Cross-Community Working Party on
ICANN and Human Rights (**CCWP-HR**)

https://icannhumanrights.net/

Due Diligence and Why It Matters

Meeting Minutes | July 31, 2018[1]

PART I: Relevance to ICANN Community (Raphael Beauregard-Lacroix, NCSG)

- Human rights law originally set out to protect individuals against actions of the State (vertical arrangement), but human rights provisions are increasingly being enforced against other individuals or companies (horizontal arrangement), particularly in light of globalization and the increasing power of companies.
- The core aspect of ICANN's Human Rights Bylaw is that it "respect internationally recognized human rights *as required by applicable law*." As we've seen with GDPR, this can be hard to define: like laws around taxes and marital status, human rights-based laws aren't necessarily bound by territorial borders.
- Even if ICANN isn't violating human rights directly, there's a risk that its operations could prohibit, prevent, or otherwise interfere with governments' duties to protect the human rights of their citizenry.

PART II: What is Due Diligence? (Michael Samway, BHR Group)

- **Where does the term and concept of due diligence come from?** The law, specifically the US Security Act of 1933's sections on "reasonable care / investigation." The practical application of this is "doing your homework" on risks you might face. This concept gained universal application when the UN Human Rights Council unanimously endorsed the United Nations Guiding Principles on Business and Human Rights in 2011.
- **How does it apply to the ICT sector?** It's not just an international norm, but increasingly an industry norm as well. Microsoft, Google, and Yahoo were founding members of the multistakeholder Global Network Initiative (GNI, launched 2008), and now companies the likes of Facebook, Nokia, Orange, and BT are full members. A great resource on how due diligence applies to platforms, telcos, providers, and other ICT companies is GNI's Implementation Guidelines:
    - 2.4: "*Consistent with the UN Guiding Principles on Business and Human rights, and considering international human rights standards, participating companies will carry out human rights due diligence to identify, prevent, evaluate, mitigate and account for risks to the freedom of expression and privacy rights that are implicated by the company's products, services, activities and operations."*
- **What is an effective due diligence methodology in the tech sector?** It revolves around the when, who, and how.

[1] Agenda, transcript, and recordings available here:
https://community.icann.org/display/gnsononcomstake/Meeting+Notes

    - WHEN? Carry out impact assessments when entering a new market, partnership or joint venture, launching a new product, changing functionality of existing product (for example, moving away from encryption by default), etc.
    - WHO? Develop a cross-functional human rights team involving not just law and policy divisions, but also the engineering team, security, products, sales, corporate / business development, local team members, etc. Identify not only internal stakeholders, but external stakeholders in anticipation of consultation as part of the impact assessment.
    - HOW? Carry out consultations through interviews or questionnaires, perhaps under Chatham House Rule to elicit candid responses without fear of retribution.
- **How might an entity structure its due diligence procedures?** A sample workflow is outlined below. At the end of the process, the executive team should literally, physically sign off on the final report to indicate that they have read it and understand the risks and mitigation strategy.
    - Survey relevant human right law and principles (international or industry)
    - Identify HR landscape in the market (opinions by civil society, academics, press, etc)
    - Document legal and regulatory environment with regards to privacy and freedom of expression (i.e., mandatory censorship, data requests requirements, bulk surveillance, etc.)
    - Clearly describe company's strategy in the market (corporate structure, data storage, etc)
    - Identify risk points: Digital rights intersection points with company's products, services, and operations (CCWP schema)
    - Consider opportunities that the service may have to promote human rights
    - Develop risk mitigation strategy.
    - Establish internal policies / principles on human rights (namely the UNDHR) as a starting point.
    - Create cross-functional human rights team with people, budget, and internal accountability
    - Designate escalation path for rights-related issues
    - Plan for routine re-evaluation of risk and mitigation strategies
    - Create an accountability framework for the outcomes, both internally and externally. Transparency reports, external audits / evaluations made publicly available, etc.

PART III: Due Diligence for DNS Actors (Collin Kurre, ARTICLE 19 and Michele Neylon, Blacknight)

- ARTICLE 19 and Blacknight collaborated to refine a self-assessment model for registrars and hosting providers (while assessing the human rights impact of Blacknight's operations) as part of an ongoing collaboration between ARTICLE 19 and the Danish Institute for Human Rights to develop new due diligence tools for internet infrastructure providers.
- Blacknight's interest in getting involved with human rights impact assessments stemmed from an initial interest in producing transparency reports on user data and content takedown requests and how they're handled to reflect the company's values

and differentiate their business, products, and client relations.

- Communicating the value and relevance of human rights in the infrastructure industry remains a challenge, particularly because the term "human rights" may lend itself to interpretations that differ to what due diligence actually entails, which could exacerbate resistance.
    - Potential solutions: give context — such as a presentation to staff about HR and its intersection with internet governance — and clearly identify the scope and intersection points with the company / organization's work.
- While Blacknight hadn't yet adopted a high-level human rights policy commitment, certain elements of human rights due diligence were already firmly in place, such as staff trainings, data protection provisions, and processes for tracking and handling content removal requests.

PART IV: Discussion

- David McAuley referred to the UNGP concept that if you have leverage to get business partners or suppliers to uphold human rights principles, you should use it. While ICANN has plenty of leverage, using it could go beyond its remit and pull it into the content layer. Michele Neylon posited that the term "human rights" may lend itself to interpretations that differ to what due diligence actually entails, which could exacerbate resistance. Michael Karanicolas emphasized the need for defining scope, and Michael Samway emphasized the importance of contextualizing human rights and defining the intersection points with the company or organization's work.[2]
- Jonathan Makowsky highlighted the intersection between cybersecurity and human rights, and asked an administrative question allowing us to remind everyone that you do not need to be an NCSG or NCUC member to participate in the CCWP-HR — any interested ICANN community member is welcome to contribute.

[2] The CCWP-HR has previously undertaken efforts to do this, see: https://community.icann.org/display/gnsononcomstake/CCWP+on+ICANN+and+Human+Rights?preview=/53772653/79433998/ICANN%20and%20Human%20Rights%20Jan2018.pdf.