Ethical question: Is it unethical for Western tech companies to actively support and/or profit from China's initiatives to surveil their population for the purposes of effecting social conformity? Likewise, is it also unethical for individuals in the West to profit from said companies? A foundational aspect of codes of conduct for Western societies is a 'discreet distance' at which governments involve themselves in the day-to-day events of their citizens. It's a distance that for Westerners engenders continuous debate. To this end, do China's actions aim to bring Orwell's worst fears from 'Big Brother' into reality? Any assistance that Western companies provide China could be argued that it makes them willing accomplices, indirectly shrinking the discreet distance between government and the governed.

China is now in the latter stages of developing an expansive and interconnected network of data capture systems. Once complete, they will have an unprecedented ability to track, record, and influence the actions of the entire population. Their strategy is to employ hardware, software, and advanced artificial intelligence methods to make that possible. Its facial recognition module is currently under evaluation in the western province of Xinjiang, enabled as part of an expansive video camera system. Xinjiang is home to China's population of eleven million ethnic Uighurs, a Muslim minority[[1]](#footnote-1).

As part of the Xinjiang trial, China plans to utilize mandatory vehicle tracking as well as biometric data capture systems. The government will gather DNA samples, fingerprints, iris scans and blood types of everyone aged between 12 and 65[[2]](#footnote-2). These will be combined with information gleaned from online shopping data and browser history data, provided courtesy of China's tech companies Alibaba and WeChat. This is not to single those two organizations out; Chinese companies are required by law to assist in the government's spying activities[[3]](#footnote-3). Undoubtedly, a significant count of Chinese companies likely do - or will in the future - contribute data and services as requested.

China's goals here are manifold: They aim to construct a complete dossier on every citizen with the express purpose of authoritarian behavioral modification amongst their population with the preference of group order over the rights of the individual. They look to identify what they consider to be internal threats to order, whether that be of a criminal nature or the suppression of dissent whether based in fact or in opinion. Furthermore, they aim to integrate these criteria into a social scoring model, affecting financial (credit availability as well as access to public services) and judicial outcomes for their citizens. Combined with existing social networking algorithms, it's not inconceivable that a poor score on one's part could propagate to friends and family and exert peer pressure on one’s behavior[[4]](#footnote-4).

The U.S. government has had an on-again, off-again mindset with allowing companies to sell technology to China that is relevant to this system. One recent case involves ZTE, China's second-largest telecom manufacturer. The ban on American companies selling them component parts has been lifted as of July 2018, to proceed under a closely-monitored relationship that hinges on national security considerations[[5]](#footnote-5). However, Western companies don't have to necessarily provide equipment or services; capital will serve nicely in its place. In 2007, China Security and Surveillance Technology (CSST) received $110 million in convertible loans from the Citadel Group, a Chicago-based hedge fund, which it used to buy up smaller Chinese surveillance companies. Some Wall Street executives defended their actions by equating the Chinese surveillance system with the surveillance cameras of London and New York[[6]](#footnote-6).

What are the ethical questions to be considered? Under what moral structures will we consider them? We will be address them through the ethical guidance of Deontology and Utilitarianism. The former is, in summary, the valuation of the human beings as having inherent value and an obligation to not use them as a means to an end, without much of an emphasis on consequences of decisions. The latter embodies the goal of maximizing happiness for as many people as possible, over present and future consequences.

The ethical questions under scrutiny here revolve around what the appropriate actions should be for individuals and organizations that are not Chinese in origin, especially for those in the Data Science community whose careers could have direct correlation. The reason for that distinction - as noted in the introduction - has its origin points in recognizing and respecting markedly different sources for determining the appropriate 'discreet distance' between the government and the governed. In China, Mao's Cultural Revolution. In the West, incrementally developed through the English *Magna Carta*, *The Declaration of the Rights of Man and of the Citizen* enacted during the French Revolution, and the American *Bill of Rights*, refined through ongoing debate.

These questions ask us to consider the prospect of making decisions that result in the debasing of the individual's inherent value, when subjected to the ongoing scrutiny of surveillance. This is counter to the notion promoted by the Chinese government that these efforts maximize the public good and should thus be considered as an ethical solution. The questions are rather interconnected:

* Is it ethical for Western companies to directly support China's surveillance infrastructure by sale or purchase of goods, services, and expertise?
* Is it ethical for Western companies to indirectly support China's surveillance state by means of capital investment? Specifically:
  + Investment in Chinese companies directly participating in the program.
  + Investment in Western companies noted in the first question.
* Is it ethical for Western individuals to invest in companies that profit from sales to China of the building blocks of the surveillance state?
* Is it ethical for Western Data Scientists to enhance their skill sets and careers through expertise gained as a direct result of the Chinese emphasis on surveillance?

Similar situations from which to base a moral equivalency can potentially be found in traditional responses to nations that overtly seek to harm large segments - or even the majority of - their population. Unfortunately, Western responses to these types of situations have been mixed. The Stalinist purges of the 1930s were downplayed by many in the west, notably on the British Left[[7]](#footnote-7). Alternatively, on the matter of South African apartheid, there was widespread international involvement in the application of pressure to South Africa. Companies were pressured by their governments to divest themselves of all investments in South Africa. This pressure did not come quickly. It only manifested itself after decades of intense debate on the appropriate ethical role of the West, culminating with the end of apartheid in the 1990s.

Clearly, similar courses of action as it pertains to China would not be arrived at quickly, or perhaps even at all. Complicating any reaction to the role of the surveillance state in China by the West is the reaction of the Chinese people to an environment of pervasive surveillance. Even taking into account their monitoring, it seems the nation is of split opinion on the matter[[8]](#footnote-8). While some are concerned about violations of consumers and citizens' rights, many are on record as championing the enhancement to law, order, and safety that it could bring. Short of the introduction of a "Tiananmen Square"-level event, it does not seem that past solutions can offer us much in the way of guidance other than that we are faced with a long and arduous debate over an appropriate reaction.

So then, how should an ethically responsible technical professional approach potential responses to the situation, understanding that theirs is but one voice? Luckily, the answer lies in our taking a structured approach to gathering information on the matter and applying our personal and professional codes of conduct to possible paths of action for ourselves and those with which we associate professionally or financially. This exercise will help us to understand the benefits and harms of the Chinese surveillance state upon their people and consider the ramifications of its potential adoption and use in some form or fashion on individuals in the West. That analysis is twofold: One must determine whether active support or neutrality are valid ethical positions, in addition to what is not necessarily an obvious decision to oppose China's endeavor.

The first argument to be analyzed involves the stance that Western companies are doing harm and violating ethical principles by supporting China's actions and should cease. This harm comes from the selling of materials allowing China to execute their plan, or from capital investment that enables the endeavor, or from purchase and utilization of an increased expertise in Chinese AI methods. Individuals would violate their ethical responsibilities unless they divest themselves from companies that benefit from involvement with Chinese mass surveillance, regardless of the method of benefit.

The second argument involves the possibility that there is nothing ethically wrong with supporting and profiting from China's surveillance, especially if the people surveilled are predominantly supportive of the measure. Such a stance would involve an in-depth consideration of China's supposition that the greater good is served by their actions. This would be a much easier sell under a Utilitarian framework and consideration of maximization of happiness for as many people as possible. It would most certainly not survive a critique using Deontological approach, but that will be considered as well.

An in-depth analysis of the first argument that a data science professional should not partake in China's efforts to surveil their citizens can be placed in context of the Code of Ethics and Professional Conduct for one of the leading professional IT organizations, the Association of Computing Machinery (ACM)[[9]](#footnote-9). The guidance that the Code provides is "...designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. ... [It] serves as a basis for remediation when violations occur... [and] includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration."

When using the Code to seek guidance for this first argument, one must keep in mind that it is constructed from a Western point of view, balancing equality, justice and respect. As such, some tenets run counter to involvement in China's surveillance policies. Section 1.1 (Contribute to society and to human well-being) directs professionals to take actions "...promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy." Expanding upon that statement, an entire section (1.6) directs the professional to respect the privacy of individuals and groups.

Not only would a member in good standing be unable to assist in such an effort, they would be duty-bound to voice their concerns. Section 2.7 asks that a professional "foster public awareness and understanding of computing, related technologies, and their consequences." Clearly, the ACM's code is constructed with a deontological basis and is incongruent with support for conducting surveillance on a national scale. From a utilitarian standpoint, there's not just the evaluation of the happiness accrued by furthering law and order, evidenced by Section 3.1 (Ensure that the public good is the central concern during all professional computing work). It has to be compared against the loss of autonomy that occurs when one does not feel free to act as one wishes both presently and in the future, when the Chinese will train systems to include additional inputs, with additional rewards and penalties as outputs.

People in the professional roles that can take action in this ethical discussion are limited by the premise of the argument to those living in the West. Data scientists and their managers are included as stakeholders. They are responsible for deciding whether to use algorithms that are or will be perfected in China as part of this endeavor, or to instead use methods less predictive but with fewer ethical concerns. This includes advances in facial recognition, genome sequencing, and traffic pattern analysis. Each have the potential of being enhanced through efforts of the Chinese state. Their use on Western citizens would be a tacit endorsement of the methods used to generate them and would elevate them to the status of stakeholders in addition to the harms inflicted upon the Chinese people. It seems beyond coincidence that the system is being perfected in an area with a high minority population; added to the list of harms is the inequitable treatment of a minority group.

We can also include manufacturers of surveillance equipment or of their component parts. Likewise, makers of network equipment and PC hardware should consider their actions and consider whether sales to China for the express purpose of pervasive surveillance violates Western ideals of - to reuse the phrase - the discreet distance inherent between government and the governed. It is their responsibility to not only act according to ethical norms set by organizations like ACM, but also to be responsible stewards of their company. A questionable decision in the pursuit of profit can many times come back to haunt a company; one must at minimum voice their concerns should such a decision arise.

Policies for conduct when determining one's response include consideration of - in addition to codes of ethics - trade agreements, or conversely trade restrictions based on national security grounds. However, worse damage could be done not with equipment, but with algorithms. For data scientists, it's a matter of evaluating whether the methods you used were ethically derived - respecting of humanity - and that the results likewise seek to minimize harm to any group.

Inside a seemingly simple statement, however, lies a complicated path. Let's take a hypothetical example and introduce a new stakeholder: Suppose that facial recognition algorithms undergo a breathtaking, generational improvement because of Chinese efforts and the massive size of the dataset they can throw at the problem. The algorithm's methodology is submitted for publication in Science magazine, long considered a clearinghouse of articles at the frontier of tomorrow's advancements. Publication opens the opportunities for review first, then adoption, then further improvement. Does Science have the responsibility to withhold publication? I imagine they would take the same stance as they have with gene editing and CRISPR[[10]](#footnote-10); advocating to convene an international summit to discuss the matter with the scientific community. There, ethical and regulatory proposals can be produced so that legislative bodies have an educated place from which to start mapping their responses.

Our second ethical option involves considering the alternative that Western companies and individuals are not substantially violating any ethical behavior by participating, even indirectly, in goods or services that facilitate China's designs on nation-wide surveillance. One must consider the goals that China wishes to attain: a culture of sincerity, a harmonious society, and an emphasis on the keeping of trust. Some of the antisocial behaviors they seek to minimize can be characterized as[[11]](#footnote-11):

At the heart of the social credit system is an attempt to control China's vast, anarchic and poorly regulated market economy, to punish companies selling poisoned food or phony medicine, to expose doctors taking bribes and uncover con men preying on the vulnerable. “Fraud has become ever more common in society,” Lian Weiliang, vice chairman of the National Development and Reform Commission, the country's main economic planning agency, said in April. “Swindlers have to pay a price.”

Certainly, ethical codes of conduct need to consider and champion trustworthiness and sincerity. The ACM Code of Ethics Section 1.3 says exactly that as it pertains to a professional's actions. Likewise, Section 1.1 summarily directs us to "Contribute to society and to human well-being", and specifically that "An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy." Granted, privacy under the Chinese social score scheme is minimized, but their stated aim is to maximize the other three. As a professional, when deciding whether to sell surveillance components to China or to utilize perfected facial recognition algorithms, privacy cannot be the sole determinant of ethical behavior. Other positive behaviors promoted by the state must as well be considered.

The professional roles examined in this argument are the same as with our other ethical option - Western data scientists and anyone looking to profit from sale of surveillance or networking components. But with this argument, the responsibilities to be evaluated take another angle: What is the ethical obligation to assist the Chinese government in the upholding of order and improvements to health, safety, and personal security? Or, given the first argument, do ethical obligations oblige us **not** to withhold goods or services resulting from others' overweighting the virtue of privacy compared to those of health, safety, and personal security? That certainly isn't a much different choice than those made by Western governments to overweight security in comparison to privacy, safety, and health.

Professionals in Western IT companies certainly have a profit motive driving them to sell to or to use Chinese advancements in AI. To ask 'were the benefits and harms distributed fairly' can be answered in the affirmative, noting that China's trial run in Xinjiang (ostensibly targeting a minority) is but a prelude to its adoption everywhere. There has been no evidence so far that the Chinese government would treat a minority accused of terrorism any differently than a majority Han. Until such evidence exists, stakeholders should continue to make decisions on the basis that support of the Chinese infrastructure does not result in an imbalance of benefits or substantive harms upon their citizens.

For those in the West that choose to use advances in Chinese facial recognition AI, for example, ethical policies surrounding how it is implemented can guide data scientists' conduct. Were the benefits to safety, health, and personal security applied equally to all citizens? Were the harms of a more pervasive government presence equally as applied? Proceeding with that choice can be an ethically acceptable one, at least as one component of the argument.

China’s surveillance methods could be considered ethical if it is shown that for events where wrongdoing is uncovered, leniency was not given in the application of penalties to high-ranking party leaders, or to the wealthy and well-connected as compared to the poor or to minorities. To extend the example, if a known black-market operative is recognized by security cameras at the headquarters of a large Chinese pharmaceutical company, and criminal behavior is uncovered and the privileged punished, that certainly promotes equity of enforcement and offers no hurdle to those critical of how underlying AI improvements were generated. Similar arguments can be made for ethically selling component materials, or for making capital investments.

Considering both arguments, the first argument is stronger and we should consider direct or indirect support of China and surveillance of their citizens to be unethical. That ethical decision doesn't have to deal with the prospect of maximizing one of the harms (privacy invasion) so that substantial benefits for the other effects of the Chinese surveillance infrastructure (health, safety, and personal security) can be achieved. Harms as well as benefits are spread a bit more evenly and results in a more balanced solution. Data scientists or other IT professionals looking for guidance on how to best make defendable ethical choices as it relates to this topic can feel confident in pursuing this course.

However, a proponent of the second argument would strenuously disagree. Two primary arguments that they could employ in rebuttal would be:

1. A Western sense of ethics should not be imposed on a culture that has a historically different model governing the relationship of the individual to the state. As such, Western citizens should not overlay their notions of privacy ethics upon decisions surrounding their relationships with China or from technical advances discovered by the Chinese in this setting. Instead, they should become more knowledgeable about the social structures leading the Chinese to this decision.
2. China is doing nothing more than applying an only slightly different weight than the West to the principles of privacy, security, health, and safety for their citizens. Western governments are just as desirous of infringing upon privacy and were only recently restrained by the Supreme Court from excessive violation of cell phone data privacy in Carpenter v. United States[[12]](#footnote-12). Revelations of NSA snooping and citizen data collection uncovered in Edward Snowden's document dump[[13]](#footnote-13) need no further elaboration. Individuals making their own ethical choices regarding direct or indirect support of China’s surveillance efforts should respect China’s balancing choices.

The following responses can ably counter those arguments:

1. While it is always prudent for one to be knowledgeable and respectful of another's foundational principles, one doesn't have to be focused solely on the foundations of privacy to find cause to consider China's path unethical. You can choose from many other reasons: A trial run of the system in a heavily minority area, maximizing the harm to them. Restriction of modes of travel options if your social score is too low. A low score adversely affecting the score of one's friends and family. State-sanctioned mass genetic data capture.
2. This is probably the most convincing counter-argument. There is a lot of truth to it. But it's not so much an argument on whether China is ethically justified or whether we should disassociate ourselves from actions that would assist them and profit ourselves. It's instead an argument that we should be just as vigilant towards our own governments, and that our ethical eye should look West as well as East.

There are several lessons from this exercise for data scientists and other IT professionals that are confronted with future ethical decisions.

1. Thoroughly understand the values (and by extension, regulations) of the societies that your decisions will affect, if they are other than your own. The things you weigh as important aren't always similarly weighted there, and vice versa. GDPR is a good example of this. Western notions on how to transact in the information age are not monolithic. Looking through the eyes of those you will affect will consistently be a good starting point whether it be through the prism of privacy, explanation of methods, or disclosure of breaches.
2. Ethical guidelines need to keep up with the times. Ethically-muddled interpretations to issues and to evolving technology will always be with us. Institutions that have vibrant debates on their application deserve your consideration. Institutions that choose not to debate their application or choose to consider them settled should either not have their guidance considered or should have their existence openly questioned. For the budding data scientist, the imperative is to become part of a group of like-minded individuals that can help guide you through difficult decision-making. If lucky, you will be able to return the favor to someone else.
3. As an extension to the last point, transparency can be your friend. Having an ethical problem with a work-related decision? Don't keep it to yourself. Enlist the help of others. When possible, consult with colleagues with expertise on the subject and publish your concerns in your publicly-available work. When disclosure agreements preclude such a course of action, air it out to those who can affect a change of direction.

1. https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report [↑](#footnote-ref-1)
2. https://www.theguardian.com/world/2017/dec/13/chinese-authorities-collecting-dna-residents-xinjiang [↑](#footnote-ref-2)
3. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ [↑](#footnote-ref-3)
4. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ [↑](#footnote-ref-4)
5. https://www.reuters.com/article/us-usa-trade-china-zte/u-s-ban-on-chinas-zte-lifted-idUSKBN1K32CN [↑](#footnote-ref-5)
6. http://prospect.org/article/cashing-chinese-surveillance [↑](#footnote-ref-6)
7. https://www.spectator.co.uk/2017/06/how-the-british-left-condoned-the-murder-of-millions/ [↑](#footnote-ref-7)
8. http://www.businessinsider.com/how-china-is-watching-its-citizens-in-a-modern-surveillance-state-2018-4 [↑](#footnote-ref-8)
9. https://www.acm.org/code-of-ethics [↑](#footnote-ref-9)
10. http://www.sciencemag.org/topic/crispr [↑](#footnote-ref-10)
11. https://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html [↑](#footnote-ref-11)
12. http://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/ [↑](#footnote-ref-12)
13. https://www.bbc.com/news/world-us-canada-23123964 [↑](#footnote-ref-13)