Power Dynamics in an Era of Big Data

STACY LANGWORTHY

LSE Ideas

STRATEGIC UPDATE

MARCH 2019

Currently ranked Europe's top university affiliated think tank.

LSE IDEAS is LSE's foreign policy think tank. We connect academic knowledge of diplomacy and strategy with the people who use it.

Through sustained engagement with policymakers and opinion-formers, IDEAS provides a forum that informs policy debate and connects academic research with the practice of diplomacy and strategy.

IDEAS hosts interdisciplinary research projects, produces working papers and reports, holds public and off-the-record events, and delivers cutting-edge executive training programmes for government, business and third-sector organisations.

 @lseideas  facebook/lseideas

Contents

> Is big data a resource of power like oil? If this is the case, do the tech companies who hold disproportionate amounts of the world's personal data also hold disproportionate amounts of power?

INTRODUCTION

We are living in an era of big data. Our interactions with mobile phones, computers, and a variety of digital devices are increasingly being processed as data; data that is growing in volume and value.[1] Compared to its predecessor, data, 'big data' has unprecedented reach, velocity, and complexity, revolutionising the way we process information and, possibly, the way we think about the world.[2]

In an era of big data, our personal data is being collected and utilised by private firms and governments alike. This data is comprised of our shopping baskets, emails, texts, tweets, photographs, employment, and more. It is professional, political, and financial, yes, but it is also quite personal. The value it has provided for us as consumers is immeasurable. From the relevant results in our online searches to traffic details along our routes to personalised recommendations of new products to try, big data has been integrated thoroughly into every aspect of our everyday lives.

The impact of big data in the business world has been equally profound. Some of the most valuable companies in the world today – Alphabet (Google), Microsoft, Amazon, Facebook – are those fuelled by the collection and extraction of big data, specifically the personal data that is created by and about individuals every second of the day. It is for this reason, its centrality in the global economy, that Meglena Kuneva, the European Commissioner for Consumer Protection, hailed it as 'the new oil of the Internet and the new currency of the digital age.'[3]

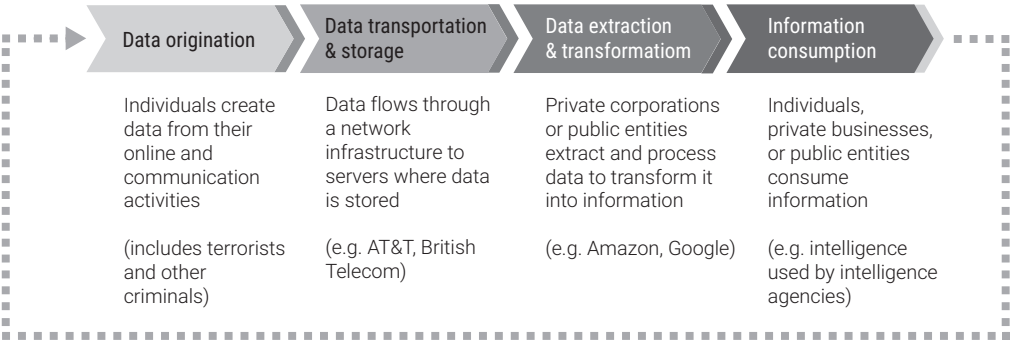
Given this analogy to oil, this raises the question: is big data a resource of power like oil? If this is the case, do the tech companies who hold disproportionate amounts of the world's personal data also hold disproportionate amounts of power? Or, is this comparison a hollow one and the power dynamics of big data are more nuanced and not (yet) fully understood?

This strategic update first summarises the impact and potential big data has across the public and private spheres. It then uses two case studies, the 2016 U.S. presidential election and the row over Huawei's 5G technology, to illustrate the strategic value of big data and to illuminate which actors have derived politically consequential power from the information big data provides. The argument presented is that the relational power dynamics of big data differ from those of oil, and the tech giants who hold significant proportions of the world's big data do not, at the same time, possess distressing amounts of power. I intend to show that big data's power potential rests not in the hands of the technology intermediaries that collect it but in the actors, state and non-state, that deploy it. In concluding thoughts, this strategic update also introduces the concept of a new global framework that would enable individuals to maintain more authority over our own personal data in an effort to check the growing economic influence and personal interventions of multinational corporations.

POTENTIAL OF BIG DATA

Before interrogating the similar power politics of oil and big data, one may easily observe their functional similarities. Similar to oil, big data is a resource that requires extraction and processing in order to derive value from it.[4] Moreover, like oil, big data has benefited from a value chain, a system for extraction and processing, which has been widely introduced:

Figure 1: Big data value chain: key activities and examples of associated actors



At the third stage in the big data value chain, raw material (i.e. data) is extracted and transformed into value, information that can be readily monetised.

As the information big data provides continues to be used for both economic and political gains, big data has increasingly become the subject of discussion in the media and on the international stage. In 2018, headlines were dominated by the story of Facebook's unprecedented data breach of 87 million users related to Cambridge Analytica's involvement in the 2016 U.S. presidential election. More recently, the news cycle has continuously highlighted national security concerns over a Chinese business, Huawei, dominating the field of 5G technology, the new pipeline of big data.

Beyond our consumer lives, big data has the potential to profoundly change how governments work. As Kenneth Neil Cukier and Viktor Mayer-Schoenberger, scholars of the social, political, and economic dimensions of big data, have written: "When it comes to generating economic growth, providing public services, or fighting wars, those who can harness big data effectively will enjoy a significant edge over others."[5] In the space of international relations, the possibilities of big data are wide-reaching across a broad range of topics, with the potential to revolutionise transnational governance, peacekeeping models, foreign policy, and national security objectives.[6]

Big data is at the core of China's hi-tech state surveillance apparatus, which is being used to target the predominantly Muslim Uighur ethnic minority in the Xinjiang province as part of an 'anti-terrorism' campaign.[7] Facial recognition from CCTVs, location data, satellite tracking, and Wi-Fi sensors that secretly collect data from network devices are being used to alert authorities when a target has shown the slightest indication of suspicion or disloyalty to the state. Once captured, the targets are sent to detention or 're-education' camps to instil loyalty to the Chinese Communist Party.[8] With the right technology, personal data has become easier to collect and process, giving governments the ability to harness big data for control over their own citizens. This power, increasingly, is not the exclusive province of large and wealthy states. Recent reports have highlighted how China has exported its surveillance capabilities to others, such as Ecuador.[9]

Big data also plays a key component in the engine driving economic mastery for those that have harnessed it such as Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft— some of the most valuable listed companies in the world.[10] These firms have created business models around technology that enables the collection, extraction, and value-add processing of big data into information that is fed back into their ecosystems to innovate, enhance services and products, retain customers, and grow sales.

Facebook is a prime example of a business model that leverages big data generated as a 'platform' technology, a digital intermediary and infrastructure where two or more parties interact.[11] Platforms like Facebook rely on a 'network effect,' an increasing base of users that makes the platform more valuable to the other parties, particularly advertisers who can reach ever larger numbers of users. This characteristic makes them a natural holder and processor of large volumes of data whereby the more users who join the platform, and the more interactions that take place, generate more data points to monetise.

> "Cambridge Analytica's former Head of Data, Alex Tayler, further praised the data's effectiveness, stating, "When you think about the fact that Donald Trump lost the popular vote by 3m votes but won the electoral college vote—that's down to the data and the research."

With more than 2 billion monthly active users, Facebook has become the largest social media platform in the world.[12] The more users that engage with Facebook, and the longer they stay engaged, the more data that is available for the firm to use in selling advertising space to brands, political campaigns, and any other entity with an interest in reaching audiences around the world. By leveraging the mountain of rich personal data that exists in the Facebook platform, advertisers are able to reach granular segments from a larger population in order to target highly customised messaging to each segment, a technique called micro-targeting.[13]

CASE STUDY 1: Cambridge Analytica and the 2016 U.S. presidential election

At the time of the 2016 U.S. election, there was widespread use of big data and micro-targeting by political campaigns by both parties. With its capabilities in this space of data and political campaigning, Cambridge Analytica, a now defunct political consultancy and data analytics firm, became a key figure in Trump's campaign for the 2016 U.S. election. Cambridge Analytica was known for its expertise in using data for 'election management strategies' and 'messaging and information operations,' the latter also known in the military as 'psyops' (psychological operations) or mass propaganda that plays off of people's emotions.[14]

The firm's unique value proposition was a twist on the concept of micro-targeting, analysing big data to understand not only what people do (their personal and professional actions and interactions) but also who they are (their emotions and preferences). This gave a more comprehensive psychological profile of the American voter which became a key aspect of Trump's digital campaign strategy.[15] In order to create the big data asset required to profile and target American voters, Cambridge Analytica needed to accumulate as much meaningful data on the U.S. electorate as possible. As a rich source of this data, there were few more suitable than Facebook.

"The problem," Chirag Shah, a professor of information and computer science at Rutgers University, has argued, "is once people access the data from Facebook, for which they often pay, that data is out of Facebook's hands and out of Facebook's users' hands."[16] This is a problem that was further exacerbated by a feature that once existed for advertisers prior to 2015, the same feature that facilitated Cambridge Analytica's possession of 87 million Facebook profiles.

Once the harvested Facebook data was in their possession, Cambridge Analytica created a data apparatus by matching the Facebook data to other data they had collected on individuals in the U.S., including voter rolls. Combined with voter roll data, the data from Facebook, the personality quiz, and other behavioural data points gave Cambridge Analytica a large dataset to analyse and mine for insights.[17] As part of the analytics process, Cambridge Analytica developed advanced algorithms that were applied to determine personal information about people's sexual orientation, race, gender, intelligence, and even vulnerability to substance abuse. Cambridge Analytica then fed this information into a software programme they built to predict and influence voters at the ballot box.[18]

The big data that Cambridge Analytica harvested has been claimed as instrumental for the Trump campaign. Alexander Nix, former CEO of Cambridge Analytica, described the Trump campaign's use of the big data as having informed all the campaign's strategy.[19] Cambridge Analytica's former Head of Data, Alex Tayler, further praised the data's effectiveness, stating, "When you think about the fact that Donald Trump lost the popular vote by 3m votes but won the electoral college vote— that's down to the data and the research."[20]

In the example of Cambridge Analytica and the 2016 U.S. election, big data was power for the ultimate information consumer, the Trump Campaign. This power was over the data originator, the U.S. electorate (the general public), to influence their perceptions and voting behaviour. This contrasts with the value chain of oil, where the originators of oil are natural resource rich states such as those in the Persian Gulf. These states maintain a great degree of power, being able to determine who has access to the oil. In the case of big data origination, the general public may have

a choice as to which platforms and services they use, but with significant lack of control as to who will ultimately use their data and how. In other words, in the case of big data it is resource consumption, not resource origination as in the case of oil, that yields political might.

> "The limiting factors of big data's power will be local data privacy laws that govern the various markets these tech companies operate in."

Whilst Facebook has a role to play in the big data value chain as the data holder, the 2016 U.S. election illustrates that those who hold the world's big data do not necessarily have control over it. The intermediary role that Facebook plays has been conducive at times to other parties having more control than Facebook realises or desires. By and large, therefore, this leaves the major technology companies in a somewhat helpless position as they have become increasingly vulnerable to external misuse of the data they collect. The empowered actor in the era of big data, on this view, is neither the data originator (individuals), nor the data collector (technology companies), but rather the data 'deployers' (state and non-state actors).

When the story of Cambridge Analytica's data breach made the headlines in 2018, it triggered a heated debate over individuals' rights to data privacy. U.S. Congressman Adam Schiff, a ranking member of the House Intelligence Committee, stated that the "misappropriation of private data is a serious invasion of the privacy interests of the American people by Cambridge Analytica and potentially other individuals and entities."[21] The limiting factors of big data's power will be local data privacy laws that govern the various markets these tech companies operate in.

Take for example the General Data Protection Regulation (GDPR), a data regulation put in place last year by the European Union.[22] GDPR gives individuals more rights over their personal data and forces companies like Facebook to make changes to the way they collect data and obtain consent from users. Whilst companies may not be based in the EU, if they collect and process any data from EU citizens, they are impacted by the regulation.[23]

CASE STUDY 2: Huawei and 5G technology

Towards the end of 2018, the CFO and daughter of the co-founder of Huawei was arrested in Canada and faced extradition to the United States for allegedly assisting Huawei in covering up violations of sanctions against Iran.[24] This story put Huawei, a Chinese multinational with expertise in 5G and the world's largest supplier of telecoms equipment, on the international stage and under the microscope of scrutiny.

5G is particularly critical for big data as it will revolutionise the speed at which data is transmitted and reduce the lag time between transmission at larger capacities.[25] These enhancements to the pipeline through which data is transported will create the foundation for transformative innovation such as self-driving cars, smart cities and autonomous factories.[26] The race is of global consequence and, at present, Huawei is in the lead. However, over the past year, Washington has been attempting to persuade allies to ban Huawei from implementing 5G technology in their respective states, labelling the manufacturer a national security threat.[27] Providing a setback to these attempts, British intelligence services have recently provided their perspective that Huawei is a manageable risk and that it is possible to mitigate the security hazards of having Huawei technology in the U.K.'s 5G networks.[28]

We know from the story of the Chinese government and surveillance of the Muslim Uighur ethnic minority in the Xinjiang province that the state is not hesitant to gather big data for domestic purposes. Does this mean China might also expand its surveillance internationally and extend Huawei's reach to foreign flows of data? Given that this is currently a hypothetical situation, it is useful to look at how other states have conducted themselves in similar contexts.

As we have learnt from the thousands of top-secret NSA documents made public by Edward Snowden, there is widespread data collection and mass surveillance being conducted by the United States and other governments' intelligence agencies.[29] Through its signal intelligence programmes, the NSA has directly or indirectly tapped into the data from 'internet servers, satellites, underwater fibre-optic cables, local and foreign telephone systems, and personal computers.'[30] Two programmes account for the majority of records gathered by the NSA: PRISM and Upstream.[31] While both programmes are intended to gather data exclusively on targeted foreigners, they incidentally also collect data of U.S. citizens due to their inability to discriminate between foreign and domestic data in internet traffic.[32]

Of these two programmes, Upstream provides the closest parallels to the hypothetical situation of the Chinese state acting through Huawei and its 5G technology. Upstream is the codename

for the subset of programmes that enable the NSA to tap directly into the fibre-optic cables and network infrastructure that transport a large amount of the world's internet and telecommunications data.[33] The vast network of subsea fibre-optic cables expands between continents, connecting the United States with the rest of the world with an estimated twenty-five per cent of the world's internet traffic crossing over the U.K. via fibre-optic cable networks.[34] The remaining traffic has landing or departure points in the U.S., giving the U.S. unparalleled access to the world's data flows.[35]

The Upstream programme has been justified under Section 702 of FISA, which grants permission 'to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.'[36] With the compelled cooperation of telecommunications providers such as AT&T and Verizon, the NSA has been able to install surveillance equipment into the infrastructure of internet traffic.[37] With the Upstream programme, the NSA has had the capacity to access approximately 75% of all U.S. internet traffic, collecting data as it is in transit.[38]

The United States is also not alone in utilising relationships with private firms for surveillance purposes. GCHQ has its own programme, Tempora, to intercept data directly from fibre-optic cables.[39] In the wake of several terrorist attacks across Europe, Germany and France have also passed laws granting their intelligence agencies the ability to conduct mass interception of communications.[40]

As illustrated by the Upstream programme example, the NSA uses big data for power over foreign targets and general citizens, the data originators (individuals). This is the same power dynamic as with the Cambridge Analytica example: data originators can limit the use of their data to a degree, but to a large extent decisions of how their data is used are out of their hands.

What we see from both examples is that the actors in power are those who decide what information is required, thus shaping what questions big data should answer. This indicates that power is not necessarily dependent on generating, holding, or processing the data but rather on who has the foresight and power to deploy the information big data becomes.

Although telecommunications companies play a key part in the big data value chain, their power to transport the world's flow of data is trumped by the intervention of the state. The tech giants, whilst still holding and owning the data that is transported by the telecommunications companies, have limited power over the government's ability to access big data in transit.

Several pertinent questions remain: Will the Chinese government use its influence to create a similar relationship with Huawei as the NSA did with U.S. telecommunications companies? What foresight and questions would the Chinese state have in using big data for potential power? What we have gleaned from other states' actions is that under the flag of national security, governments will go to great lengths in accessing the information they desire.

CONCLUSION & POLICY RECOMMENDATION

As this strategic update attempts to elucidate, there is massive positive potential for big data's capacities to change and grow the global economy. However, there are many challenges with big data that exist, and with its continual rise there is more personal data at risk of data breaches and improper use, or use without consent. There are several factors related to the vulnerability of personal data. The following are two that if addressed, could help mitigate the risks associated with personal big data.

> "If we want a world where big data can be safely harnessed, there are policy changes that need to be introduced."

First, there is an issue of the 'privacy paradox.' Professors Vincent Mitchell and Bernadette Kamleitner describe the 'privacy paradox' as follows: people say they want to protect their data privacy, but due to the lack of a sense of ownership, they often do very little to keep it safe. [41] One way to increase the sense of ownership would be to create a system where individuals are able to sell their personal data or, as has been promoted by California governor Gavin Newsom, to institute a 'data dividend' whereby some percentage of the revenue generated from users' personal data is returned to the user.[42]

Second, there is a lack of global governance in data regulation and data protection. Although GDPR is viewed as having global reach in its impact, global governance for personal data does not really exist.[43] This area has room for significant progress, with a need for governance that represents the complexities of a big data era where national security and individual rights converge. The governance model also needs to involve a strong public-private partnership given the private sector's critical role in generating and amassing the lion's share of the world's data.

There is a bold concept that could provide a means to addressing both of these challenging factors. In partnership with Bain & Company, the World Economic Forum developed the concept of a personal data ecosystem which assigns personal data as a new asset class. In this system, personal data would be controlled, managed and exchanged for compensation, similar to other assets, giving individuals

transparency and ownership over their data. The asset class approach would mean individuals know what data is being collected about them, the value it has, and how they are compensated for it. Personal data would become the equivalent of currency and reside in an account where it is managed and exchanged like today's financial system.[44]

The ecosystem of personal data as an asset class would require collaboration between private firms and governments to build the framework. There would need to be consideration regarding the economic value for the private sector, whilst balancing the needs of policy makers who look at data from a national security and public safety point of view.[45] As a collective, the private and public sector would need to determine global principles and standards around data sharing and usage, as well as the supporting legal framework.

Much like the financial system in place today, if states want access to the economic benefits of personal data, they have to sign-up and adhere to the universal principles and standards. Creating this type of system would by no means be an easy task, but it could create a common global infrastructure, legal and regulatory framework that places needed accountability at the individual and state level.

Big data is inevitably a part of our future. This is a new era, one that has really only just begun. There are many areas yet to be properly understood, and many challenges yet to be addressed. If we want a world where big data can be safely harnessed, there are policy changes that need to be introduced. Perhaps the concept of a personal data asset class is a good place to start.

How much is your data worth? ■

REFERENCES

1 WEF World Economic Forum (2011) 'Personal Data: The Emergence of a New Asset Class' [Online] http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf [Accessed: 24 August 2018].

2 Cukier, K. and Mayer-Schoenberger, V. (2013) 'The Rise of Big Data, How It's Changing The Way We Think About the World' ***Foreign Affairs*** (92:3), pp. 28-40.

3 WEF World Economic Forum (2011).

4 Srnicek, N. (2017) ***Platform Capitalism***, (Cambridge: Polity Press).

5 Cukier, K. and Mayer-Schoenberger, V. (2013).

6 Zwitter, A. (2015) 'Big Data and International Relations' ***Ethics & International Affairs*** (29, 4), 377-389.

7 Rollet, C. (2018a) 'In China's Far West, Companies Cash in on Surveillance Program That Targets Muslims' [Online] https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/ [Accessed: 15 June 2018].

8 Thum, R. (2018) 'China's Mass Internment Camps Have No Clear End in Sight' [Online] https://foreignpolicy.com/2018/08/22/chinas-mass-internment-camps-have-no-clear-end-in-sight/?utm_source=PostUp&utm_medium=email&utm_campaign=Flashpoints%20LiveIntent%208/24/2018&utm_keyword=Flashpoints%20OC [Accessed: 24 August 2018].

9 Rollet, C. (2018b) 'Ecuador's All-Seeing Eye Is Made in China' [Online] https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/?utm_source=PostUp&utm_medium=email&utm_campaign=Flashpoints%20LiveIntent%208/10/18&utm_keyword=Flashpoints%20OC [Accessed: 10 August 2018].

10 The Economist. (2017) 'The world's most valuable resource is no longer oil, but data' [Online] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [Accessed: 28 May 2018].

11 Srnicek, N. (2017).

12 Statista (2019) 'Number of monthly active Facebook users worldwide' [Online] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [Accessed: 23 February 2019].

13 Murray, G. and Scime, A. (2010) 'Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies' ***Journal of Political Marketing*** (9:3), pp. 143-166.

14 Cadwalladr, C. (2017a), "Robert Mercer: the big data billionaire waging war on mainstream media' ***The Guardian*** [Online] 26 February. https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage [Accessed: 20 August 2018].

15 Solon, O. (2018b), 'Cambridge Analytica whistleblower says Bannon wanted to suppress voters' ***The Guardian*** [Online] 16 May. https://www.theguardian.com/uk-news/2018/may/16/steve-bannon-cambridge-analytica-whistleblower-suppress-voters-testimony [Accessed: 20 August 2018].

16 Urbain, T. (2018) 'Facebook as an election weapon, from Obama to Trump' [Online] https://phys.org/news/2018-03-facebook-election-weapon-obama-trump.html [Accessed: 17 August 2018].

17 Cadwalladr, C. and Graham-Harrison, E. (2018b), 'How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool' ***The Guardian*** [Online] 17 March. https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm [Accessed: 21 August 2018].

18 Cadwalladr, C. (2018), '"I made Steve Bannon's psychological warfare tool": meet the data war whistleblower' ***The Guardian*** [Online] 18 March.

19 Baynes, C. (2018), 'Christopher Wylie hearing: Cambridge Analytica whistleblower to give evidence to US Congress over Facebook data breach' ***The Independent*** [Online] 23 April. https://www.independent.co.uk/news/world/americas/us-politics/christopher-wylie-congress-hearing-evidence-facebook-data-breach-trump-a8318016.html [Accessed: 20 August 2018].

20 Graham-Harrison, E. and Cadwalladr, C. (2018), 'Cambridge Analytica execs boast of role in getting Donald Trump elected' ***The Guardian*** [Online] 20 March. https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-execs-boast-of-role-in-getting-trump-elected [Accessed: 3 June 2018].

21 The Washington Post (2018) 'Transcript of Mark Zuckerberg's Senate hearing' [Online] https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/ [Accessed: 27 August 2018].

22 ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)' [Online] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed: 28 August 2018].

23 Solon, O. (2018c) 'How Europe's 'breakthrough' privacy law takes on Facebook and Google' ***The Guardian*** [Online] 19 April. https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation [Accessed: 27 August 2018].

24 Horowitz, J. (2018) 'What is Huawei, and why does the arrest of its CFO matter' [Online] https://edition.cnn.com/2018/12/06/tech/what-is-huawei/index.html [Accessed: 24 February 2019].

25 Fildes, N. and Lucas, L. (2018) 'Huawei spat comes as China races ahead in 5G' [Online] https://www.ft.com/content/0531458a-fd6c-11e8-ac00-57a2a826423e [Accessed: 2 February 2019].

26 Triolo, P. and Allison, K. (2018) 'The Geopolitics of 5G' [Online] https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g [Accessed: 24 February 2019].

27 Fildes, N. and Lucas, L. (2018).

28 Sevastopulo, D. and Bond, D. (2019) 'UK says Huawei is manageable risk to 5G' [Online] https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a211d90d5 [Accessed: 18 February 2019].

29 Harding, L. (2014) ***The Snowden Files, The Inside Story of the World's Most Wanted Man***, (New York: Vintage Books).

30 Greenwald, G. (2014) ***No Place to Hide***, (London: Penguin Books).

31 Greenwald, G. (2014).

32 Hautala, L. (2018) 'NSA surveillance programs live on, in case you hadn't noticed' [Online] https://www.cnet.com/news/nsa-surveillance-programs-prism-upstream-live-on-snowden/ [Accessed: 29 June 2018].

33 The Washington Post (2013) 'NSA slides explain the PRISM data-collection program' [Online] http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ [Accessed: 2 July 2018].

34 Greenwald, G. (2014).

35 Harding, L. (2014).

36 Greenwald, G. and MacAskill, E. (2013a), 'NSA Prism program taps in to user data of Apple, Google and others' ***The Guardian*** [Online] 7 June. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [Accessed: 19 August 2018].

37 Gorski, A. and Toomey, P. C. (2016) 'Unprecedented and Unlawful: The NSA's "Upstream" Surveillance' [Online] https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/ [Accessed: 22 August 2018].

38 Gorman, S. and Valentino-DeVries, J. (2013), 'New Details Show Broader NSA Surveillance Reach' ***The Wall Street Journal*** [Online] 20 August. https://www.wsj.com/articles/new-details-show-broader-nsa-surveillance-reach-1377044261 [Accessed: 19 August 2018].

39 Fidler, D. (ed), (2015) ***The Snowden Reader,*** (Indiana: Indiana University Press).

40 Privacy International (2017) 'A New Era of Mass Surveillance is Emerging Across Europe' [Online] https://medium.com/privacy-international/a-new-era-of-mass-surveillance-is-emerging-across-europe-3d56ea35c48d [Accessed: 30 August 2018].

41 Mitchell, V. and Kamleitner, B. (2018) 'You don't care enough about your data. This is why' [Online] https://www.weforum.org/agenda/2018/06/we-don-t-own-data-like-we-own-a-car-which-is-why-we-find-data-harder-to-protect [Accessed: 29 August 2018].

42 Foroohar, R. (2019) 'California leads the way on data regulation' [Online] https://www.ft.com/content/3406505e-36b9-11e9-bd3a-8b2a211d90d5 [Accessed: 27 February 2019].

43 Denhart, C. (2018) 'New European Union Data Law GDPR Impacts Are Felt By Largest Companies: Google, Facebook' [Online] https://www.forbes.com/sites/chrisdenhart/2018/05/25/new-european-union-data-law-gdpr-impacts-are-felt-by-largest-companies-google-facebook/#4f28b9984d36 [Accessed: 29 August 2018].

44. WEF World Economic Forum (2011).

45. WEF World Economic Forum (2011).

THE AUTHOR

Stacy Langworthy is a management consultant with PricewaterhouseCoopers. She has over 13 years of experience working with businesses to create value through the strategic use of data in the United States, South Africa, and the United Kingdom. She holds an MBA degree from the University of St. Thomas Opus College of Business and an MSc in International Strategy and Diplomacy from the London School of Economics and Political Science.

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

EXECUTIVE MASTERS PROGRAMME

INTERNATIONAL STRATEGY AND DIPLOMACY

LSE IDEAS, a Centre for the study of international affairs, brings together academics and policy-makers to think strategically about world events.

This one year **EXECUTIVE MASTERS PROGRAMME** is at the heart of that endeavour. While studying in a world-leading university you will be able to learn from top LSE academics and senior policy practitioners.

The programme will sharpen your ability to challenge conventional thinking, explore new techniques for addressing risk and threats, and coach you in devising effective strategies to address them.

The course has been especially tailored so that you can accelerate your career while holding a demanding position in the public or private sector.

"Right from the first week I was able to apply the lessons I had learnt to our operational and policy work and to coach my teams to look at issues differently."

- Karen Pierce
British Ambassador to the United Nations

CONTACT US

ideas.strategy@lse.ac.uk
+44 (0)20 7955 6526
lse.ac.uk/ideas/exec

Power Dynamics in an Era of Big Data

STACY LANGWORTHY

In this Strategic Update, Stacy Langworthy investigates a force under-explored and under-theorised in the world of International Relations and policy making: big data. Who can hold it? Who can harness it? What can it do?

For general enquiries:

ideas@lse.ac.uk
+44 (0)20 7849 4918

LSE IDEAS
Houghton Street
Floor 9, Pankhurst House
1 Clement's Inn, London
WC2A 2AZ

lse.ac.uk/ideas
twitter.com/lseideas
facebook.com/lseideas

Cover image credit
xresch on Pixabay