Walking the Talk:

2021 Blueprints for a Human Rights-Centered U.S. Foreign Policy

Chapter 2: Confronting Digital Authoritarianism By Stemming the Proliferation of AI-Enabled Surveillance Technology

human rights *first*

October 2020

Acknowledgments

Human Rights First is a nonprofit, nonpartisan human rights advocacy and action organization based in Washington D.C., New York, and Los Angeles.

Walking the Talk: 2021 Blueprints for a Human Rights-Centered U.S. Foreign Policy was authored by Human Rights First's staff and consultants. Senior Vice President for Policy Rob Berschinski served as lead author and editor-in-chief, assisted by Tolan Foreign Policy Legal Fellow Reece Pelley and intern Anna Van Niekerk.

Contributing authors include:

Eleanor Acer
Rob Berschinski
Cole Blum
Benjamin Haas
Scott Johnston
David Mizner
Reece Pelley
Rita Siemion
Trevor Sutton
Raha Wala

Significant assistance was provided by:

Chris Anders
Abigail Bellows
Brittany Benowitz
Jim Bernfield
Heather Brandon-Smith
Christen Broecker
Felice Gaer
Bishop Garrison
Clark Gascoigne
Liza Goitein
Shannon Green
Steven Feldstein
Becky Gendelman
Ryan Kaminski
Colleen Kelly
Kate Kizer
Kennji Kizuka
Dan Mahanty
Kate Martin
Jenny McAvoy
Sharon McBride
Ian Moss
Stephen Pomper
Jennifer Quigley
Scott Roehm
Hina Shamsi
Annie Shiel
Mandy Smithberger
Sophia Swanson
Yasmine Taeb
Bailey Ulbricht
Anna Van Niekerk

Human Rights First challenges the United States of America to live up to its ideals. We believe American leadership is essential in the struggle for human dignity and the rule of law, and so we focus our advocacy on the U.S. government and other key actors able to leverage U.S. influence. When the U.S. government falters in its commitment to promote and protect human rights, we step in to demand reform, accountability, and justice.

When confronting American domestic, foreign, and national security policies that undermine respect for universal rights, the staff of Human Rights First focus not on making a point, but on making a difference. For over 40 years we've built bipartisan coalitions and partnered with frontline activists, lawyers, military leaders, and technologists to tackle issues that demand American leadership.

Human Rights First is led by President and Chief Executive Officer Mike Breen and Chief Operating Officer Nicole Elkon.

We thank the many foundations and individual donors who provide invaluable support for the organization's research and advocacy.

This and other reports are available online at humanrightsfirst.org.

Confronting Digital Authoritarianism By Stemming the Proliferation of AI-Enabled Surveillance Technology

human rights *first*

Introduction

One of the most significant threats to the enjoyment of human rights in the world today is the proliferation of new and emerging surveillance technologies, including those that incorporate artificial intelligence (AI). AI-enabled surveillance technologies powered by big data analytics provide governments with the ability to identify, track, and monitor millions of individuals at a time.[1] By pairing complex computer algorithms with more traditional tools of surveillance, such as video cameras and microphones, AI-enhanced systems of surveillance facilitate the collection of massive quantities of personally identifiable information and enable governments to use that information to engage in the automated real-time monitoring of entire civilian populations.[2] These omnipresent systems of surveillance allow governments to repress political dissent, discriminate against ethnic and religious minorities, and violate the general privacy rights of their citizens. So far, the United States government has failed to adopt policies sufficient to confront potential abuse of AI-enabled surveillance tools by domestic law enforcement agencies, or the proliferation of such technologies that is fueling the rise of digital authoritarianism.[3] In order to minimize the long-term negative impact that these technologies can have on democracy, the rule of law, and the enjoyment of human rights around the world, the next administration must prioritize the implementation of a whole-of-government approach to stopping their proliferation and abuse.

[T]he United States government has failed to adopt policies sufficient to confront potential abuse of AI-enabled surveillance tools by domestic law enforcement agencies, or the proliferation of such technologies that is fueling the rise of digital authoritarianism.

AI-enabled surveillance technology is already directly contributing to the violation of human rights. Authoritarian regimes, including the Russian and Chinese governments, currently use or are in the process of establishing AI-enabled biometric data collection technologies, such as the hardware and software behind facial and voice recognition systems, to build systems of mass surveillance that can track and catalog the movements and activities of millions of people at a time.[4] Technologies that rapidly collect, capture, and enable the genetic profiling of ethnic groups via their DNA may lead to abuses heretofore unseen. Other states, such as the United Arab Emirates and Uganda, are employing AI-enabled surveillance technology in more limited ways, including by harnessing the technology to enhance the efficacy of pre-existing policies of political repression.[5] In such cases, the aggregation and exploitation of personal data is being used to silence political opposition, stifle free expression and the free exercise of religion, target minority populations, and eviscerate any semblance of privacy that previously existed.

---

1 Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, New York Times (Apr. 14, 2019) available at https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

2 Jay Stanley, American Civil Liberties Union (ACLU), *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, p. 5 (2019) available at https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf.

3 In 2018, the Department of Commerce acknowledged the lack of export restrictions on certain "new and emerging" technologies, including enhanced surveillance technologies, and signaled that new restrictions may be imposed; however, as of this writing, no such restrictions have been introduced. *See* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58201 (Nov. 19, 2018) (to be codified at 15 C.F.R. § 744) available at https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies. The Department of State has similarly demonstrated concern over the unregulated export of surveillance technology but has also failed to take any concrete action beyond the publishing of a non-binding guidance document intended to help exporters comply with the U.N. Guiding Principles on Business and Human Rights (UNGPs) and the OECD Guidelines for Multinational Enterprises. *See* U.S. Department of State, *Draft U.S. Government Guidance for the Export of Hardware, Software and Technology with Surveillance Capabilities and/or Parts/Know-How* (Oct. 29, 2019) available at https://www.eff.org/files/2019/10/29/draft-guidance-for-the-export-of-hardware-software-and-technology-with-surveillance-capabilities.pdf.

4 The Chinese government has used biometric data collection technology to track and catalog the movement of the country's minority Uyghur population. *See supra* note 1. The Russian government is currently building a nation-wide facial recognition network that will soon rival China's network in size. *See* Felix Light, *Russia is building one of the world's largest facial recognition networks*, Coda (Nov. 8, 2019) available at https://codastory.com/authoritarian-tech/russia-facial-recognition-networks/.

5 National police in the UAE, a country with the highest rate of political prisoners per capita in the world, have been working toward the creation of a nation-wide facial recognition network that will undoubtedly be used to target the regime's political opponents. Megha Rajagopalan, *Facial Recognition Technology Is Facing A Huge Backlash In The US. But Some Of The World's Biggest Tech Companies Are Trying To Sell It In The Gulf.*, BuzzFeed (May 29, 2019) available at https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision. In Uganda, shortly after Huawei technicians helped government officials spy on the government's political opponents, the Ugandan government entered into a $126 million agreement with Huawei to purchase the company's AI-powered facial recognition system. Steven Feldstein, Carnegie Endowment for International Peace, *The Global Expansion of AI Surveillance*, p. 14 (Sep. 2019) available at https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

The speed with which this technology is proliferating amongst the world's worst human rights violators is staggering. Since the Arab Spring, popular protests have eclipsed military coups as the principle threat to authoritarian and autocratic regimes.[6] Recognizing this, autocrats and authoritarians have further concentrated their domestic policing efforts on repressing the civil liberties of their citizens.[7] According to experts at the Carnegie Endowment for International Peace, as of 2019, AI-enabled surveillance technology has been incorporated into these systems of political repression in 37 percent of "closed autocratic states" and 41 percent of countries identified as "electoral autocratic/competitive autocratic states."[8]

As a critical element in curtailing the spread of AI-powered human rights abuse, the next administration should adopt policies aimed at preventing the further proliferation of AI-enabled surveillance and biometric data collection technologies to countries where these technologies are likely to be abused. The U.S. is far from the world's only proliferator of such technologies to repressive regimes. China, a government that makes no claim to upholding individual rights, is arguably the world's leading supplier of AI-powered surveillance technologies to both repressive and non-repressive governments.[9] Companies based in France, Germany, and Japan also export similar technologies.[10] As a world leader in the development and export of cutting-edge technology, and a nation that benefits strategically from the maintenance of rights-respecting democratic governance abroad, the United States maintains a special interest in limiting the extent to which its products can be used for repressive purposes.

The first step in this effort should focus on preventing companies and private institutions, both inside and outside the United States, from selling these technologies to known human rights abusers. Currently, U.S. agencies do not

6 Andrea Kendall-Taylor, Erica Frantz, Joseph Wright, *The Digital Dictators: How Technology Strengthens Autocracy*, Foreign Affairs (Mar. 2020) available at https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

7 As popular protests have become the primary threat to authoritarian regimes, there has been a global rise in the repression of civil liberties. *Id.*

8 Feldstein, *supra* note 5, at p. 2.

9 *Id.* at p. 8-9.

10 *Id.* at p. 8.

Photo by Studio Incendo

effectively use existing authorities to regulate these types of items and services, and several U.S. technology companies have sold such software to governments with well-established records of systemic gross violations of human rights, including China, Egypt, Russia, Saudi Arabia, Singapore, Turkey, the UAE, and the Philippines.[11] U.S.-based financial institutions have also played a role in the proliferation of this technology by investing in foreign companies that develop and sell AI-enabled surveillance products to authoritarian regimes.[12] On the international stage, the U.S. government has failed to use its geopolitical influence to push the international community to modernize and amend multilateral export control regimes that could limit the global spread of AI-enabled surveillance technologies.

In order to remedy these flaws in U.S. policy, the next administration should use existing executive authorities to prevent private U.S. entities from contributing to the spread of AI-enabled surveillance technologies used for repressive purposes and establish an international consensus regarding surveillance-related export restrictions. To achieve these goals, the next administration should begin by establishing domestic "end-use" and/or "end-user" export controls on the specific technologies used in AI-enhanced systems of mass surveillance, such as the hardware and software that facilitates the collection and analysis of surveillance images and biometric data. Properly crafted, such export restrictions could help prevent U.S. technology from facilitating human rights abuses while allowing U.S. companies to remain competitive in the global AI market. Additionally, in order to address the flow of American financing and intellectual property to the foreign firms that are helping build authoritarian systems of surveillance, the next administration should use targeted human rights sanctions to prevent such firms from doing business with U.S. persons or entities. With these domestic measures in place, the next administration should turn its attention toward the inclusion of AI-enhanced surveillance-related technologies on multilateral export control lists, such as the Dual Use List of the Wassenaar Arrangement.

To prevent U.S. firms from actively facilitating human rights abuses abroad, the next administration should impose restrictions on the export of AI-enabled surveillance technology under the Export Controls Act of 2018.

Recommendations

✓ Impose licensing requirements on the export of U.S. origin AI surveillance and biometric data collection technologies by amending the Export Administration Regulations

To prevent U.S. firms from actively facilitating human rights abuses abroad, the next administration should impose restrictions on the export of AI-enabled surveillance technology under the Export Controls Act of 2018 (ECA).[13] The Department of Commerce regulates the export of so-called "dual-use" items, products that have both a civilian and military or police application, through the Export Administration Regulations

11 *Id.* at p. 25-28; Sui-Lee Wee, *China Is Collecting DNA From Tens of Millions of Men and Boys*, Using U.S. Equipment, New York Times (Jun. 17, 2020) available at https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html?referringSource=articleShare; Emile Dirks, Dr. James Leibold, International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI), *Genomic Surveillance: Inside China's DNA dragnet* (Jun. 2020) available at https://www.aspi.org.au/report/genomic-surveillance.

12 During a 2018 fundraising round for the Chinese company SenseTime, the principle architect of China's oppressive AI-powered surveillance network in Xinjiang, some of the largest investors were American firms, including Fidelity International, Qualcomm, and Silver Lake. *See* Jon Russell, *China's SenseTime, the world's highest-valued AI startup, closes $620M follow-on round*, TechCrunch (May 30, 2018) available at https://techcrunch.com/2018/05/30/even-more-money-for-senstime-ai-china/. Additionally, U.S.-based private equity and venture capital firms have funneled millions of dollars of their clients' money into foreign companies that are selling enhanced surveillance technology to human rights abusers. Ryan Mac, Rosalind Adams, Megha Rajagopalan, *US Universities And Retirees Are Funding The Technology Behind China's Surveillance State*, BuzzFeed (last updated Jun. 5, 2019) available at https://www.buzzfeednews.com/article/ryanmac/us-money-funding-facial-recognition-sensetime-megvii.

13 The Human Rights Committee, the treaty body that interprets the obligations of states parties to the International Covenant on Civil and Political Rights (ICCPR), has stated that Article 2(1) of the treaty requires state parties to take affirmative steps to prevent both public and private actors from violating the rights and obligations of the ICCPR. *See* U.N. Human Rights Committee, *General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, para. 8, U.N. Doc CCPR/C/21/Rev.1/Add.13 (May 26, 2004) available at https://undocs.org/CCPR/C/21/Rev.1/Add.13.

(EAR).[14] Items that are controlled for national security or foreign policy purposes are listed under the Commerce Control List (CCL) of the EAR.[15] One of the primary "foreign policy" considerations that can lead to the inclusion of an item on the CCL is the "protection of human rights and the promotion of democracy."[16] In the 2019 National Defense Authorization Act (NDAA), Congress specifically authorized the executive branch to impose new regulations on the export of "emerging and foundational technology."[17] In November 2018, the Department of Commerce published an advanced notice of proposed rulemaking that signaled the Department's intention to promulgate new rules under the CCL for the export of various emerging technologies, including technologies related to "advanced surveillance."[18] Since this announcement, the Department of Commerce has refrained from placing any new restrictions on the export of AI-powered surveillance technologies. The Department of Commerce should use existing regulatory authorities to restrict the export of AI-enabled surveillance technologies to countries where human rights abuse is likely to occur.

- In order to immediately impose restrictions on the export of AI-enabled surveillance technology, the next administration should promulgate an interim final rule pursuant to § 742.6(a)(7) of the EAR and temporarily classify certain AI-enabled surveillance technologies under the Export Control Classification Number (ECCN) 0Y521 series.[19] By classifying AI surveillance technology under the 0Y521 series of the ECCNs, the Department of Commerce will have the authority to immediately impose licensing requirements on the export of such technology for up to one year.[20] Export licenses for items classified under the 0Y521 series are reviewed on a case-by-case basis.[21]

14 Congressional Research Service, R41916, *The U.S. Export Control System and the Export Control Reform Initiative*, p. 2 (last updated Jan. 28, 2020) available at https://fas.org/sgp/crs/natsec/R41916.pdf.

15 Ian F. Fergusson, Congressional Research Service, RL31832, *The Export Administration Act: Evolution*, Provisions, and Debate, p. 10 (Jul. 15, 2009) available at https://fas.org/sgp/crs/secrecy/RL31832.pdf.

16 *See* 50 U.S.C. § 4811(2)(D) available at https://www.law.cornell.edu/uscode/text/50/4811.

17 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1703(a)(6), 132 Stat. 1636 (2018).

18 Review of Controls for Certain Emerging Technologies, *supra* note 3.

19 An item may be added to the 0Y521 series of ECCNs if the Department of Commerce, in concurrence with the Departments of Defense and State, determines that "foreign policy reasons justify control." *See* Addition of Software Specially Designed To Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series, 85 Fed. Reg. 459 (Jan. 6, 2020) (to be codified at 15 C.F.R. § 744) available at https://www.federalregister.gov/documents/2020/01/06/2019-27649/addition-of-software-specially-designed-to-automate-the-analysis-of-geospatial-imagery-to-the-export.

20 *Id.*

21 *Id.*

Photo by Codelco

- To permanently control the export of AI-enabled surveillance technology, the next administration should use the notice and comment rulemaking process and amend the list of items that are controlled under the "Crime Control and Detection" provision of the CCL (15 CFR § 742.7) to include all devices, technology, and software that are used for the identification or analysis of human biometric features, including but not limited to facial recognition technology, DNA sequencing, iris and retinal recognition, and speech recognition.[22] Under § 742.7, export license applications are "considered favorably" unless "there is evidence that the government of the importing country may have violated internationally recognized human rights."[23] As such, this effort should also provide a comprehensive, regularly updated list of countries and entities for whom a license application would be subject to a presumption of denial due to the risks of implication in human rights abuse. The proposed expansion of § 742.7 will provide predictability and clarity to American exporters, and thereby facilitate business planning in emerging markets while protecting American companies from inadvertently supplying end users that are likely to engage in human rights abuse.

Finally, in line with the actions above and the final recommendation below, the new administration should work with like-minded allies to coordinate multilateral arrangements for any new controls directed against end-users presenting high risk of human rights abuse.

✓ Use the Global Magnitsky Act and E.O. 13818 to prevent U.S. firms from providing financial support to foreign companies that manufacture AI-enhanced surveillance technology for authoritarian regimes

The next administration should identify foreign companies that are developing and selling AI-enabled surveillance and biometric data collection technologies to authoritarian regimes and, where appropriate on the basis of support to sanctionable activity, designate those companies under the Global Magnitsky Human Rights Accountability Act and Executive Order 13818.[24] (For a detailed analysis of and recommendations concerning the Global Magnitsky Act and similar targeted human rights and anti-corruption sanctions,

22 One of the stated goals of the "Crime Control and Detection" provision of the CCL is to prevent human rights abuse abroad. *See* 15 C.F.R. § 742.7 (b) (noting that "[t]he judicious use of export controls is intended to deter the development of a consistent pattern of human rights abuses, distance the United States from such abuses and avoid contributing to civil disorder in a country or region.").

23 *Id.*

24 The Global Magnitsky Human Rights Accountability Act, 22 U.S.C. § 2656 note (2016) available at https://www.humanrightsfirst.org/sites/default/files/GMA-Law.pdf; Executive Order 13,818, Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption, 82 Fed. Reg. 60839 (2017) available at https://www.humanrightsfirst.org/sites/default/files/eo-13818-glomag.pdf.

see the *Walking the Talk* chapter entitled "2021 BLUEPRINT FOR POLICYMAKERS: Targeted Human Rights and Anti-Corruption Sanctions Programs.") Foreign firms that are "designated" under E.O. 13818 are added to the Department of Treasury's Specially Designated Nationals and Blocked Persons (SDN) list. Under existing law, U.S. persons and companies are prohibited from "making any contribution or provision of funds, goods, or services" to a listed entity.[25] By using E.O. 13818 to sanction foreign firms that are selling AI-enabled surveillance technology to known human rights abusers, the next administration will prevent these companies from accessing the highly sought-after financing of U.S. based private equity and venture capital firms. Additionally, such sanctions will bar U.S.-based academic institutions, such as research universities, from collaborating or otherwise partnering with designated foreign companies. Related actions should include:

- Establishing an inter-agency team comprised of representatives of the Departments of Commerce, Treasury, and State to publish predictable, credible thresholds of sales or export activity that could trigger designation for sale or transfer of AI surveillance-related technology to human rights abusers likely to have committed sanctionable acts under the Global Magnitsky Act and E.O. 13818, and to monitor the global AI-powered surveillance market and identify incidents of such activity warranting designation.

- Designating under Section 1(a)(iii)(A) of E.O. 13818 any foreign entity that is identified by the interagency task force as having provided goods or services, including but not limited to devices, technology, or software that are used for the identification or analysis of human biometric features, to a government entity that has engaged in sanctionable violations of internationally recognized human rights.

✓ Negotiate additions to Wassenaar Arrangement (WA) on export controls for conventional arms and dual-use goods and technologies

Export controls are only effective when they substantially limit the global availability of the controlled product. In the case of advanced surveillance technology, Chinese firms account for the majority of global exports (with American companies coming in a distant second place).[26] According to the Carnegie Endowment for International Peace, Huawei alone has exported advanced surveillance products to 50 different countries.[27] Due to China's dominance of the global market for advanced surveillance tech, export controls imposed unilaterally by the United States will have only limited impact on the proliferation of these technologies. In addition to the steps outlined above, therefore, the next administration will have to rely on U.S. diplomacy to push the international community to adopt a global control regime for the export of AI-enabled surveillance technology. This diplomatic effort should begin with the modernization of the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The WA is a voluntary multilateral export control framework that establishes guidelines for the creation of national export restrictions on goods that have a foreseeable impact on international security and stability.[28] Forty-two countries participate in the

[T]he next administration will have to rely on U.S. diplomacy to push the international community to adopt a global control regime for the export of AI-enabled surveillance technology.

25 Executive Order 13,818, *supra* note 24, at § 4(a).

26 Feldstein, *supra* note 5, at p. 9.

27 *Id.*

28 The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, *About us*, available at https://www.wassenaar.org/about-us/. Although human rights impact is not a traditional criterion for listing, advanced surveillance technologies could be covered under several existing categories due to the potential military application of such technologies. *See* Tim Maurer, Edin Omanovic, Ben Wagner, New America Foundation, *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*, p. 28 (Mar. 2014) available at https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf. In 2017, the head of the Wassenaar Arrangement, Philip Griffiths, stated in an interview that "new technologies," such as AI, "remain [a] focus" of the WA. See Rainer Himmelfreundpointner, *Wassenaar Arrangement: "Global risks have greatly expanded."*, Cercle Diplomatique, Issue 01/2017, p. 63 (2017) available at https://www.wassenaar.org/app/uploads/2019/consolidated/CD_012017_Interview.pdf.

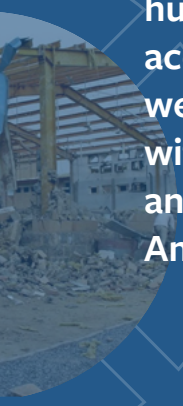
WA and coordinate their export controls with the WA's Dual Use and Munitions List.[29] Although China is not one of the 42 participants, the country's conventional weaponry control list mirrors the Wassenaar Arrangement's Munitions List.[30] By amending the WA's Dual Use List to include technologies that are critical to the creation or maintenance of AI-enhanced systems of surveillance, the international community will limit the export of these technologies by WA participants and pressure non-WA participants, such as China, to adopt similar restrictions. Related actions should include:

- Working with members of civil society and the U.S. tech industry, the next administration should draft a narrowly tailored amendment that would expand the WA Dual Use List to control devices, technology, and software that enable the identification or analysis of human biometric features, including but not limited to facial recognition technology, DNA sequencing, iris and retinal recognition, and speech recognition; spyware powered by deep learning algorithms; and tools used to surveil social media for the purpose of persecuting government critics and dissidents.
- At the next meeting of WA members, the U.S. delegation should propose the adoption of the draft additions, either under an existing category of the WA Dual Use List or through the establishment of an entirely new category.

29 The 42 participants include the United States, all EU member states (with the exception of Cyprus), and other major tech exporters, such as Russia, Turkey, Canada, Mexico, South Africa, Japan, and South Korea. *See* Maurer et al., *supra* note 28, at p. 27.

30 *See id.*

Human Rights First challenges the United States to live up to its ideals. When the U.S. government falters in its commitment to promote and protect human rights, we step in to demand reform, accountability, and justice. For over 40 years, we've built bipartisan coalitions and partnered with frontline activists, lawyers, military leaders, and technologists to tackle issues that demand American leadership.



humanrightsfirst.org

@humanrightsfirst

@humanrightsfirst

@humanright1st