching at Columbia Law School, where he was a Fulbright Scholar, and at Victoria University, where he was a Senior Research Fellow and Lecturer in the law faculty. A graduate of Dalhousie University and native Nova Scotian, he has served as Associate Editor of the Oxford University Commonwealth Law Journal, and worked as a lawyer and as a policy adviser at the federal level. At Oxford, he is pursuing an interdisciplinary project, studying the "chilling effect" that certain laws and regulatory schemes, like take-down notices, have on speech and expression online. His broader research interests include constitutional & public law, intellectual property, and technology law, both separately and where these areas intersect.*

Sarah McKune *is a senior researcher for the Citizen Lab at the Munk School of Global Affairs, University of Toronto. Her research and analysis focuses on cyber threats targeting civil society, control of surveillance technology exports and international cyber security initiatives. Prior to joining the Citizen Lab, she was Law Officer and Special Assistant to the Executive Director at the nongovernmental organization Human Rights in China, where she focused much of her efforts on the counter-terrorism policies and human rights impact of the Shanghai Cooperation Organization. Her previous experience also includes work as a litigation associate at the New York office of Morrison & Foerster LLP, and teaching English in China.*

Lex Gill *is a former Research Fellow at The Citizen Lab, an interdisciplinary laboratory focused on research, development, and high-level strategic policy and legal engagement at the intersection of technology, human rights, and global security. She has written and spoken internationally on issues ranging from privacy, freedom of expression, and equality rights to cybersecurity policy, national security law, and the*

regulation of censorship and surveillance technology. Lex holds a B.C.L./LL.B. from McGill University's Faculty of Law. She is currently clerking at the Supreme Court of Canada.

***Ronald J. Deibert** (OOnt, PhD, University of British Columbia) is Professor of Political Science, and Director of the Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto. The Citizen Lab is an interdisciplinary laboratory focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. He was a co-founder and a principal investigator of the OpenNet Initiative (2003-2014) and Information Warfare Monitor (2003-2012) projects. Deibert was one of the founders and (former) VP of global policy and outreach for Psiphon, one of the world's leading digital censorship circumvention services.*

ENDNOTES

[1] Delek, Jakub, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert. 2018. "Planet Netsweeper." Rep. Citizen Lab. https://citizenlab.ca/2018/04/planet-netsweeper/.

[2] Ibid, see "Section 3 – Discussion & Conclusions."

[3] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III). http://www.un.org/en/universal-declaration-human-rights/; UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; See specifically freedom of opinion and expression (UDHR Art. 19, ICCPR Art. 19); rights to liberty and security of the person (UDHR Art. 3, ICCPR Art. 9); the right to privacy (UDHR Art. 12, ICCPR Art. 17); protections against discrimination (UDHR Art. 7, ICCPR Art. 26); and minority rights (ICCPR Art. 27).

[4] See e.g., Burrough, Brian. 2016. "How a Grad Student Found Spyware That Could Control Anybody's IPhone From Anywhere In The World." *Vanity Fair*, November 28, 2016. https://www.vanityfair.com/news/2016/11/how-bill-marczak-spyware-can-control-the-iphone;

Robins-Early, Nick. 2012. "Meet the Cynical Western Companies Helping the Syrian Regime." *The New Republic*, March 15, 2012. https://newrepublic.com/article/101732/syria-spyware-surveillance-revolution-assad-activists-human-rights; Pangburn, DJ. 2017. "The Secretive Billion-Dollar Company Helping Governments Hack Our Phones." *Fast Company*, November 30, 2017. https://www.fastcompany.com/40469864/the-billion-dollar-company-helping-governments-hack-our-phones; Thomson, Ian. 2015. "FinFisher, the Spyware Loved by Cruel Dictators, Stomps All over Human Rights, Says UK Govt." The Register, February 26, 2015. https://www.theregister.co.uk/2015/02/26/oecd_rules_anglo-german_finfisher_spyware_violated_human_rights/;

See also "Data and Information Collection for EU Dual-Use Export Control Policy Review." 2015. European Commission Report. ECORYS & SIPRI. http://www.cecimo.eu/site/fileadmin/documents/EU LEGISLATION AND DOSSIERS/Dual-use_legislation/FINAL_REPORT.pdf

[5] Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. 2018. "Bad Traffic." Rep. *Bad Traffic*. Citizen Lab. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/; Dalek, "Planet Netsweeper."

[6] McKune, Sarah, and Ron Deibert. March 2017. "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking." Rep. Citizen Lab. https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf;

Marczak, Bill, John Scott-Railton, and Sarah McKune. 2015. "Hacking Team Reloaded? US-Based

Ethiopian Journalists Again Targeted with Spyware." Rep. Citizen Lab. https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/; See full 7-part series on abuse of NSO spyware by Marczak, Bill, John Scott-Railton, Claudio Guarnieri, Masashi Crete-Nishihata, Bahr Abdul Razzak, and Ron Deibert. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links," "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware, "Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware," "Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware," "Part 7: Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware." Citizen Lab. August 2016 to August 2017. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[7] Deibert, Robert, Lex Gill, Tamir Israel, Chelsea Legge, Irene Poetranto, and Amitpal Singh. 2017. "Submission to the United Nations Special Rapporteur on Violence Against Women, Its Causes and Consequences, Ms. Dubravka Šimonovic." Rep. Citizen Lab. https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf.; Penney, Jonathon. 2017. "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Study." *Internet Policy Review* 6 (2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959611. Often these targeted threats disproportionately impact certain groups, including women and young people.

[8] "Investments." 2018. Francisco Partners. https://www.franciscopartners.com/investments.

[9] Marquis-Boire, Morgan, Collin Anderson, Jakub Dalek, Sarah McKune , Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman. 2013. "Some Devices Wander by Mistake: Planet Blue Coat Redux." *Citizen Lab*, July 2013. https://citizenlab.ca/2013/07/planet-blue-coat-redux/; Dalek, Jakub, and Adam Senft. 2011. "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma." Citizen Lab, November 2011. https://citizenlab.ca/2011/11/behind-blue-coat/#update; Clark, Greg. 2016. "Symantec CEO Greg Clark Ushers in New Era of Cyber Security." Symantec. August 1, 2016. https://www.symantec.com/connect/blogs/symantec-ceo-greg-clark-ushers-new-era-cyber-security. See re: Symantec acquisition: Greg Clark.

[10] Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibart. 2018. "Bad Traffic." Rep. Citizen Lab. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.

[11] Clark, Simon. 2018. "U.S. Software Firm Verint Is in Talks to Buy NSO for About $1 Billion." *The Wall Street Journal*, May 28, 2018. https://www.wsj.com/articles/u-s-software-firm-verint-systems-is-in-talks-to-buy-nso-group-for-about-1-billion-1527491415.

[12] Marczak, Bill, and John Scott-Railton. 2016. "The Million Dollar Dissident: NSO Group's IPhone Zero-Days Used against a UAE Human Rights Defender." *Citizen Lab*, August 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[13] Marczak, Bill, John Scott-Railton, Claudio Guarnieri, Masashi Crete-Nishihata, Bahr Abdul Razzak, and Ron Deibert. 2017. "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links." "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware, "Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware," "Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware," "Part 7: Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware." Rep. Citizen Lab. https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

[14] "Media Release: Netsweeper Responds to Media Enquiries Regarding International Operations." 2018. Netsweeper Inc. https://citizenlab.ca/wp-content/uploads/2018/04/Media-Release-Netsweeper-23-Apr-2018.pdf; Lyndon Cantor of Sandvine. Letter to Claire M.C. Kennedy, Michael H. Wilson, Meric Gertler. 2018. "Letter to Claire M.C. Kennedy, Michael H. Wilson, and Meric Gertler of University of Toronto ," March 7, 2018; Deibert, Ronald J, and Citizen Lab. Letter to Perry Roach, Lou Erdelyi. 2018. "Letter to Perry Roach and Lou Erdelyi of Netsweeper ," April 10, 2018. https://citizenlab.ca/wp-content/uploads/2018/04/Citizen-Lab-Letter-to-Netsweeper-April-2018.pdf.

[15] Fox-Brewster, Thomas. 2018. "Did This American Tech Help Turkey Spy In Syria?" *Forbes*, March 9, 2018. https://www.forbes.com/sites/thomasbrewster/2018/03/09/turkey-egypt-spyware-spreads-via-procera-sandvine/#74b85e40b59f.

[16] Deibert, Ronald J, and Citizen Lab. Letter to Dipanjan (DJ) Deb, Andrew Kowal. 2018. "Open Letter to Dipanjan (DJ) Deb and Andrew Kowal of Francisco Partners ," May 29, 2018. https://citi-

zenlab.ca/wp-content/uploads/2018/05/Letter-to-Francisco-Partners-May-29-2018.pdf.

[17] "Guiding Principles on Businesses and Human Rights: 135 Implementing the United Nations 'Protect, Respect and Remedy' Framework." 2011. Rep. United Nations Human Rights Office of the High Commissioner. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[18] "Planet Netsweeper: Section 3 – Discussion & Conclusions."

[19] Ibid., see "3.4 Netsweeper's relationship with the Canadian government," for examples of financial support and trade promotion by the Canadian federal government and the Ontario provincial government. See also: Deibert, Ronal J. Letter to Mr. Randy Boissonnault. 2018. "Open Letter to Mr. Randy Boissonnault, Member of Parliament and Special Advisor to the Prime Minister on LGBTQ2 Issues," May 3, 2018. https://citizenlab.ca/wp-content/uploads/2018/05/Letter-to-Boissonnault_DEIBERT_May-2018.pdf.

[20] *Proposal for a Directive of the European Parliament and of the Council on the Protection of Persons Reporting on Breaches of Union Law*, COM(2018)218 . 2018. European Union, Directorate-General for Justice and Consumers.

https://ec.europa.eu/info/law/better-regulation/initiatives/com-2018-218_en#proposal-for-a-directive.

[21] United Nations Human Rights Office of the High Commissioner, "Guiding Principles on Businesses and Human Rights."

[22] Wheeler, Tom. 2018. "The General Data Protection Regulation Sets Privacy by Default." Web log. *Brookings Institution Blog* (blog). Brookings Institution. May 23, 2018. https://www.brookings.edu/blog/techtank/2018/05/23/the-general-data-protection-regulation-sets-privacy-by-default

[23] "Global Network Initiative Home." 2018. Global Network Initiative. 2018. https://globalnetworkinitiative.org/.

[24] "Letter to Google CEO Sundar Pichai." Letter to Sundar Pichai. 2018. *New York Times*, April 2018. https://static01.nyt.com/files/2018/technology/googleletter.pdf; Shane, Scott, and Daisuke Wakabayashi. 2018. "'The Business of War': Google Employees Protest Work for the Pentagon." *New York Times,* April 4, 2018.

[25] Simonite, Tom. 2018. "Google Sets Limits on Its Use of AI but Allows Defense Work." *Wired*, June 7, 2018. https://www.wired.com/story/google-sets-limits-on-its-use-of-ai-but-allows-defense-work/.

[26] Pichai, Sundar. 2018. "AI at Google: Our Principles." Web log. *Google* (blog). Google. June 7, 2018. https://blog.google/topics/ai/ai-principles/amp/.

[27] Gotterbarn, Don, Keith Miller, and Simon Rogerson. October 1999. Executive Committee, IEEE-CS/ACM Joint Task Force on Software Engineering Ethics and Professional Practices. "Computer Society and ACM Approve Software Engineering Code of Ethics." *Computer*. 84-88. https://www.computer.org/cms/Publications/code-of-ethics.pdf.

[28] See, for example, the indicators developed by Ranking Digital Rights for the ICT sector: https://rankingdigitalrights.org/index2018/indicators/.