Technology and Human Rights

From product misuse to labour abuse, technology and communications companies are increasingly exposed to risks that may be challenged in the court of public opinion. TwentyFifty’s Luke Wilde and Monique Bianchi outline why CEOs must think ahead.

Modern communications capabilities have transformed the world; connecting markets, reconnecting old friends and even democratising states. But as the companies that bring us these capabilities have grown in size and influence, questions have started being asked as to whether they are always ‘a good thing’.

It seems that in the information, communications and technology (ICT) industry there is a fine line between being on the side of ‘good’ or ‘evil’, with companies being accused of impinging privacy, aiding repressive regimes and sustaining conflict – not to mention the alleged labour abuses recently reported in Chinese factories manufacturing the iPhone.

ICT companies, more than most, have a wide range of risks and impacts that must be identified and addressed, from product misuse, breaches in security and freedom of speech to the more familiar issues such as labour and sourcing issues. To avoid incurring damaging public opprobrium there are a number of elements that companies operating in this field need to consider.

**THE COST OF OPERATING IN ‘BADLANDS’**

The Arab Spring highlighted the dilemmas that business faces when operating in, or supplying to countries with repressive regimes. The role that mobile phones and social media played in helping opposition
activists to connect, coordinate protests and distribute news of their suffering has been much reported and lauded.

However, Vodafone found itself criticised by non-governmental organisations (NGOs) for allowing messages to be sent over its network by the Mubarak government and later complying with the government’s demands to shut down its network at a critical point in the protests in Tahrir Square. Not doing so would have contravened its licence, may have put its employees at risk and led to a delay in restoring the network if it had been closed down by the government, not the company.

Elsewhere technologies sold by Western companies which can be used for surveillance have come under focus. For example, Nokia-Siemens has faced public condemnation for providing Iran with censorship and surveillance technologies which the European Parliament described as ‘being instrumental in the persecution and arrest of Iranian dissidents’.

Nokia-Siemens has subsequently pulled out of Iran and committed not to work with governments which use its technology to commit abuses, but its technology remains in the country. And, in response to a recent Pakistan government tender for the installation of surveillance technology, public pressure led to several companies, including Websense, Verizon, Cisco and Sandvine, making public statements that they will not tender due to human rights concerns and the government has since withdrawn the tender.

THE RIGHT TO PRIVACY

In the West, there is growing awareness and concern about the use to which companies put information about private individuals; for example, the ease by which customer’s private details can be accessed by apps on smartphones.

In a US class action, companies including Facebook, Apple and Google are being sued for allegedly passing on address book data held on smartphones without users’ permission. The suit alleges invasion of privacy, intentional interception, disclosure or use of wire or electronic communication, breach of computer security, negligence, unjust enrichment and racketeering, among other claims.

Apple has responded quickly and has stopped developers from accessing contact lists without users’ explicit permission to respect users’ right to privacy. Meanwhile the European Protection Commission is considering whether Facebook’s data protection policy is breaching EU privacy rules: the company’s vast user data store is its most valuable asset behind its upcoming public offering that has valued the company at more than £3 billion.

SUPPLY-CHAIN SCRUTINITY

ICT companies are also being challenged in areas beyond the use of their product and services. Component materials sourced from areas of conflict are under the spotlight.

ICT companies, more than most, have a wide range of risks and impacts that must be identified

The introduction of section 1502 of the Dodd-Frank Act in the US, requires companies to disclose whether minerals such as coltan, tungsten, tantalum, tin and gold have been sourced from the Democratic Republic of Congo or ‘any adjoining country’. This has required companies to look anew at their complex supply chains.

One of the industry’s responses has been the conflict-free smelter (CFS) programme. The CFS is a voluntary programme in which an independent third party evaluates a smelter’s procurement activities to check that the materials they process originate from conflict-free sources. As the world’s most valuable company, it’s not surprising that Apple is getting particular attention from NGOs and other campaigners: the thorny old problem of factory conditions in Asia, particularly in China, remains at the fore.

Apple has recently published a review of the labour practices at FoxConn, its major supplier, undertaken by an independent third party, the Fair Labor Association. It found major problems in areas like payroll, working schedules and health and safety risks, which show that the social and human rights landscape for these companies is not simple.

However, these initiatives have come about in reaction to public campaigns and if companies are to navigate changing social expectations, tightening environmental limits, remain commercially competitive and keep on the side of ‘good’, they need to be thinking ahead and acting ahead.

Leaders in the industry are looking into what human rights due diligence in particular high-risk regions or product segments might encompass and to seek to build the knowledge to act mindfully of the changing social and market dynamics into their practices.

© Criticaleye 2012