August 11, 2017

Via e-mail: MyLanh.Graves@Vermont.gov

My-Lahn Graves
Office of the Attorney General of Vermont
109 State St.
Montpelier, VT 05609

RE: Statement to The Data Broker Regulation Working Group

Dear Working Group Members:

On behalf of Amnesty International, I am here to welcome this discussion regarding the data broker industry in Vermont.

Amnesty International is a global movement of more than 7 million people who are campaigning for a world where human rights are enjoyed by all.

My comments take as their starting point international human rights law. Governments have binding legal obligations to protect human rights under international law. But businesses also have a responsibility to respect human rights. This is expressed most clearly in the United Nations Guiding Principles on Business and Human Rights (UNGPs), which make clear that, among other things, businesses must undertake human rights due diligence to identify,

prevent, mitigate and account for the possible human rights impacts of their operations. Companies must also be transparent so that people are fully aware of how their rights may be affected by their operations.[1]

What are some of these possible human rights impacts, with regards to data brokers?

In February of this year, Amnesty International, together with a coalition of 16 other experts, non-governmental organizations and academic institutions, addressed a joint letter to nearly 50 data brokers and analytics companies.[2] In light of political discussions calling for increased deportations, and talk of a so-called "Muslim registry," we called on these companies to take a pledge – consistent with their responsibility to respect human rights under the UNGPs:

> "We will not allow our data, or services, to be purchased or otherwise used in ways that could lead to violations of the human rights of Muslims or immigrants in the United States. If we cannot guarantee that our data, or services, will not ultimately be used for such purposes, we will refuse to provide them."

We received only 7 responses, of which only 4 were willing to make this pledge, albeit some with caveats.

This is a worrying sign. The potential for human rights harms from the collection, storage, sale, and analysis of large amounts of data is considerable. In our research, it took only a few clicks for us to find a list of 1.8 million names and addresses of Muslims in the US.[3] This is remarkable since the US census has considered religious information too sensitive to collect, and refused to do so since the 1950s. Similar lists of people believed to be undocumented migrants were similarly easy to come by.

It is important to note that such profiles of people based on

---

[1] United Nations Guiding Principles on Business and Human Rights, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[2] Amnesty International, *Tell Data Brokers: Do Not Help Build A Muslim Registry or Facilitate Mass Deportations*, 27 February 2017, AMR 51/5784/2017, https://www.amnesty.org/en/documents/amr51/5784/2017/en/

[3] Amnesty International, *Why Build a Muslim Registry When You Can Buy It?*, https://medium.com/amnesty-insights/data-brokers-data-analytics-muslim-registries-human-rights-73cd5232ed19

their protected characteristics, such as their race, religion, sexual orientation or gender identity, can be discerned or inferred from analysis of seemingly innocuous pieces of data. As Georgetown Law Professor Paul Ohm has noted, "privacy harms can cascade in unexpected ways." Not only is there a risk that ostensibly anonymized data, such as movie preferences or internet search queries, can reveal a unique identity, but also that with advances in machine learning, it is increasingly simple to profile someone, or discern their protected characteristics, based on inference.

The human rights harms that could flow from this, even beyond the threats to privacy, are multi-faceted.

Data or inferences about us are increasingly being used in decision making processes in all areas of our lives – from sentencing and bail decisions,[4] to university admission,[5] to hiring and firing. As the mathematician Cathy O'Neill makes clear in her book, *Weapons of Math Destruction*, the risk of error or unfairness from such decisions is significant, either due to inaccurate data, or flawed decision making, and often disproportionately impacts on the less economically well off, or on members of minority groups.

Additional human rights risks are presented by the increased use of private data brokers by government agencies specifically.

At least one "predictive policing" software – Beware - is reportedly making use of commercially available datasets to make individualized determinations of risk of future criminal activity.[6] Increasingly, police departments across the country are making use of data analytics by private companies to make predictions about crime in specific neighborhoods or "hotspots". There is much we don't know about how this functions, but already there is cause for concern. Researchers at the Human Rights Data Analysis Group have demonstrated, through the use of public health

---

[4] Human Rights Watch Advises against Using Profile-Based Risk Assessment in Bail Reform, https://www.hrw.org/news/2017/07/17/human-rights-watch-advises-against-using-profile-based-risk-assessment-bail-reform.

[5] Cathy O'Neill, *How Big Data Transformed Applying to College: It's Made it Tougher, Crueler and Even More Expensive*, Slate Magazine, http://www.slate.com/articles/business/moneybox/2016/09/how_big_data_made_applying_to_college_tougher_crueler_and_more_expensive.html

[6] Upturn, Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights, August 2016, https://www.teamupturn.com/reports/2016/stuck-in-a-pattern

data and a reconstructed commercial predictive policing algorithm, that such tools can reinforce and amplify existing discrimination in policing practices.[7]

The risk of error in databases or analysis poses substantially more severe risks where law enforcement is concerned, as what is at stake is not a line of credit, but one's liberty, or even life.

Data brokers also have importance for the issues of surveillance and privacy. Federal intelligence, law enforcement, immigration, or other agencies can - and do - easily access private information provided by data brokers.[8] As Professor Ohm has also written: "Our mental image of the FBI agent conducting surveillance, wearing headphones in a white van parked on the curb, clipping alligator clips to telephone wires, and working with a white-coated FBI scientist will soon be replaced by an agent sitting in his office, hitting the refresh button on his web browser, and reading the latest log file dump sent from private industry."[9] While surveillance may be used for completely legitimate purposes consistent with human rights law, it may also be abused, and it is of concern if the data broker industry allows authorities to in effect do an end run around the 4th amendment by purchasing private information about Vermonters that they would be barred from gathering on their own.

There may be many more human rights risks of which we are not aware, because there is much we don't know about how our data is used. This highlights the need for transparency.

Regarding this point on the importance of transparency, I would like to speak about Belarus.

I visited Belarus in 2015 to conduct research on the impact of secret surveillance on civil society there.[10] Surveillance in

---

[7] Kristian Lum and William Isaac, *To Predict and Serve?* Significance, 7 October 2016, http://onlinelibrary.wiley.com/doi/10.1111/j.1740-9713.2016.00960.x/full

[8] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. Int'l L. & Com. Reg. 595 (2003), Available at: http://scholarship.law.berkeley.edu/facpubs/678

[9] Paul Ohm, *The Fourth Amendment in a World Without Privacy*, Mississippi Law Journal, Vol. 81, No. 5, p. 1309, 2012: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2073574

[10] Amnesty International, *It's Enough for People to Feel it Exists: Civil Society, Secrecy and Surveillance in Belarus,* EUR 49/4306/2016:

Belarus is conducted on the basis of vague laws, and via a system known by the acronym SORM, whereby the KGB and other state agencies can directly access communications data without alerting telecoms providers and without adequate oversight. As a result, people are left constantly suspicious that they may be subject to surveillance at any time. This is especially problematic for civil society activists since many routine activities protected by human rights law, such as holding an unauthorized protest or soliciting funding from a foreign donor, can lead to legal problems, or even criminal punishment.

The reason I mention this is because most of the harm that flows from this system of secret, unlawful surveillance, comes from the uncertainty that surrounds it, from the chilling effect that flow from a lack of transparency. For that reason, the title of this report is, "It's Enough for People to Feel It Exists," based on one activist's characterization of how surveillance kept civil society in line. Activists there jokingly refer to mobile phones as "the police officer in your pocket." You cannot know whether your phone is tracking you or listening to you – but it could be.

This self-censorship – the act of refraining from exercising one's rights out of fear – is itself a human rights concern, as the Grand Chamber of the European Court of Human Rights noted in the case of *Zakharov v. Russia*.[11] In that case, the court considered the surveillance system in Russia, that is in many ways identical to that in Belarus, and ruled that in situations where the law is so vague that anyone could be subject to surveillance, and where subjects of surveillance do not have a legal remedy, "widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified... In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right [to privacy]."

And this interference is visible on the ground in Belarus. Activists fear their offices are bugged, their phone calls listened in on, their locations tracked and their online communications at risk of hacking. The most basic and crucial daily activities of activists – discussing politics, organizing a

---

https://www.amnesty.org/en/documents/eur49/4306/2016/en/

[11] Case of Roman Zakharov v. Russia, 47143/06, 12/4/15, http://hudoc.echr.coe.int/eng?i=001-159324, para. 171.

meeting, making phone calls, arranging public protests, raising funds – are made fraught and difficult, undermining their ability to function.

While this may be a very different situation than the one facing Vermont, it should serve as a lesson on the importance of transparency. The internet of things is here, and only becoming more commonplace. As numerous speakers yesterday mentioned – we are producing more and more data from more sources all the time. If we cannot know or control the uses to which that data may eventually be put, or meaningfully predict the ways in which decisions or inferences based on this data may impact on our rights, then this is a human rights concern.

If we cannot know whether the websites we visit will be used to create a risk score for us that may be shared with government agencies, how freely will we seek out information or express ourselves online? If we cannot know whether our purchase history could be used to infer our sexual orientation and who might be able to access that inference, how might we self-censor in the marketplace? If we cannot know whether our location data or the people we associate with will reveal our irregular immigration status, how freely will we move around, or go to work, or school? Without transparency around the use of our data, the chilling effects that could come from the increased production and use of data could be significant.

It is worth noting that efforts to create regulation that will bear directly on the operations of data brokers are already underway elsewhere. A key example is EU's General Data Protection Regulation (GDPR), which comes into force in May 2018, and which will create new obligations on companies regarding allowing access to information about the storing or processing of personal information, erasing data in certain circumstances, protecting children's data and much more.

Such measures will help companies ensure that they meet their responsibility to respect human rights, particularly the right to privacy, and are transparent about their human rights impacts.

Importantly, the GDPR will apply to all companies processing the personal data of individuals in the EU, and so will apply directly to many US-based data brokers. Moreover, if existing US privacy protections are not brought substantially in line with the GDPR, it could jeopardise the current framework for transferring personal data between the EU and the USA, profoundly damaging

transatlantic business operations.[12] The Vermont legislature has an opportunity to take the lead in closing this gap.

For these reasons, Amnesty International makes the following recommendations for the regulation of data brokers in Vermont:

- **Human Rights Due Diligence**: Vermont should make explicit that data brokers have a responsibility under the UN Guiding Principles on Business and Human Rights to exercise human rights due diligence to identify, prevent, mitigate and account for the potential human rights risks of their operations. This includes putting strong systems in place to prevent the company contributing to human rights abuses through the sale of data or services to government agencies and other actors.

- **Right to Know**: A key requirement of the UNGPs is that businesses be able to show that they respect human rights – "showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted."[13] Accordingly, Vermont should ensure that data brokers make freely available easily accessible information about the information they hold, its sources, and purposes for which information is sought and sold. Vermont should consider a centralized, easy-to-use tool for people to opt out of the use of their data.

- **Non-discrimination**: Vermont should ensure that the services of data brokers are used neither with discriminatory intent, nor in ways that have discriminatory impact.

---

[12] See for example, Amnesty International and Human Rights Watch: *Joint Letter to European Commission on EU-US Privacy Shield*, https://www.hrw.org/news/2017/07/26/joint-letter-european-commission-eu-us-privacy-shield

[13] United Nations Guiding Principles on Business and Human Rights, Commentary to Principle 21, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf; See also United Nations Office of the High Commissioner for Human Rights, Report on the Right to Privacy in the Digital Age, A/HRC/27/37, 30 June 2014, para. 46, "In the context of information and communications technology companies, [the requirement of meaningful consultation with stakeholders in the UNGPs] also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions."

- **State Actors:** Government agencies that purchase data or services from data brokers must demonstrate that doing so will not harm human rights. To this end, they should be proactively transparent about the use of these products, including by making contracts publicly available, as well as disclosing the measures taken to ensure that data is accurate, and that data, or inferences, about people or groups of people will not lead to discriminatory, or otherwise unlawful outcomes.

Addressing these topics would help ensure that both state actors and private businesses act in accordance with human rights.

Thank you.