PROJECT MUSE®

Regulation by Revelation: The Opportunities and Challenges of Information Control in an Intelligence Era

Robert Dover

SAIS Review of International Affairs, Volume 36, Number 2, Summer-Fall 2016, pp. 103-111 (Article)

Published by Johns Hopkins University Press

DOI: <https://doi.org/10.1353/sais.2016.0023>

➔ *For additional information about this article*

<https://muse.jhu.edu/article/641163>

Regulation by Revelation: The Opportunities and Challenges of Information Control in an Intelligence Era

Robert Dover

Over the last twenty years, revolutions in data capture and analysis have given enforcement and security agencies unparalleled access to the inner workings and private lives of their adversaries—and ordinary citizens. As a consequence, we would expect to see dramatic improvements in state and private security. However, domestic security agencies are overwhelmed by the sheer volume of information available to them, and have only marginally improved their operational effectiveness. The third wave global Jihadist insurgency works from a model that is analogous to “unicorn” technology corporations, which then provides insights on how to counter these groups. Attempts to keep up with the evolving enemy shift the social contract between governments and citizens. Whilst technologically advanced functionaries create ever more impressive technology, legislators struggle to understand and regulate its impact: the focus on the rights of the individual has been replaced with the primacy of protecting the state. Whistleblowers like Edward Snowden and the LuxLeaks and Panama Papers regarding tax evasion have been the route to transparency for these developments and have made these revelations without protection and to wide scorn. Yet whistleblowers remain the key route for legislators to generate popular and interest group support to try to impose governance over the ungovernable information wars.

Introduction

In the classic work of Hobbes, the life of the ordinary individual was “nasty, brutish, and short,” prior to the formation of the modern state. In theory, modern states removed some of this personal jeopardy, creating a social contract that exchanged some autonomy for security and surety of ownership.

Dr Robert Dover is Associate Professor in Intelligence and International Security at the University of Leicester. He was previously the Director of the Glendonbrook Institute for Enterprise Development, and Associate Dean for Enterprise at Loughborough University in London. Since 2011, Dover has been the Convenor of the UK Political Studies Association's Security and Intelligence Studies Group, which is a specialist group within the association. He is a long-standing contributor to the European Parliament with research and policy papers on a range of security and trade issues. With Michael Goodman, he has jointly convened and edited the UK Arts and Humanities Research Council Intelligence and Security series, which is now published online and which is a joint project with UK Government. They have also recently published the Routledge Companion to Intelligence Studies. Dover is a past winner of the Political Studies Association's annual prize for the best article in Political Studies, which was for his work on intelligence and the arms trade.

Contemporary life, by contrast, is a paradoxical mix of being simultaneously comfortable, radically uncertain, free and yet demonstrably unfree. For much of the post-World War II era, the stark realities of physical threats, like the prospect of war impacting Europe and North America, were replaced by other uncertainties connected to economic development and social change. The central argument in this essay is that the post-war political and social consensus has been replaced by a social environment that is being conditioned by two technology-facilitated drivers: first, the subjective violence that emerges from publicly and privately developed technological innovation and the government use of that technology, and second, the use of this technology by armed belligerents to wage a global war on liberal democratic states and liberal philosophy. This presents an echo of globalization turned back upon the liberal nations who helped to foster and develop neoliberal economic relations.

Jihadist Unicorns

One key insight into Al-Qaeda that emerged in the early 2000s was that it had a sophisticated understanding of branding.² Al-Qaeda's messaging to the world placed it within a niche segment that served to alienate those who were not sympathetic to those core messages, thus appealing to a wider demographic for support. Such conceptual leaps were analogous to, and occurred alongside, the growth in the literature of such insights around 'McDonaldization', 'Disneyfication', and the 'CNN effect'.³⁴ These insights blended an understanding of how globalization helped to push brands and messages into new markets, a quasi-anthropological measurement of the impact of these developments and a refraction of this assessment through the lens of "soft-power." The implied focus of this work is to question whether America's hegemony was partly delivered via its dominance of popular cultural transmission. Whether Al-Qaeda explicitly understood these lessons or was merely reflecting and reproducing the cultural transmission norms already being advanced by the liberal West is moot. More importantly, Al-Qaeda advanced a brand that contained a relatively clear and easily understood set of values, allowing those susceptible to the message to align themselves with the message and therefore the group, and thus to execute these values through a personal jihad or other supportive means. Identifying and challenging the means by which these messages are broadcast, and containing the threats that result, is a battle being fought in cyberspace as part of information control and capture activities.

Al-Qaeda initially carried out its business through face-to-face training in Afghanistan, Pakistan, and parts of the Maghreb, as well as through informal franchises in parts of Europe and the Balkans. During the Afghanistan campaign, the US-led coalition's attack on Al-Qaeda's training structures caused a change in the business model for the group. The command and control structure was no longer tightly formed and the franchise model was given more freedom.⁵ This was, in part, a necessity to avoid being operationally undermined by the number of senior officers killed by the coalition and operational degradation through the destruction of the physical training camps; so, like

most traditional businesses operating in the 2000s, Al-Qaeda moved some of its operations online. Training was then available online (albeit on the so-called “unindexed” deep and dark webs) and in ad hoc camps established like “pop-up shops,” whilst communications moved around a variety of web and satellite-based platforms. The one exception to this move online was financing, which went back to ancient models of passing cash between intermediaries.⁶

The “business model” of Al-Qaeda looks like the “click and collect” variant of traditional supermarkets compared to that of the so-called Islamic State; it still has a physical presence, it has a traditional work force, and it has adopted internet technologies to improve operations. But Al-Qaeda is not a predominantly digital brand utilizing all the multimedia channels and it has been usurped by an insurgent online company with a much savvier take on the digital domain.⁷ And so, if Al-Qaeda is a click and collect supermarket, the Islamic State is the equivalent of a technology “unicorn.” A “unicorn” is broadly defined as a high-value entity (with an estimated value of over one billion dollars) that is disrupting a traditional industry area, staffed by very few people, but which retains high global impact. Prominent “unicorns” include the taxi firm Uber and accommodation facilitator Airbnb. The Islamic State fits this model because its primary existence is online, it has a very clearly delineated brand, a production unit with industry-standard production values, a large number of social media advocates, and cyber-warriors who conduct aggressive operations in the cyber-sphere.⁸ The Islamic State has also bifurcated its physical presence to capture and control ground, population, and resources (with some success in Syria, Iraq and Libya) and to carry out asymmetric military attacks on adversary targets, notably in Paris and Brussels. Even without a physical presence in Iraq, Libya, and Syria the Islamic State would be capable of generating a physical effect on the ground: this is because of the interaction of the brand with potential followers, the *carte blanche* given by Islamic State to prospective followers to do as they wish in their countries of origin in the name of Islamic State’s war against the West. The brand centers on the ends justifying the means and unrestrained, but allegedly theologically justified, actions.

The systems that Al-Qaeda used, such as Voice Over IP (VOIP) and satellite telephony, are a generation behind, and governments have invested very heavily in technologies to intercept these kinds of communication.⁹ Bulk collection of these types of communication technology does, however, impact large swathes of the ordinary population whose communications are now being collected in some form, arguably eroding core rights to privacy. By contrast, the technologies being predominantly used by the Islamic State are not entirely immune from government interception, but are vastly more complicated to intercept. Further, they are not mainstream forms of communication used by ordinary citizens. The Islamic State has not endured the problems with communications across its networks for several distinct reasons. The first is that it has used a panoply of secure messaging systems, be they the Russian hosted and encrypted “Telegram,” various Tor compliant (and thus effectively encrypted) systems, and even an innovative use of multiplayer videogame platforms to pass messages during live gameplay. The other operational success of the Islamic State is the use of “clean skins” to carry forward its brand and to carry out

its operations. In intelligence terms, a “clean skin” is someone who has never come to the attention of law enforcement agencies before and thus would not be someone to whom law enforcement would readily turn in the course of an investigation. The use of such people radically improves the chance of a terrorist plot being successful, or at least that person being able to operate for longer before being identified. This partly accounts for why there has been such an emphasis on the role of intelligence agencies in detecting and preventing terrorist activities, and why the agencies have placed a great emphasis on bulk collection of electronic intelligence.

The ICT Arms Race

There is a technology arms race between extremist movements and government intelligence agencies (and those private companies who support or sell services to the intelligence community). For intelligence services across the transatlantic areas, the profound scarring from significant terrorist attacks—for the US in 2001, for the UK in 2005, and for France and Belgium in 2015 and 2016—and the resulting negative public and political attention those have brought were then transformed by officials and legislators into a permissive environment for security agencies. This permissive environment delivered enlarged budgets, government oversight and regulation which is geared towards securing better outcomes, and technologists who have taken advantage of rapidly evolving and cheaper technology to create ever more effective intelligence related technologies. The revelations from Edward Snowden demonstrated that intelligence technologists have been developing technology and operational methodologies more quickly than regulators and legislators can adjust to. Consequently, mass interception of entire populations discreetly became the industry standard within the intelligence community during the 2000s. Snowden himself demonstrates the flip-side of agencies employing people capable of breaking technological paradigms, namely that when these technologists are matched to libertarian political beliefs (as a lot of creative technologists are) it can be acutely hazardous to the business of state secrecy.¹⁰ Snowden’s central political belief was that the NSA had gone beyond its core mission of protecting the American people and that the actions of the NSA were becoming injurious to liberty in general. According to this libertarian belief, one held by a marginalized few, the social contract that currently exists between state and citizen is in flux and there is a gap between the government’s understanding of the social contract and the understanding of citizens.

For the most part, citizens believe that they have a right to privacy, and so their electronic communities are as protected and private as other types of analog means of communication.¹¹ The Snowden argument is that privacy is a collective rather than individual right and, as Hobbes also noted, that we cannot delineate between an important thought that will impact humanity as a whole, and one that is superfluous in the contemporary moment. In the contemporary sphere, commentators and activists have evoked both the suffragettes and the activism of Nelson Mandela as examples where a harsher restriction

on freedom of speech could have further curtailed the rights of women and the equality of races, something that we now consider to be fundamental and universal human rights. Such is the tension in modern society between those who believe that radical Jihadists should be allowed to say what they want in the belief that the marginal effect of terrorist recruitment does not supersede the individual's right to privacy and those who believe that individual rights need to be curtailed in the face of what they perceive to be the existential threat of Jihadist terrorism. This debate is relevant both in the analog space—for the speaker on the sidewalk, or a view expressed in a classroom—and in cyberspace, where the positions drawn are somewhat more stark. This tension between Western, liberal traditions, and those seeking to broadcast extremist or fundamentalist views partly fuels the contest, and these tensions became manifest in the contests with fascism and communism during the twentieth century. For liberals, the continued extremist narratives and their escalation reinforces that those holding extremist views require additional measures, whilst for Jihadists the continual attempted curtailment of their activities fulfils their narrative of marginalization.

The erosion of individual privacy is not just a product of state security. It is a function of post-industrial capitalism and the transition from the consumption of material goods to the consumption of services. Service industries reliant on the internet (be it PC or mobile) are dependent on the throughput of individualized data to be able to send targeted messages encouraging consumption in a given area or of a particular thing that is of interest to the recipient. In their own ways, Google and Facebook have achieved near monopoly positions in terms of search, news, and advertising precisely because they are incredibly good at being able to deliver bespoke and personalized content to billions of users. The trade-off for the user is ostensibly free-to-use services in exchange for personal data. What is interesting, in sociological terms, is the jarring juxtaposition of conflicting narratives about information collection across the modern era. The film “The Lives of Others” depicts the somewhat soulless existence of an intelligence officer in the Communist East German Stasi collecting intelligence minutiae on a theatre director and his actress partner.¹² They are involved in low-level dissent against Communism, but nothing that posed a significant threat to the regime. We are invited and readily accept the invitation to be reviled by this level of intrusion and yet, in comparison to the sort of data that the Stasi were able to collect, our expensive and impressive smartphones out-collect and out-power the Stasi at its zenith by multiple orders of magnitude.

The Snowden corrective to our understanding of our relationship to technology is that technology has radically undermined the ability of citizens to conduct themselves in private, and technology has greatly increased the knowledge available to the security state about aspects of the citizenry's private lives that have no impact upon security. One of the more interesting conclusions we should draw from the prominence of the testimony of whistleblowers is that the public's conception of issues such as privacy and how their electronic communications should be treated, as well as other related issues such as tax morality, has been shaped by activist individuals in privileged positions ignoring the risks they face in producing unauthorized disclosures.

International Tax Avoidance - Technology and Revelation

The issue of aggressive corporate tax planning and avoidance has been exposed by the interaction between technology, information, and whistleblower revelation. The major accelerants in making aggressive tax planning salient in the policy sphere have largely come through the series of leaks from whistleblowers in Luxembourg, Liechtenstein, and Panama. The increasing capacity of movable data storage and the inexpensiveness of that storage have exponentially increased the amount of harm that data leaks can do to a particular organization. The explicit trigger for the European Parliament's investigation and legislative initiative on corporate taxation in 2015 and 2016, for example, was the *LuxLeaks* of November 2014, in which Antoine Deltour revealed to the International Consortium of Investigative Journalists (ICIJ) the secret tax deals to which the authorities in Luxembourg had agreed with Multinational Enterprises (MNEs).¹³ Deltour had used a secure messaging service to “drop” the files to the ICIJ, which illuminated practices which have now been subject to restriction by the European Parliament and Commission. Deltour's actions were praised by the European Commission, amongst others, whilst he was prosecuted in Luxembourg and sentenced to a 12-month suspended jail sentence in June 2016.¹⁴

In 2008, Heinrich Keiber (who now lives in hiding), an employee of LGT Liechtenstein, sold a disk containing financial data to the German internal intelligence agency, the BND, which showed how nearly one thousand high-value individuals had hidden their tax affairs through contrived or artificial business arrangements. The BND passed the information on to German tax authorities who began legal proceedings against some of those named on the disk. In 2013, *Offshore Leaks* was published by the ICIJ, which revealed details of 130,000 offshore trusts that, while legitimate, have also been used to avoid tax. The *Swiss Leaks* scandal of February 2015 was triggered by an HSBC software engineer, Hervé Falciani, who had initially released information to the French tax authorities in 2008 detailing the alleged tax avoidance from HSBC account holders and 20,000 offshore companies, but which became part of a further ICIJ release in 2015. Falciani was prosecuted *in absentia* in Switzerland and sentenced to five years in prison. Most recently, in April 2016, a presumed internal leak by ‘John Doe’ (who also remains in hiding), released over a terabyte of data to the ICIJ, which became known as *The Panama Papers* and which amounted to 11.5 million records relating to 114,488 offshore companies from the law firm Mossack Fonseca. This was the largest leak of this series demonstrating, in part, the use of offshore company structures to avoid taxes of various kinds.

Leaks represent a significant challenge for areas of government dealing with sensitive issues, including tax authorities. The public policy challenge is that whilst whistleblowers can be seen as a counterintelligence problem, they have also been demonstrably more effective than parliaments and oversight regimes at revealing widespread, international abuse of tax codes, and yet have done so with very little protection. This seems even starker when it is governments that stand to benefit from collecting a large proportion of the €150–190 billion corporate taxes eluded via base erosion and profit shifting.

When it comes to personal finance, the increased use of technology is having—in some parts of Europe—a strong impact on reducing the evasion of value-added taxes on goods, as physical cash is phased out and replaced with public use touch-technologies such as *Apple* or *Android Pay*, or RFID-enabled debit cards to make micro-payments, allowing fully auditable and traceable transactions to occur and reducing the ability to manipulate value-added tax. This technology has been warmly embraced in the Scandinavian countries, whilst almost universally shunned in Germany because of deeply embedded fears around state surveillance and oppression.¹⁵ Cash transactions have also played a large role in the attempts to track terrorist logistics lines. Pushing terrorists to move physical cash disrupted some of their activities in the mid-2000s; the Islamic State learned from this and instead carries on its own petrochemicals and extortion trade to secure funds directly at source.

Conclusion

Advances in communication technology have offered consumers unprecedented access to knowledge, news, and competition in goods and services. These advances are capable, via advanced cryptography, of providing individuals with enhanced levels of privacy. But the problems associated with attempting to go “off-grid” are manifold; for example, it is technically very difficult to do so, particularly while continuing to enjoy the trappings of contemporary Western life. With geo-positional services being built into “smart” and “dumb” mobile phones, the only option to move without a trace is to travel without a telephone and seek to avoid CCTV. The alternative, which is to engage privacy software, is to raise suspicions about what motive one might have to do so. Many of the platforms that provide such privacy are now tainted by government and media narratives. TOR browsers and services, and encrypted email and messaging platforms are almost ubiquitously described in the media as services that are used by those engaged in organized crime, terrorism, or child sex exploitation. There is also increasing evidence that these platforms are becoming insecure as well.

The ability of intelligence services to remotely access the microphones in mobile phones has brought the security and surveillance state into the home. But the success of the jihadist extremists has been to unleash the security state onto their own ordinary citizens, in a way that could not be imagined even as recently as the early 1990s. Consequently, through legislation and the development of technology, the social contract in Europe, and to some degree the United States, has radically shifted to a state-first social contract, albeit whilst the majority of the electorate believe that it remains premised around the rights of the individual.

The new social contract essentially provides no right to privacy and a privileging of collective security and the security of core infrastructure over those individual rights. The public has largely been in favor of curtailing the rights of “dangerous others,” whilst not realizing that mass surveillance also applies to them and fundamentally changes their relationship with the state. The dangers inherent in the state’s overwhelming dominance in the surveil-

lance space only arise if the state uses these tools for radically illiberal purposes, which is becoming increasingly likely in Europe as nationalist politicians gain traction in the face of the immigration and terrorism crises that are dominating political discourses across the continent. The ubiquity of communications technology raises the prospect of a totalitarian Western state being able to successfully manage dissent and threats to its existence in way that was previously unimaginable. That the major advances in public and political knowledge about the potential and operational use of these technologies has come from whistle-blowers demonstrates the relative weakness of official oversight and regulatory regimes. The alleged treachery of Snowden may well have the consequence of rebalancing and strengthening democratic control of the intelligence services and of making the general public less accepting of the surveillance potential of their communications technologies.

Notes

¹ Dr Robert Dover is Associate Professor in Intelligence and International Security at the University of Leicester. He was previously the Director of the Glendonbrook Institute for Enterprise Development, and Associate Dean for Enterprise at Loughborough University in London. Since 2011, Dover has been the Convenor of the UK Political Studies Association's Security and Intelligence Studies Group, which is a specialist group within the association. He is a long-standing contributor to the European Parliament with research and policy papers on a range of security and trade issues. With Michael Goodman, he has jointly convened and edited the UK Arts and Humanities Research Council Intelligence and Security series, which is now published online and which is a joint project with UK Government. They have also recently published the Routledge Companion to Intelligence Studies. Dover is a past winner of the Political Studies Association's annual prize for the best article in Political Studies, which was for his work on intelligence and the arms trade.

² Brian A. Jackson, "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda," *Studies in Conflict and Terrorism* (2006): 241–262.

³ Piers Robinson, *The CNN effect: The myth of news, foreign policy and intervention* (London: Routledge, 2005), pp.192.

⁴ Uri Ram, "McDonaldization," in *The Wiley-Blackwell Encyclopedia of Globalization*, by G Ritzer (London: John Wiley & Sons, 2012), 342–347.

⁵ Mary Uhl-Bien and Russ Marion, "Complexity Theory and Al-Qaeda: Examining Complex Leadership," *Emergence* (2003): 54–76.

⁶ Aimen Dean, Edwina Thompson, and Tom Keatinge, "Draining the Ocean to Catch one Type of Fish: Evaluating the Effectiveness of the Global Counter-Terrorism Financing Regime," *Perspectives on Terrorism* (2013): pp.62–78.

⁷ Helen Roby, "'Click and collect': how will this affect e-tailing?," *British Academy of Management* (2014). Belfast: BAM

⁸ Charlie Winter, *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy* (London: Quilliam Foundation, 2015), 52.

⁹ Marco Benini and Sabrina Sicari S, "Assessing the risk of intercepting VoIP calls," *Computer Networks* (2008): 2432–2446.

¹⁰ Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (London: Guardian & Faber, 2014), 352.

¹¹ For example, see the COMRES poll conducted in March 2015: <http://www.bigbrother-watch.org.uk/wp-content/uploads/2015/03/Big-Brother-Watch-Polling-Results.pdf>

¹² *The Lives of Others*, Directed by Florian Henckel von Donnersmark (2006; Germany: Buena Vista International, 2007), DVD; Gregory Jordan and Thomas Catlaw, "Public Administration and "The Lives of Others": Toward an Ethics of Collaboration," *Administration & Society* (2009): 290–312.

¹³ Erik Jones and Robert Dover, 'Bringing transparency, coordination and convergence to corporate tax policies in the European Union. Part I: Assessment of the magnitude of aggressive corporate tax planning,' Brussels: European Parliament (2015): pp.1–63 in Robert Dover, "Fixing Financial Plumbing: Tax, Leaks and BEPS in Europe," *The International Spectator* (2016) Forthcoming.

¹⁴ Quentin Aries and James Panichi, "The #LuxLeaks whistleblowers verdict," *Tax Justice Network* (2016).

¹⁵ Liz Alderman, "In Sweden, a Cash-Free Future Nears," *New York Times* (2015).