A Realist Critique in the Eyes of Privacy and Human Rights

*“Realists reject human rights promotion because they regard the pursuit of human rights as an unnecessary, sometimes even a dangerous extravagance, often at odds with the national interest. Statists or legalists reject human rights promotion in target states because it represents an unwarranted intrusion into the domestic affairs of others and an infringement upon the principle of state sovereignty. Relativists or pluralists view human rights promotion as a form of moral (cultural) imperialism”*

*(Charles Kegley and Shannon Blanton 2013, 447-448).*

The pursuit of human rights was born out of conflict, either between equal citizens or oppressive systems. The law as we know it, with constitution and amendments of all sorts, seeks to properly protect citizens and systems, and grant them rights. It is no coincidence that most often than not - but not necessarily always - the law aims to protect human rights. After all, even if the denomination of ‘universal human rights’ is new, what it represents is as close to humanity as a physical presence: every person has inherent rights to intangible things that manifest as the ability to act (or restrain) upon certain elements. Violence and conflict have historically arisen only when “necessary”, but it was otherwise accepted that such behaviors were not usual, or at the very least, not normally needed.

In the United States, several articles and amendments embody in local law what the declaration of human rights guarantees. For instance, Article 8 of the UDHR, the right to a private life, is clearly reflected in the 4th amendment. It doesn't matter who or which one came first, so much as they are equal. The discussion of this amendment has traditional referred to physical, tangible things and places, but has not adapted completely yet to the ever-changing panorama of information exchange: communication through a computer is not physical as a telegram is, and so it has been argued that it should not be protected by this amendment. However, just as human rights, laws are - or should - be interpreted as timeless and applied to what they represent, and not necessarily exclusively to what they specifically say. ‘The law should be interpreted in spirit’, is what it has been called, as opposed to be followed word to word. Two cases, ‘Olmstead & Katz vs United States (1928)’ and ‘Carpenter vs the United States (2017)’ have been taken to the Supreme Court to argue how privacy - and so the fourth amendment - should protect citizens from the ever-growing misuses of technology. The United States holds a unique position in the world: being one of the most powerful countries there is, whatever is ruled here has a precedent for what other countries might or might not do. Considering that most major technological advances in communications and technology have been done there, whatever decisions it makes in terms of what is legal and what is not, how citizens can protect themselves etc., also has a deep impact in how other countries manage their own systems, not only in the laws they might adopt, but also in the way they have to behave without adopting them. For example, the EU set a precedent by adopting and enforcing the GDPR: since it protects the EU citizens anywhere they might stand, other countries’ companies had to change their policies to comply with other countries’ laws.

The realist position regarding human rights - the claim that they are utopian, and so unattainable, and might even go against national security by disregarding the measures a government has to take to protect its citizens - supports many of the controversial stands that surround technology. Realists would argue, considering the many tools technology offers, that things such as mass surveillance and backdoors would benefit national security:

“(..) *the traditional realist view that national security is essentially the freedom from fear of attack by another country or non state terrorists. Realists maintain that armed aggression is a paramount security priority and that preparing for war to prevent war overrides every other security concern. (...) Therefore, "security" must be defined primarily in terms of each country's capacity to resist armed threats to survival and national values by either foreign enemies or insurgents at home. This definition puts the protection of entire states' interests above those of individual people.*” [add reference]

‘Armed aggression’ no longer refers to just traditional military arms such as missiles and guns, but also attacks to infrastructure, media and supply chain, which is what is colloquially referred as ‘cyberwarfare’. As such, investments of various kinds have been made by different governments - namely the United States, the UK, Russia and China - to have tools for both offense and defense. Mass surveillance, backdoors (access to devices that are not ‘normal’), agreements/collaboration with technology conglomerates for ease of information access, AI, drones, and search without warrant or proper cause are among the most discussed programs that these countries participate in, albeit with different means. Rumors of ‘cyberwarfare’ squads consisting of security and technology professionals of various kinds have been widely discussed, and the generally accepted 2016 election meddling by Russian adversaries has been attributed to their existence. Just this week, a mayor news outlet released a story of the Chinese government placing spies in the supply chain of Supermicro, a California based board manufacturer with operations in China, which affected the core infrastructure of mayor companies such as Apple and Amazon by giving an undisclosed third party the power to override certain critical hardware aspects and create a backdoor. The investigation is controversial and even thought to be fake, but also highly plausible with all things considered. Companies have outsourced most of their infrastructure production to other countries - India, Thailand, Mexico and China are among the most popular - in the name of cutting costs. But their products are so widely used and depended on, that an interested party in the same country could easily infiltrate and wreak havoc; these factories run under said countries’ laws, and so it would be harder to spot them. The products these companies produce are so widely available and used, that would it make the most sense to use them to get the information they want or need.

“*Promoting the rights and dignity of ordinary people around the world is a formidable*

*challenge. Yet, as global security analyst David Rieff notes, "The old assumption that*

*national sovereignty trumps all other principles in international relations is under*

*attack as never before." "Even in a world of security dilemmas, some societies will come to see the linkage between their long-term interest and the common good- at some times and places, states can overcome their bounded origins as sovereign security managers to act as 'global citizens'" (Brysk, 2009, p. 4).* ”

Ironically, it is the same permanent and persistent always-on communication that the internet created that has been the primary media for the arguments against the traditional realist approach. The internet allows for on-demand content and information transfer, not only for government and institutions but also for the common man. Where in the past only professionals and/or people in power would voice their opinion about a subject - and only through highly curated and limited media, such as books or newspapers - social media and websites have given rise to the empowerment of civilians by giving a way for other people to talk about the subjects. Information sharing has become much more accessible both in the format it happens, as well as who receives it and initiates it. This is not perfect, however, as such a huge network also allows for misinformation to spread very quickly and puts the responsibility in people to educate themselves properly as opposed to outlets to push the correct information forward; that by itself is another subject not relevant to the present argument. By allowing people to be connected, to share information and experiences, people saw each other as that: people, not enemies, not adversaries or otherwise wildly unknown parties. The realist point of view - that we do not know other people, that we should think the worst and be prepare for the worst, that everyone is out to get us - falls apart easily under proper and constant communication.

The realist pushes forward paranoia. When there are no further motives to fear the outsider, or even when there are, the insider will be doubted:

*“ (...) secure states do not automatically mean secure peoples. Protecting citizens from foreign attack may be a necessary condition for the security of individuals, but it is not a sufficient one. Indeed, during the last one hundred years far more people have been killed by their own governments than by foreign armies. All proponents of human security agree that its primary goal is a protection of individuals. But consensus breaks down over what threats individuals should be protected from (...)" [Human Security Centre (2006, p. 35)]*

In the name and case of national security, governments will go through a Machiavellian schema of justifying the goal of security to do unspeakable things to both their citizens and foreigners. The war on terror pushed this up to eleven, but it was there even before: from the Black Chamber that spied the world during WWI to the NSA’s PRISM program, multiple United States’ administrations have made a point of wanting to have information everywhere, from anything, whatever the cost, no matter whose rights they trample.  Fortunately, they have always been met with backlash, from officials, citizens or NGOs.

The American Black Chamber was a cryptanalysis office that specialized in decrypting and reading encoded messages from various high-ranking offices and countries in the world. It was said that nothing happened without them knowing about it. However, once WWI ended, the shift in the political climate went from paranoia to trust in ‘civilization’ and core values and virtues: ‘a man should not read another man’s mail’, was the motto and thought behind the shift. This means, we should trust each other and expect people to respect us, as we respect them; going against the realist point of view, specially just right after a war, was not easy but a priority. The Black Chamber was dismantled, and less ‘spying’ was done in general.

*“The most common manifestation of this trend is the expansion in recent years of laws*

*that regulate the practices that sovereign states may use. The human rights revolution has* *advanced in oral progress by breaking states' monopoly on international affairs and over* *citizens (Ignatieff, 20046). In this sense, liberalism triumphed and realism was repudiated,* *for the human rights movement has rejected the harsh realist vision expressed by Thomas* *Hobbes, who argued in the seventeenth century that because world politics is "a war of all* *against all, the notions of right and wrong, justice an. injustice have there no place."*

The thought that we should always be on the watch for attacks, that we should bolster our defenses and be ready for anything, is compelling. Security and safety are paramount to anything in life and to life itself, and any argument that is to make something more secure relies on one of the most basic of emotions: fear. As someone deeply invested into cybersecurity, I understand and relate to all the arguments the realist view defends. However, I also understand that humanity relies on trust to work, and that security relies on *not* trusting. This does not mean that everything is vulnerable and we should be ok with it, but rather, it gives the implication that to mitigate risks fear should not be the motivation, but rather education. We by nature fear the unknown; knowing something, understanding it, takes away the fear. If we know someone’s intentions, even if they are dangerous, the action stops being fear but transforms into certainty and action. Fear promotes reaction, knowledge promotes action.

It would seem counterintuitive to promote knowledge while also condemning the mechanisms governments put in place to get said knowledge. But there is an important distinction in this, and it is disclosure and consent. Each party should have clear statements and communication protocols to establish data gathering, even if it might not be completely transparent: if a store chose to film the floor, it should communicate its customers why it is doing it, even if it does not list all cameras, where they are located, etc. Giving all information would provide a security risk, as the only interested parties would probably be people who want to avoid the camera anyway, which gives rise to the question of why you would not want to be on camera. However, being filmed and not knowing about also robs the customer of the choice of not going into a place if they don't want to be filmed. Maybe they are a political refugee or want are under some sort of protection program and so don’t want anything or anyone to have a record of their face. The store should not privy into these matters, so long as it gives the information that it will do something, the customer has a choice to participate or not. This is how the ‘Terms and Conditions’ came to be. And we could get into another entire paper on how the concept of Terms and Conditions has devolved into a authoritarian client to provider relationship where customers are expected to surrender some or all of their rights in order to use a product or service.

*"States are now widely understood to be instruments at the service of their people, and not vice versa. When we read the Charter today, we are more than ever conscious that its aim is to protect individual human beings, not to protect those who abuse them." [Kofi Annan]*

The realist approach is tempting. It is much easier to doubt parties than to trust them. The 9/11 attack on the United States changed the shift of partial trust to complete distrust, and the War on Terror that resulted created justifications for the most atrocious of things, both to foreigners and citizens. While the current administration’s stance is unclear and not traditionally realist, some of their actions and policies are clearly aligned with distrusting and punishing foreign and local parties; the backlash to these is widespread and gigantic, and the actions taken have thrown us back and will take years to remediate. This approach cannot last. With the raised awareness of people’s rights, and more visibility into the government’s morally questionable programs with the help of whistleblowers and activists, the notion that a realist approach is the only way towards security is falling apart.

Sources:

Habeas Data: Privacy vs. the Rise of Surveillance Tech (2017, Cyrus Farivar)

World Politics: Trend and Transformation (2013, Charles William Kegley, Shannon Lindsey Blanton)

Carpenter vs. the United States (2017, <https://www.oyez.org/cases/2017/16-402>)

Olmstead & Katz vs the United States (1928, <https://www.oyez.org/cases/1900-1940/277us438>)

Terms of Ab(use) - EFF (<https://www.eff.org/issues/terms-of-abuse>)

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography (1999, Simon Singh)