Legal Clouds: Balancing Privacy and Surveillance in the Cloud

Constantinos Macropoulos (macro@greenhatlabs.com) and Keith M. Martin (keith.martin@rhul.ac.uk)

As cloud computing grows, the private sector has a pivotal role to play in balancing the privacy needs of the individual and the security demands of the state.

Abstract

As technology integrates into every aspect of people's daily lives, it's easy to lose sight of the vast amounts of data generated by the devices and services that they've come to rely on. When productively harnessed through cloud-based technologies, this data has the ability to empower the individual. However, it also brings significant privacy challenges, particularly when states seek to leverage this same data to enhance law enforcement and intelligence capabilities. The authors suggest that the private sector has a pivotal role in establishing norms in this area and that doing so in a manner respectful of the individual is ultimately in everyone's best interests.

Introduction

At the intersection of privacy and technology in cloud computing environments lies the private sector, which has played a significant role in shaping the development of cloud computing technology. Although technological development tends to be driven by the financial motivations of private-sector interests, its scale and ubiquity is ultimately mediated by individuals (all of us), who have come to rely on it in our daily lives.

However, the devices and services that individuals depend on are increasingly collecting data about us at a scale and rate never before conceived. In parallel, as organizations seek to maximize the value of these vast swathes of data, the potential economies of scale achievable through cloud computing make it a compelling proposition for big data initiatives. This almost symbiotic relationship between big data and cloud computing means that the data will increasingly reside under the control of cloud service providers.[1] This trend is likely to accelerate as Internet of Things (IoT) and cloud-based solutions gain traction. Although our ability to harness this data productively empowers us as individuals, all too often our control over it is limited and potentially comes at the expense of our personal freedom.

Similarly, law enforcement and intelligence arms of states across the globe are keenly aware of the empowering possibilities inherent in accessing the dense pockets of data that have developed as a result of cloud computing. Before the widespread adoption of cloud computing, the dispersed and often ephemeral nature of data concerning individuals didn't as readily lend itself to aggregation and analysis. Its very nature made bulk collection for the purpose of preempting threats to public safety challenging, tedious, and resource intensive, even at the smallest scale.

Although this is but a single aspect of far broader state "cyber" aspirations, which bring with them diverse implications for the private sector,[2] it is to a degree unique. In this instance, the private sector has found itself in the position of arbiter between the state's desire for visibility into the daily lives of individuals, and the individual's desire to control what, and with whom, to share. This position has become more pronounced since the emergence of cloud computing. The private sector has to an extent put itself into this position, and it might not be able to extricate itself. When it comes to the thorny question of how to balance privacy and surveillance, the private sector has a responsibility to contribute actively and meaningfully in any search for acceptable answers.[3]

Pivotal Role of the Private Sector

Some might consider it unusual to look to the private sector to play a pivotal role in addressing wider societal issues surrounding privacy in cloud computing. Its reputation has been affected by "surveillance as a business model" being at the core of many online services.[4] Despite this, when assessing the private sector's role in the future of privacy, we need to take a more pragmatic approach.

Looking at the existing distribution of personal data, both created by and generated about individuals, we can better appreciate that the cumulative data under the control of private interests provides greater insight into our lives than would normally reside under state control. This disparity between the volume and nature of data in private control, compared to state control, explains why we've seen such significant efforts on the part of states, effectively deputizing the private sector in data collection.

Over time, much of the data states retain on individuals might also move into private-sector custody. We're already seeing many governments take tentative steps toward migrating less sensitive functions to public cloud providers. It seems reasonable to assume that as comfort with cloud technologies grows, and if the level of cost efficiencies envisaged are realized, we'll see a shift in perceived risk-to-reward ratios. In turn, this could justify, at least in the eyes of some governments, migration of increasingly sensitive data to public cloud environments. In parallel, the desire of many states to engage in greater public–private partnerships with regard to increasingly sensitive services will ensure that even more data makes its way out of direct physical state control.

The state's willingness to expose its data on individuals to the private sector, while simultaneously seeking access to existing private-sector data, gives insight into state perceptions regarding where true value resides. Clearly, the private sector lies at the heart of the problem, and is therefore central in any viable solutions.

Problems for the Private Sector

"Private sector" is a nebulous term, encompassing a wide range of industries, structures, objectives, and challenges. With respect to privacy and the cloud, all face some fundamentally similar problems.

Threats to Data and Reputation

In an information-based economy, an enterprise's two most valuable assets are data and reputation: data because it's the raw material used in the creation of information; and reputation, not only because it's the grease that in many cases lubricates data acquisition, but also because it increases the perceived integrity and therefore the value of the information generated. Additionally, there's often a complex yet symbiotic relationship between these assets. The core problem for the private sector is that trying to balance the demands of states against individuals' expectations of privacy will affect these assets' value.

Meanwhile, the accumulation of data about or from individuals, whether they're customers, partners, employees, or users, is increasing. Often this data is considered innocuous and privacy considerations are rarely afforded much thought, particularly when the data is securely stored on internal systems. Once this data migrates to the cloud, however, the dynamics change.

As data with similar "selectors" from multiple sources comes under the physical control of a single entity, its density increases its surveillance appeal. In parallel, the data's security increasingly relies on a chain of assurances, invariably leading to it becoming decoupled from the relationship surrounding its initial collection. This is of particular concern where a veil of secrecy surrounds state access to data, and immunity from civil liability is extended to directly cooperating parties, since this raises questions as to how vociferously privacy concerns might be challenged in the absence of direct interest. The risks to reputation, and in particular trust perception, not to mention liability concerns,

are problems that the private sector is just beginning to wrestle with. The quandary for the private sector is that managing and creating value from this ever-increasing mountain of data results in an insatiable appetite for computing services at costs and scales that are often prohibitive to provide internally.

This fundamental undermining of trust speaks directly to a subtle, yet perceptible, devaluation of the reputations so carefully cultivated by many private-sector entities. Recent revelations into the relationships that have developed between states and some private sector interests haven't helped. In some cases, these appear to have been based on exploitation or coercion; in others, they've raised suspicions of collusion. This has undermined trust, not just between individuals and the private sector, but also within the private sector itself.

If customers believe their privacy is under threat, their choice of provider will be heavily biased by trust considerations, or they might choose not to use a service at all. This is of particular concern to the private sector, since negative perception can significantly influence consumer decisions, particularly in competitive markets where product differentiation is often tenuous.

Threats to Flexibility

The evolution of cloud computing is a reflection of economic imperative. At a physical level, it's driven by developments in the underlying technologies that make computing possible. Although the individual projections of Gordon Moore, Mark Kryder, and Gerry Butters might strain over time, when combined they highlight the dynamic nature of "economically optimal" computing.[5] The ability to flexibly adapt to this ever-evolving computing ideal, allowing providers to cost-effectively utilize, modify, and scale their environments to meet changing needs, is in part what makes it attractive. This architectural flexibility, when combined with cost efficiencies derived from scale, gives customers access to computing capabilities they might not have ordinarily been able to afford.

Insertion of the state into this equation, however, raises issues for the provider and potentially affects the service level. For example, having to implement state surveillance capabilities within a cloud architecture complicates decisions, inhibits flexibility, restricts change, and invariably increases operational costs. All of this erodes provider competitiveness.

Threats to Innovation

It's also important to consider that the form state surveillance capabilities take can impact innovation. A physical surveillance infrastructure will primarily cause operational difficulties for providers. But physical surveillance infrastructures in cloud environments is of limited use since it can't match the elasticity and scalability of the environment it needs to process, making it less than ideal for bulk surveillance.

Because software is at the core, a more sensible technical approach would be to develop state surveillance capabilities at this level. In such cases, the state would likely seek to exercise some influence over technological developments, thereby ensuring that its capabilities are maintained and its investment protected. Likewise certain advances, though advantageous from a technological perspective, might be abandoned under pressure from the state if they have potential to inhibit surveillance. Overall, a situation such as this would likely see the state position itself as final arbiter on innovation.

Paradoxically, the state doesn't even need to be directly involved to stifle innovation. Revelations of the pressures exerted by states to ensure the advancement of surveillance efforts undoubtedly have a cooling effect on the development and provisioning of privacy-enhancing technologies. On the one hand, private-sector entities must consider the potential repercussions of drawing the state's ire, and

on the other hand, the secrecy that surrounds state efforts to compromise such technologies means that distrust has become the default initial response to any such innovations.

Threats to Data Movement and Competitiveness

It's important to recognize that privacy issues extend well beyond the actions of the intelligence services of a few states. Most states are engaged, or aspire to engage, in many of the same activities recently documented for the Five Eyes nations.[6] Although the Edward Snowden revelations forced questions about privacy onto the global stage and brought them to the forefront of many state agendas, the focus of these agendas has in many cases revolved around issues of sovereignty, capability sharing, and boundaries on the surveillance of state officials, rather than around individual privacy.

Indeed, a common trend among many states is to advocate for the retention and processing of their citizens' and residents' data within their respective jurisdictions, believing that this will address privacy issues. Unfortunately, this has more to do with issues of sovereignty than privacy. In real terms, we know little about the activities of the US and its partners, but we know even less about similar activities by other states. This is cold comfort for the individuals concerned about their privacy, or for private-sector entities operating in a global economy.

The specter of restrictions on the movement of data creates operational difficulties for private-sector entities trying to compete internationally, particularly where cloud computing is concerned. At a fundamental level, this geographical constraint undermines the economic underpinnings of the cloud concept. For larger cloud providers and customers, this "Balkanization" inhibits the elasticity of cloud services, resulting in an inability to fully realize the cost advantages. For small niche players, it has an even greater impact because it restricts their ability to compete globally, and in turn inhibits further innovation, particularly with innovations where viability relies on scale. This in turn ensures that only large providers that can afford to invest in dedicated infrastructure at multiple locations across the globe can compete. Although this scenario might at first glance appeal to large players, the resultant impact on innovation potentially restricts their options to access new technology streams through acquisition. It's also noteworthy that states are becoming distrustful of companies based on national origin.[7] The "incentivization" of domestic cloud providers potentially undermines the competitiveness of international providers and inhibits market access.

The Challenge for the Private Sector

Ultimately, issues related to privacy are a major, sometimes disregarded, source of problems for the private sector, and they'll become more so as reliance on cloud environments grows and global markets become more competitive. The challenges left to the private sector are balancing the privacy needs of the individual and the needs of the state as cloud computing grows, and determining what role it should play in this process.

When considering policy and law in relation to technology, semantic differences are often the biggest obstacles. The lack of a common nomenclature across disciplines leads to misinterpretation among stakeholders, which in turn leads to fractious debate. Being mindful of this potential for misinterpretation is particularly important for the technical community. Technicians must convey to other disciplines knowledge not only of the capabilities and limitations of technology, but also of the physical world implications of technology. Likewise, a greater level of technical literacy is required from those in other disciplines attempting to address privacy problems since the technology is complex and its implications far-reaching.

When we look at cloud computing within the context of lawful data access and legitimate surveillance, one aspect is particularly relevant. At a basic level, "the cloud" conceptually refers to computing uninhibited by physical—and by extension geographical—constraints. This poses significant challenges when we then consider legitimate surveillance and lawful data access, as these

activities have historically been bound by geography to cultural norms, jurisdiction, and sovereignty—concepts that are the antithesis of what "cloud" means to computing.

Similar problems arise when looking at the idea of "privacy." Like many important concepts, privacy isn't easy to define universally. The concept of privacy and its role in society is underpinned by complex cultural norms and unique value systems that have developed and been refined over time, often within unique historical contexts. Adding to this diversity are the practical aspects of how an individual exercises privacy, and the dynamic nature of trust, which influences how an individual reinterprets trust over time. What is shared, with whom, and when, are all aspects of privacy that guarantee that one size will never fit all.

The Role of the Private Sector in Solutions

There are rarely easy or straightforward solutions to complex problems, particularly those with global dimensions. However, political, legal, and technological approaches can be taken to ease the gradual establishment of generally accepted norms, and the private sector has an important role to play in their development.

The Need for International Consensus

Although technology has an important role to play, political and legal problems can only be solved through political and legal means. Information technology is merely the newest arena within which societies are seeking to balance the needs of the state with the expectations of individuals.

What is particularly complex is that the technologies we're building bring with them a global, cross-jurisdictional dimension, where concepts of physical distance and physical barriers have reduced relevance. For political and legal means to have a chance of addressing these problems, there first needs to be a sustainable level of consensus among states. In the current environment, where distrust and secrecy dominate the state's involvement in technology, and heated dialogue centers on topics such as cyberespionage, cyberterrorism, and cyberweapons, individuals and their immediate needs tend to be forgotten. There's an immediate need for productive multilateral discussion between states.[8] However, with few, if any, countries retaining sufficient moral authority to influence dialogue, the private sector could be the catalyst that changes the direction of discourse.

The Role of Education

Before contemplating any shifts in state attitudes, we need to help policymakers better understand and appreciate the societal and economic benefits of information technology. Historically, we've seen a wide range of interest groups espousing and promoting these benefits; however, the success of these efforts is questionable. Repeatedly we find ourselves in scenarios where state activities and aspirations, particularly with respect to intelligence and law enforcement, reach such proportions that they're perceived as excessive by numerous individuals and private-sector entities. Once a trust deficit develops, the integrity of technologies from certain countries is questioned and relationships with some types of technology are reassessed. Sometimes this occurs to an extent that sentiment shifts risk damaging the technology sectors of the states involved, and inhibit the adoption of technological advancements in the private sector globally.

The traditional attitude in the technology sector is that governments "don't get it." Perhaps it's a generational problem, or perhaps a technical literacy issue, but recent events appear to confirm a need to redouble our efforts to improve governments' understanding of technology and its implications for privacy. This is particularly important with respect to policymakers, because they can't be ignored if technology and privacy are to have a cohesive future. It's also important that efforts focus not just on what technology can do for the state and society, but also on the positive and negative impacts the state can have on technology and privacy.

The private sector has an important role to play here. It has access and influence, but needs to use these far more progressively. Instead of focusing on advancing its own agendas, it needs to start thinking strategically. What's needed is the careful creation of overarching initiatives, with broad private-sector support, aimed at promoting a common understanding of the issues and technologies among governments, with deference to the needs of the individual.

Changes in Attitude

Strategic thinking will require changes in the private sector's perspectives and attitudes, but companies that transition might well flourish as their reputations increase. For example, companies that view the individual as "the product" rather than "the customer" might need to investigate more flexible business models, since exploiting privacy ignorance might not be sustainable if privacy awareness increases.

Related to this is the need for individuals to decide what privacy is worth to them and pay for services accordingly. Educational, pricing, and business modelling research needs to be conducted. Ensuring a future Internet that balances security and privacy for all requires the participation of individuals, not just corporations.

Transparency

Events over the past few years have shone a spotlight on issues of transparency. In particular, its absence from state intelligence and law enforcement activities has caused significant headaches for private-sector entities. Secret interpretations of law, exercised in secret courts, ultimately engender an air of mistrust in a legal system's integrity, which in turn gives rise to perceptions of underlying sinister intent. For private-sector entities that find themselves embroiled in controversies relating to rulings from such a legal system, and unable to discuss any aspect of their involvement as a result of legal orders, these perceptions are transitive.

Although it might be necessary at times to shroud what is referred to as lawful data access and legitimate surveillance in a veil of secrecy, excessive secrecy in perpetuity is potentially counterproductive. States operating these types of legal regimes, and states moving toward them, need to carefully consider the potential consequences of their existence coming to light.

The private sector needs to encourage governments globally, through engagement with representatives or through litigation where necessary, to put in place appropriate mechanisms that allow it to make public information about the government requests it receives. In parallel, the private sector needs to work in unison to consolidate this information, preferably through independent third parties, into a meaningful and accurate depiction of the state of privacy globally. This will provide greater transparency on not only what is happening in a given country, but also on how other countries compare. Additionally, it creates a valuable body of information that researchers across disciplines can use to bridge global gaps in privacy norms.

Legality

Although failures in certain government attitudes have played a significant role, the private sector has acted as an enabler.[9] Private-sector entities must ensure that all state collections of data in their custody are subject to the full rigors of the law, and that any requests they process are fundamentally lawful and necessary. Where doubts exist as to a request's veracity or necessity, it must be challenged by all available means. Ultimately, private-sector entities must establish a reputation, supported by a substantial track record, of defending data in their custody with as much determination as the individual who provided it would afford.

Once all avenues of challenge have been exhausted, private-sector entities need to ensure that they provide only what is legally required. Their responsibility doesn't end there, however. The private sector needs to push for mechanisms to ensure that once data is handed over, it's used only by those in government who need it, and then only for the purpose for which its collection was ordered. Further, it needs to ensure that the retention of this data in perpetuity is the exception rather than the norm. What isn't required by the state, as defined by the criteria of its original collection, needs to be disposed of securely.

Although these principles are applicable to all data, they're particularly important with respect to metadata, which can pose a significant threat to privacy,[10] particularly once aggregated. Because of its nature, metadata can often be difficult to protect, from a privacy perspective, using purely technological means. Metadata creation must therefore be kept to a minimum and it should be retained only for as long as is necessary.

At a more general level, it's in the private sector's best interest to ensure that it isn't left alone in the spotlight when there are perceived excesses in the state's exercise of power. The private sector must therefore push for the establishment of accountability and meaningful independent oversight, designed to inform policymakers on the programs and mechanisms used by government in its pursuit and collection of private-sector data.

Empowering the Individual

All the measures discussed thus far are, to an extent, limited but necessary. Their ability to influence norms will vary from state to state, depending on the mechanisms available to initiate change. Calls for balancing the privacy needs of the individual with the needs of the state are, for example, unlikely to garner much support in a tyranny. Although mileage might vary when it comes to political and legal means as instruments of change, technology has consistently proven to be a powerful instrument of change, with the ability to influence norms on a global scale.

When we look at privacy based on all we've discussed thus far, we see the importance of the individual. We also see that meaningful privacy is shaped by individuals based on their needs and perspectives. Thus, from a technological perspective, we need to focus on empowering users, allowing them to translate their physical worldview of the trust relationships in their lives into an accurate digital representation. This isn't a new concept, but thus far we've failed to develop privacy-protecting tools that are user-friendly enough for the typical user. Sometimes the difficulty lies in the technology's complexity; other times it comes down to a lack of technical literacy among users.

Directly related to the concept of empowering users is diversity. We need to give individuals choices, not only in the tools they use to protect their privacy, but also in the ability to fine-tune how those tools implement those protections. This might seem contradictory to a user-friendly approach, but we need to find a way to reconcile these because, by permitting others to be the arbiters of an individual's privacy, we're allowing the societal stratification of privacy. Those with sufficient influence and power to protect their privacy will succeed; those with the technical knowledge to defend their privacy will try but their privacy will be under perpetual threat; and the majority will be left with little autonomy over their privacy.

Zero-Knowledge Principles

In relation to cloud computing we face a range of technical conundrums, primarily because it's far more difficult for individuals to control what happens to their data on someone else's system. We need a widespread adoption of "zero-knowledge principles," where neither the cloud service provider nor anyone else, apart from data owners and their delegates, has visibility of unprotected data. Ultimately, this prevents the service provider from being able to act as a surrogate for the state's

actual target of investigation, relieving the service provider from associated legal, ethical, operational, and commercial burdens.

Although there has been remarkable commercial progress in the storage-as-a-service arena in adopting these principles, a need remains for additional research and development in technologies and protocols to secure privacy across the broadest range of possible use cases, particularly collaboration.[11] Unfortunately, although the nature of storage-as-a-service lends itself particularly well to established technologies that can secure privacy, other cloud services are less fortunate. In particular, services where processing is conducted within the cloud face significant constraints in implementing zero-knowledge principles with existing technologies. Concepts such as fully homomorphic encryption[12] and program obfuscation[13] could yield solutions but, although researchers have made significant strides in the recent past, progress toward practical application is only achievable through open and collaborative efforts among private-sector interests.

The widespread availability of a diverse range of tools geared at protecting the privacy of individuals, when combined with an established widespread acceptance of zero-knowledge principles among cloud service providers, should, over time, shape international norms. This could be further strengthened by adherence to free software principles, which will enhance transparency, improve diversity, and, given sufficient private-sector support, lead to accelerated innovation.

Overcoming Resistance

Any approach seeking to balance privacy and state controls will invariably meet with some resistance from the state and its subordinates. Technological efforts, in particular, will meet with resistance.[14] Fundamentally, it's important that the private sector make the case that these efforts don't prohibit the state from policing or conducting intelligence activities. They merely restrain a "collect it all" ethos from undermining the privacy of the majority.

As has always been the case, no technical measure can completely inhibit the state from exercising its powers if it's determined to target an individual. The state has technological capabilities that can make short work of personal computing devices and intercept data before privacy-protecting mechanisms come into play. Additionally, it has other levers of power at its disposal that can be exercised against the individual, and extend beyond purely technological means. States might argue that this is time consuming and difficult, yet when have policing or intelligence activities not been?

This isn't the first time that society has engaged in this type of debate. The battles that raged between the state and the technology community throughout the 1990s in the US and elsewhere over state attempts to restrict the use, capabilities, and distribution of encryption technologies are a prime example.[15] From the state's perspective, the spread of this technology would effectively blind its intelligence services and allow criminals to operate with impunity. Ultimately, encryption technologies became widely available, yet chaos didn't ensue. Instead we got e-commerce and the proliferation of encryption in the myriad digital technologies we use today.

Conclusion

Clearly, we aren't currently in a position to balance the individual's need for privacy with the law enforcement and intelligence needs of a wide range of states globally, while simultaneously using technology to its full societal and economic potential. A collision is forming between the constraints of the physical world in which states operate, and an unchaining of technology in the virtual world enhanced by cloud computing. This is occurring as individuals' daily lives are becoming ever more integrated into the virtual world. In response, states have sought to transpose, sometimes opportunistically, their control on this virtual realm without fully appreciating the repercussions of their actions, or the potential implications when other states follow suit. As these states grapple for

control, technology has found itself in the crossfire, as have the individuals and private-sector entities that rely upon it.

It's in the interest of the individual and the private sector to ensure that states cease using technology in a manner that unilaterally imposes their needs on a global environment. Instead, they need to be guided back toward the use of political and legal approaches, where collaboration with other states leads to the establishment of international norms. This will likely be a slow process, but technology isn't a replacement for political and legal mechanisms. If states insist on taking the same approaches they have in the recent past, progress will soon falter, and we'll continue to find ourselves in similar, or perhaps worse, situations than today, with distrust and animosity surrounding technology.

The mutual interest between the individual and the private sector comes not only from a shared reliance on technology, but also from a deeper symbiotic relationship between the parties, particularly in relation to privacy. Although the private sector too often ignores this relationship, it must be mindful of its responsibility to the needs of the individual. Minor shifts in sentiment can have significant consequences for businesses and, as we've seen, the actions of states can dramatically influence sentiment.

As the influence of the individual on government has waned over time, the private sector's influence has grown. Some might point out that this is inherently undemocratic. There's merit in this view, but it misses the point that issues surrounding privacy and the state, particularly given the rise of cloud computing, are global in nature. Even states that claim to be full-fledged democracies operate some aspects of policy and law in secrecy. The nature of technology means that the more the state integrates its apparatus into the technologies we rely on, the more difficult it will be to remove. To make progress, we'll need to address this as soon as possible. The private sector must appreciate that privacy isn't just a problem for the individual. As we take cloud computing forward and embrace all of its advantages, the private sector needs to recognize its pivotal role in building an acceptable future that balances the needs of society and the individual.

References

1. J. McKendrick, "Cloud and Big Data, Together: A Huge Springboard to Innovation," Forbes, 17 Mar. 2013; www.forbes.com/sites/joemckendrick/2013/03/17/cloud-and-big-data-together-a-huge-springboard-to-innovation.

2. C. Macropoulos and K.M. Martin, "The Militarization of Cyberspace: Implications for the Private Sector," ISSA J., vol. 12, no. 11, 2014, pp. 32–36.

3. United Nations High Commissioner for Human Rights, Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37), 2014; www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Pages/Documentation.aspx.

4. B. Schneier, "Surveillance as a Business Model," blog, 25 Nov. 2013; www.schneier.com/blog/archives/2013/11/surveillance_as_1.html.

5. D. Geer, "Data-Centric Security: A Must in Today's Threat Landscape," Keynote at Digital Guardian Customer Advisory Group, 2014.

6. A. Preuschat and A. Troianovski, "German Intelligence Admits to Frankfurt E-Mail Tap," blog, 9 Oct. 2013; http://blogs.wsj.com/digits/2013/10/09/german-intelligence-admits-to-frankfurt-e-mail-tap.

7. T. Samson, “Germany Joins in Voicing Distrust of U.S.-Based Cloud Services,” InfoWorld, 3 July 2013; www.infoworld.com/article/2611522/data-security/germany-joins-in-voicing-distrust-of-u-s--based-cloud-services.html.

8. I.S. Rubinstein, G.T. Nojeim, and R.D. Lee, Systematic Government Access to Personal Data: A Comparative Analysis, tech. report, 2013; https://cdt.org/files/2014/11/government-access-to-data-comparative-analysis.pdf.

9. D. Kravets, “U.S. Telcos Have Never Challenged NSA Demands for Your Metadata,” Wired, 17 Sept. 2013; www.wired.com/2013/09/telcos-metada-orders.

10. B. Schneier, “Metadata = Surveillance,” blog, 13 Mar. 2014; www.schneier.com/blog/archives/2014/03/metadata_survei.html.

11. D. Wilson and G. Ateniese, “To Share or Not to Share in Client-Side Encrypted Clouds,” 2014; http://arxiv.org/abs/1404.2697v2.

12. NSA Research Directorate, “Securing the Cloud with Homomorphic Encryption,” The Next Wave, vol. 20, no. 3, 2014; www.nsa.gov/research/tnw/tnw203/articles/pdfs/tnw203_article5.pdf.

13. M. Green, “Cryptographic Obfuscation and ‘Unhackable’ Software,” blog, 20 Feb. 2014; http://blog.cryptographyengineering.com/2014/02/cryptographic-obfuscation-and.html.

14. D. Kravets, “UK Spy Chief, Parroting His US Counterparts, Calls for Crypto Backdoors,” Ars Technica, 4 Nov. 2014; http://arstechnica.com/tech-policy/2014/11/uk-spy-chief-parroting-his-us-counterparts-calls-for-crypto-backdoors.

15. American Civil Liberties Union, Big Brother in the Wires: Wiretapping in the Digital Age, American Civil Liberties Union special report, Mar. 1998; https://web.archive.org/web/20041019081750/http://archive.aclu.org/issues/cyber/wiretap_brother.html.