REIMAGINING DIALOGUE ON ONLINE PRIVACY

Prateek Pathak*

The paper proposes *a theory of change* in the form of an interactive online course which can be developed by academia and used by business (specifically information technology companies) to promote a meaningful dialogue on human rights (specifically the right to privacy) with different stakeholders in the national context. Indeed, our theory of change aims to promote meaningful dialogue within online community on whether business practises are actually sensitive to their human rights commitments under the UN Business and Human Rights (UN-BHR)

The recent revelation that USA's National Security Agency (NSA) was conducting mass surveillance on foreign communities by tapping into systems of technology giants like Google, Apple, Microsoft, Facebook and others has raised serious questions about lack of business obligation to protect the privacy of ordinary people. Similarly, the Octopus data leak fiasco in Honk Kong highlights the need for better regulations against irresponsible dissemination of personal data and related privacy breaches. Although, the private sector has played a key role in enabling new and dynamic forms of communication, it has also been criticised for snooping on user's personal sensitive data as well as facilitating state surveillance of individuals compromising user's right to privacy[1]. Little wonder then that cybersecurity expert Bruce Schneier observes that 'Surveillance is the business model of the Internet'.

These increasing incidents of violation of online privacy have raised the two important issues:-

1. There is a lack of explicit articulation of the content of the right to privacy which has contributed to difficulties in its application and enforcement in the cyber world.[2]

2. There is an increasing concern that national legal and policy standards might have not kept pace with rapid advances in information technology. These inadequate legal and policy standards have increased the risk of individuals being exposed to different human right violations including the violation of right to privacy due to increased surveillance by authorities holding positions of power[3].

In this period, the United Nations Economic and Social Commission for Asia and Pacific along with UN's International Telecommunication Union (ITU) have launched an interactive *Information Superhighway* map to show policy makers and investors the location of the missing links in the digital divide in the Asia-Pacific region.[4] The Asia - Pacific region is keen to convert its digital divide into digital opportunity. However, this opportunity can be fully realised only if online business practises respect human rights including the right to privacy.

---

*Prateek Pathak works as a Research Associate to the JGU Vice Chancellor.

[1] The right to privacy is enshrined by the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (ICCPR, art. 17), the Convention on the Rights of the Child (art. 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14). At the regional level, the right to privacy is protected by the European Convention on Human Rights (art. 8) and the American Convention on Human Rights (art. 11).

[2] UNESCO, Global Survey on Internet Privacy and Freedom of Expression, 2012, p. 51.

[3] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue(),p.13

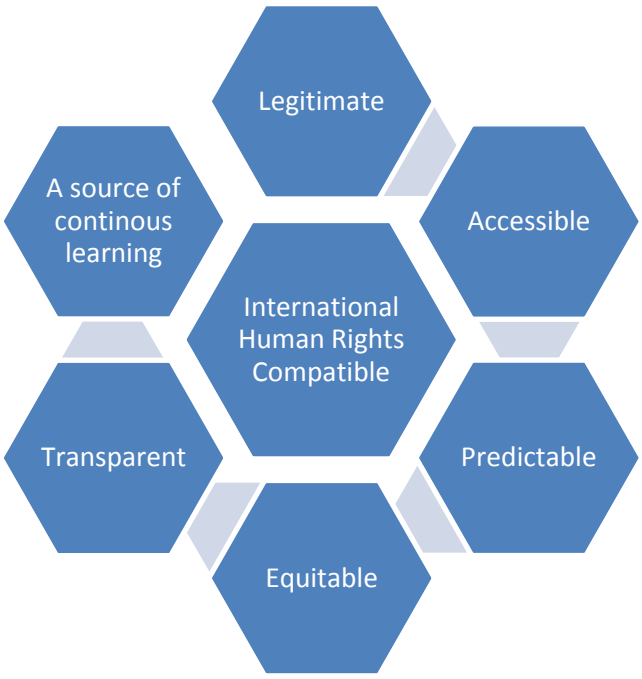
[4] http://gadgets.ndtv.com/internet/news/un-unveils-asia-pacific-information-superhighway-maps-to-expose-digital-divide-448437

Electronic copy available at: http://ssrn.com/abstract=2533087

It is important to note that the complex and trans-disciplinary nature of these issues in the online world as well as the involvement of different stakeholders (national government, private sector, civil society, international organisations etc.) warrant the need for a multi-stakeholder solution. Accordingly, there is a need to facilitate dialogue between online business and other stakeholders in the society for better identification and resolution of these issues. Indeed, this dialogue will be critical for IT firms to creatively design and provide IT services which value user privacy and subsequently improve their online reputation without compromising their business revenues

In this context, we propose a theory of change[5] which can be used to facilitate increased dialogue between business and other stakeholders especially its online customers/users for better articulation, application and enforcement of the right to privacy in the online world. The proposed theory of change includes an interactive online course which can be used to actively inform and engage online users with respect to their human rights including their right to privacy. This online course can be developed by academia (like IIT Bombay, O.P. Jindal Global University) in collaboration with business (like Google, Microsoft,TCS,Infosys etc.). The course should be designed to communicate user feedback and expectations to business with regard to their perceived progress on human rights commitments.

Further, this theory of change should promote awareness and deliberation on UN BHR principles which are based on 'Protect Respect and Remedy' framework in national context. Apart from right to privacy, this theory of change can be broadened and appropriately contextualised to include other human rights as well. Before proposing our theory of change, we firmly believe that any such initiative (which is sensitive to multi-stakeholder interests) should ensure that effective grievance mechanisms are available. With respect to our initiative, these mechanisms could be developed in future based on the following matrix of values [See figure 1] which are self-explanatory[6].

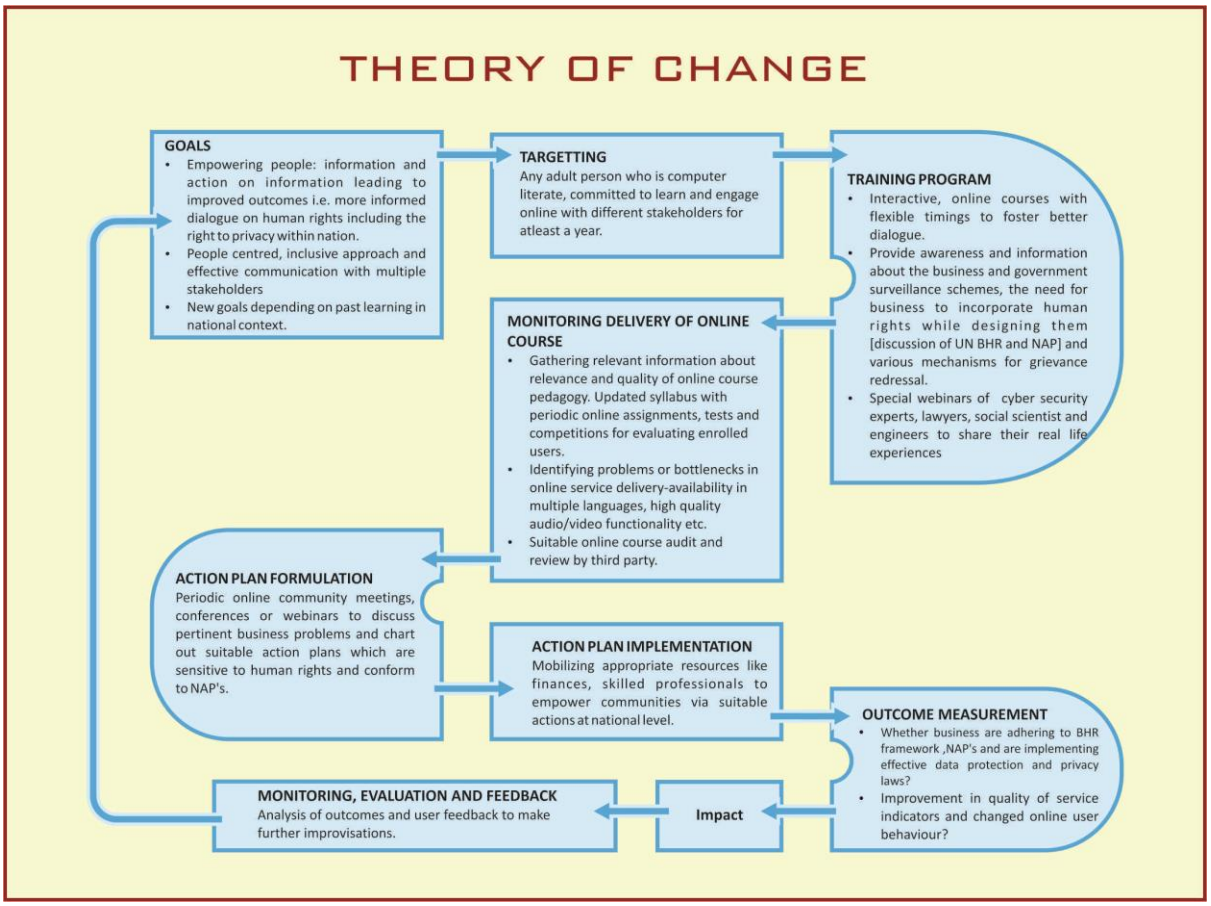


[*Figure 1: The matrix of values which should form the basis of an effective grievance redressel mechanism with respect to violation of individual privacy]*

THEORY OF CHANGE:

[5] http://blogs.worldbank.org/publicsphere/what-theory-change-and-how-do-we-use-it
[6] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie(2011).p.26

Electronic copy available at: http://ssrn.com/abstract=2533087



[*Figure 2: The iterative sequence of 9 steps which will help in better articulation and realisation of right to privacy through a win-win solution for all concerned stakeholders]*

Our proposed theory of change can be implemented through the following sequence of steps iteratively

Step 1: Goals: First, we need to determine the set of goals which should define the nature of intervention to bring about the desired change. Some of these possible goals have been illustrated in Figure 2

Step 2: TARGETTING: Any adult person who is computer literate and willing to commit around 5hrs a week for one year. There are no restrictions with respect to caste, class, educational status, gender etc. of participants. The program will be targeted to closed user group to minimize spillover effects.

Step 3: TRAINING PROGRAM: An interactive online course will commence upon enrolment of suitable number of adults. The training program shall be of duration of not more than 40 weeks/2-3 hours per week. It can be conducted in local languages, with flexible timings .The pedagogy will be application oriented with suitable emphasis on relevant legal, policy and business theories.

IT policymakers, computer engineers, social scientists and cyber lawyers will be specially invited to participate in online discussions, apart from regular academics. This is because they are generally more aware of real time bottlenecks and can provide useful insights in online discussions. Additionally, their experience and contacts will help in effective implementation of ideas proposed during the discussion at national level.

An application oriented training program also requires an understanding of policy debates on existing business process at national level. Accordingly, participants will be asked to identify problems in existing online world (e.g. lack of judicial oversight, whether laws and policies are reasonable or not, how unregulated surveillance/snooping contributes to lack of transparency and accountability) and will also be tested on their consequent actions (e.g. whether they actually lodge a complaint against relevant cyber tribunal or contact grievance officer in case of grievances).

Information collected by participants in this stage may be useful for further interventions. For example, the fact that engineers are not properly trained in ethics of privacy should explain poor quality of data security practises. Accordingly, these participants can advocate for business policies requiring technology companies to suitably train their engineers as well as provide them incentives for safeguarding user privacy.

Step 4: MONITORING DELIVERY OF ONLINE COURSE: The online course should be continuously updated to keep pace with rapidly changing nature of online issues. It should test user's understanding and learning outcomes through assignments, tests and online competitions like online debating, group discussion, quiz, mooting, COASE BRIEF COMPETITION etc .Online course delivery should also be evaluated on technological parameters (quality of service like good audio/video, functionality of high speed internet etc.)

Step 5: ACTION PLAN FORMULATION: Virtual community meetings or physical group meetings of around 1hr each can be designed starting from 5th week to collectively deliberate on problems, brainstorm possible solutions and formulate suitable action plans, based on grievances and problems identified by the participants. An effort should be made to synchronise these plans with the National Action Plan

Step 6: ACTION PLAN IMPLEMENTATION: Once an action plan is formulated, all the stakeholders and resources are mobilized to implement it. Tools like online advocacy through social network, RTI, PIL's etc. and various fora like meetings with entrusted decision makers (government officials. policy makers) are strategically used to push pertinent demands for improved outcomes.

Step 7: OUTCOME MEASUREMENT: To measure the efficacy of an action plan, it is not only necessary to define the outcomes but also measure them at appropriate intervals. Such an outcome measurement should be carried out keeping the following two dimensions in mind.

a. Conformance to human rights framework

We need to define and measure outcomes which assess whether business are exercising due diligence and are conforming to UNBHR framework and as mentioned in National Action Plans based on participant survey and feedback.

b. Change in online user behaviour

There is a need to develop a set of indicators pertaining to change in online user behaviour which are tangible, easy to measure (like increased user alertness, increased number of complaints, increased participation in community mobilization activities etc.) and understand their contribution to eventual evolution of cyber jurisprudence

Step 8: IMPACT ASSESSMENT:

Setting goals and measuring outcomes is incomplete in itself. There is a need to understand the impact of change on online user community.

Some of possible impacts of this intervention which should be assessed include.

- Better online governance and more profits for IT companies
- Safety of human rights like privacy at national level without much cost to IT firms.
- Empowerment of individuals in the online community at national level.

Step 9: MONITORING, EVALUATION and FEEDBACK:

We need to analyse the existing strategies to learn valuable lessons that contribute to more effective further actions at national level .This is important because it is necessary to combine creativity with lessons learnt as it might help us to proactively tackle potential pitfalls.

We are completely cognizant of the fact that our proposed theory of change is based on certain assumptions- enrolled users will actually stay committed for atleast one year, change in behaviour of users is only due to active participation in online course, technology facilities like high speed internet connection will not fail anytime, online issues have no effect on offline users and people with no access to internet, internet is a global public good whose governance can be effectively influenced by national governments etc. These might not always hold true and expected outcomes might be very different. Still, we firmly believe that our proposed theory of change can prove an important starting point for promoting a more impactful and informed dialogue on business and human rights within online user community at national level.