Surveillance: “The Individual” Perspective of Rights

Kirby Hood

Syracuse University

The debate about the roles of governments and businesses within the context of the internet, is a question of how democratic and totalitarian societies view the rights of the individual. Living in a post-Cold War society and have entered into a world that is considered the market state, one of the hallmarks of this is capitalism. Business decisions are playing a greater role in national level decision making, whereas previously the nation state government had more control of people’s lives. This means that the nation state rule of law and the political philosophy drove decisions. In a market state it is the market and profitability that is playing a more equal role in this philosophy. (Bisson, Kirkland, & Stephenson, 1)

**Democratic View of the Individual and their Rights**

The European Union (EU) has a history that demonstrates the impact of commoditized of information and people that goes back thousands of years. This information has fueled slave trades, genocides, and empires. While the internet is able to accelerate the accessibility and transfer of information, decision makers do not have the luxury of time to debate the merits of philosophy, law, the market, and how this will impact the freedoms of the individual. The General Data Protection Regulation (GDPR) article 17, “the right to be forgotten” is an attempt to counter the market state which learns from the past and hopefully prevents the occurrence of out of control commoditization of an individual’s data. Article 17, states that, “the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay” (General Data Protection Regulation (GDPR)). This means that populations within the EU now have the ability to have any data that could be misleading or harmful erased. The EU’s advancement of the GDPR is a turning point for the world on the basis of policy and provides more transparency and ultimately returning control to the individual.

Article 5 of the GDPR, states that the individual must grant consent to any personal information that is being collected, and that individual must be made aware of the purpose for the collection of their sensitive information. This allows the individual more control over their own information. The United States fails to have the same ideology or the practice of these methods and continues to acquire sensitive information from its citizens. With the implementation of the GDPR and the impact on the global economy the United States, as well as other countries will have to possess standards that will raise to meet the standards that are being set forth to create a transparent digital exchange.

**Impact of Non-democratic Societies on Individual Rights**

In less democratic societies that are more feudal in nature, the rights of an individual are surrendered for the greater good of the collective, as is directed by a single person or a group of people. This model of government, often seen in communist nations, typically has a command economy, where data drives industry and advances the agenda of the central committee and the rights of the individual are insignificant. The individual is a production agent for the agenda of the central committee and therefore all data is property of the government. In many places around the world, whole cities have become smart cities. Censors and surveillance technologies are placed throughout the city to detect production rates of the citizens and deter civil unrest. Such cities are setting the stage for the surveillance of its population due to law enforcement agencies not being able to emulate the magnitude in which policing needs to be done.

**Unfavorable Collection of Sensitive Information of the Individual**

“Businesses have historically tracked their customers’ behavior (e.g., through credit card purchases) and have often sold this information to third parties” (Cockfield 367). The sale of information through third parties, including government entities, is the base of commoditization of information. Private entities use this information to serve consumers with the advertisements that they believe that individual would be interested in purchasing, and it is up to the consumer to make that decision. On the other hand, the private entities, then turn around and sell the information to other businesses and governments. For instance, the information that is collected from smart watches such as the FitBit, is sold to insurance companies. The insurance companies are then able to use the health information from these devices to increase premiums or deny coverage. The information that is shared about an individual’s personal activity, directly links the business to the exact individual’s name.

The private sector is also utilizing other forms of technology to collect individual’s information ranging from cell phones that will give the location that the call was made, software within computers to monitor its health and activity, frequent buyer cards at retail stores, RFI (radio frequency indicators) sensors in vehicles that tell the speed and other information about the vehicle, and many more. Even if this information is protected by various statutes, regulations, and policies, if a government or other business is wealthy enough and willing to pay top price for the information collected, the information will be sold. This allows for loopholes to be created. If there are people who are backed by very wealth governments or activist groups, they are able to keep their identity and information hidden, what is stopping these entities from purchasing the information of individuals and keeping the transaction quiet as well?

Whether it is a government or private entity that is collecting sensitive information about the individual, when an individual knows that their information is being collected, stored, and analyzed without their consent, that individual’s behaviors change. This is referred to as the “chilling effect.” According to a report done by the European Parliament’s Civil Liberties Committee, the altering of behavior due to surveillance infringes on their democratic right to detest, praise, publish works, or research government policy.

“The Canadian Islamic Congress indicates that hate crimes against Canadian Muslims have increased by more than 1,600% since September 2001, and reports ‘numerous cases’ of warrantless interviews and interrogations of individuals of Muslim or Arab origin” (Cockfield 396).

Racial profiling is often times feared as more governments obtain information on its citizens as well as citizens abroad. Because humans are the ones writing the algorithms and analyzing the data, biased is often written into the code, even if it is unintended.

Governments such as the United States, United Kingdom, Canada, Australia, and New Zealand engage with a program called Echelon, which monitors chats and emails. Echelon has been reported to have scanned 90% of the traffic on the internet. This program scans internet traffic for certain words to aid investigations. If there is behavior that raises suspicions the FBI will remotely install software that can track everything done on the suspect’s computer called the “Magic Lantern.” This software program can help to obtain information that could lead to terrorist threats or similar activity.

**Benefiting the Individual**

The internet is an information infrastructure that requires constant monitoring in order to keep it up and running. Many times, people assume that governments and private entities are collecting information that is sensitive, when they are monitoring the internet for its performance. Accountability of the government is at the forefront of these policies as well as the private entitles that assist in the collection of the individual’s information. “For human rights to have any meaning, it is therefore essential for someone to be responsible for that data are used” (Buttarelli 2).

Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA) in January 2004. PIPEDA was created with the intent to protect the individual’s information from being shared or bought without their knowledge. If a business intends to conduct transactions with citizens of Canada, they must make the intentions well known if sensitive information is collected and the individual must consent to the use of that information. This is a very similar idea to the GDPR that the European Union has recently put into practice. If consent is given to collect the information and the purpose of the information that is collected is stated, this can in turn become a commodity. The selling and use of individual’s information gives a new perspective on the world in which we live.

Canada and the EU are setting precedence for the rest of the world by allowing the individual to regain control of their rights and their privacy. This allows the individual to not be scrutinized for their information and the ability to exercise their democratic right to freedom of expression. Taking away the democratic rights of the individual is most concerning. The US should turn to Canada and the EU for guidance to advance the technological policies for the better well-being of the individual. With their guidance the US could model policies after the GDPR, the ultimate setting of precedence in today’s society.

Word Count: 1496

Sources

Albrecht, J. (March 2016). How the GDPR will change the world. *European Data Protection Law Review*. *Vol 2, Issue 3*. pp. 287 – 289. doi: <https://doi.org/10.21552/EDPL/2016/3/4>

Anon, D,. (2018). What does the US government know about you?. *Citizen Surveillance.* Retrieved from <https://privacy.net/us-government-surveillance-spying-data-collection/>

Cockfield, A. (2003). Who watches the watchers? A law and technology perspective on government and private sector surveillance. *Surveillance as Law. ResearchGate. Queens University. Pp. 364-407.* Retrieved from <https://heinonline.org/HOL/LandingPage?handle=hein.journals/queen29&div=17&id=&page>=

Bisson, P., Kirkland, R., & Stephenson, E,. (June 2010). The market State. *Governments around the world are facing complex, difficult decision. Business leaders would do well to work with them to develop solutions.* Retrieved from <https://www.mckinsey.com/industries/public-sector/our-insights/the-market-state>

Buttarelli, G. (May 1 2016).The EU GDPR as a clarion call for a new global digital gold standard, International Data Privacy Law, *Vol 6, Issue 2, Pages 77- 78*, <https://doi.org/10.1093/idpl/ipw006>

General Data Protection Regulation (GDPR). (2018). General Data Protection Regulation. *Intersoft Consulting.* Retrieved from <https://gdpr-info.eu/>

Gelb, C. (May 2018). As “smart cities” come into focus, California laws seek to limit surveillance technology. *Future Society.* Retrieved from <https://futurism.com/smart-cities-surveillance-technology-california/>

Wakefield, A., (2005). The public surveillance functions of private security. *Surveillance & Society. Vol 2. No 4. People Watching People. pp. 529-545.* ISSN: 1477-7487. doi <https://doi.org/10.24908/ss.v2i4.3362> Retrieved from <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3362/3325>