30 ARTICLES ON THE 30 ARTICLES

THE UNIVERSAL DECLARATION OF HUMAN RIGHTS AT 70: STILL WORKING TO ENSURE FREEDOM, EQUALITY AND DIGNITY FOR ALL

Article 12: Right to Privacy

Should schools use cameras in the classroom to monitor children's faces and determine whether they are paying attention? Would you use free WiFi at a street kiosk if you knew its cameras and sensors were collecting data on you, and that you would continue to be tracked even after you left the WiFi zone? If you wear a fitness tracker on your wrist, how would you feel if an insurance company used its data to deny you coverage?

These are not fragments of a dystopian nightmare, but very real issues of our digital age that could not have been foreseen in 1948 by the drafters of the Universal Declaration of Human Rights (UDHR). Yet the concept of privacy, enshrined in Article 12, has in fact become ever more central to all our lives over the last 70 years, with the increase in data collection by governments and business.

Privacy is often asserted as a "gateway" right that reinforces other rights, online and offline, including the right to equality and non-discrimination, and freedom of expression and assembly.

However, privacy is also a value in itself, essential to the development of human personality and protection of human dignity, one of the main themes of the UDHR. It allows us to protect ourselves from unwarranted interference in our lives, and to determine how we want to interact with the world. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information.

Privacy is not an absolute right, and can be limited in some cases, such as prison authorities searching cells for contraband. However, intrusions on privacy have to be in proportion to the benefit to society. The European Court of Human Rights, for example, ruled in 2000 that it was not "necessary in a democratic society" for the secret service to amass a dossier against a Romanian citizen including details (some false) dating back 60 years.

Privacy, especially digital privacy, can seem an abstract concept. As concerns about terrorism have mounted in recent years, governments have sought to intrude ever more into citizens' privacy, citing national security as the reason. "If you have nothing to hide," so the argument goes, "what are you worried about?"

Perhaps the value of privacy can be more easily understood in the physical world. Suppose someone broke into your house and didn't take anything, but snooped into your closets and read your private letters. Such an intrusion would make most of us feel, at a minimum, uncomfortable. Yet something very similar is happening today in cities blanketed with closed-circuit TV cameras, with companies that sell information about your online search history, and with government surveillance of individuals.
Sometimes we choose to surrender aspects of our privacy. Whenever we order something online, or use a free WiFi service, we give up some privacy in exchange for something of value.

However, individuals are not always aware of what they are surrendering, or to whom. They may not know that when whenever you get something free in the digital world, you are not the customer, you are the product. In 2018, some 87 million Facebook users discovered they had been turned into a commodity – without their knowledge or permission – when their browsing habits, purchases, political opinions and networks of friends were analysed and sold for profit.

> "Governments in every region are also using digital surveillance tools to track down and target human rights defenders and people perceived as critics – including lawyers, journalists, activists on land rights or the environment, and people who support equality for members of the LGBTI community."
>
> – **Michelle Bachelet, UN High Commissioner for Human Rights, November 2018**

Privacy defenders are also concerned that many uses of technology presented as an advantage may have a darker side. Some insurance companies offer a discount to customers who can prove their health habits by wearing a tracker. Is it a big leap to their denying insurance to those who decline to wear the "smart" wristband? You may be happy to "smile and pay" – use facial recognition as a shortcut to your bank account. But what if your face becomes part of a massive government surveillance scheme that can track you anywhere?

Massive data banks now hold information – search history, location, financial and health data – on every single woman, man and child in certain parts of the world. This does not mean "everyone perceived to be a critic or an activist, or even every Internet user, but quite simply: everyone," says the UN High Commissioner for Human Rights, Michelle Bachelet.

The extent of global government snooping came to light in 2013 when former Central Intelligence Agency (CIA) contractor Edward Snowden leaked classified information from the U.S. National Security Agency. According to the leaks, some 90 percent of those whose communications had been intercepted, were not the intended targets, but ordinary people. This has major ramifications, as collecting and linking many types of information on individuals could be abused to determine their "social value" to reward or blacklist them in ways they know nothing about.

Around the world, some are fighting back in order to preserve privacy. Public pressure has caused many companies to tighten their digital security and offer fully encrypted communications services to their customers. Some governments are adopting legal frameworks that protect individuals against intrusions by States and businesses. And

such boundary-breaking projects as building a “smart” neighbourhood in Toronto are facing increased scrutiny of their data practices. “I imagined us creating a Smart City of Privacy, as opposed to a Smart City of Surveillance,” wrote Ann Cavoukian, a leading Canadian privacy expert, as she resigned from the project.

Seventy years on, the UDHR offers a clear framework to secure the dignity and rights of all people, even in a digital age its drafters could not foresee. UN Human Rights Chief Michelle Bachelet says human rights lawyers, computer scientists and engineers, and government representatives have to work together “to ensure the continued application of human rights in the way in which States operate in the digital age, and in the way in which they regulate the activities of companies in the digital space.”

To read more, and view a video, on this topic go to:
https://www.ohchr.org/EN/NewsEvents/Pages/DigitalPrivacy.aspx

This is one in a series of articles published by the Office of the High Commissioner for Human Rights (OHCHR) to mark the 70th anniversary of adoption of the Universal Declaration of Human Rights on 10 December 1948. All rights enshrined in the UDHR are connected to each other, and all are equally important.

To read the previous articles in this series, please visit:
https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23871&LangID=E