New America Foundation

Lessons from the Summer of Snowden

The Hard Road Back to Trust

October 2013

By

Georg Mascolo

and

Ben Scott

Introduction

The revelations of Edward Snowden have opened a breach of trust between the United States and Europe that will not be closed easily or quickly. This rift reflects the results of a decade of actions by US secret services (with the cooperation of many other governments) to conduct mass surveillance (mostly) for counter-terrorism. The technologies they use have extraordinary, supra-national reach. And the invasion of privacy required by these programs goes beyond what many citizens will comfortably tolerate now that it is out of the shadows and under the heat lamp of media attention. Trust in the integrity of online communications - and especially those delivered by American companies - is broken.

So now what? Both sides of the Atlantic have deep interests - political and economic - in repairing the damage. Yet the debate over solutions is polarized. It is divided between critics demanding immediate termination of any kind of mass surveillance and the defenders of the status quo. Neither of these choices appear to offer realistic answers.

To find realistic answers, we must begin by acknowledging a hard truth that Edward Snowden has demonstrated to Americans and Europeans like: there is no political or economic power in the world that can guarantee privacy and security in digital communications. The information systems of modern society are fundamentally insecure. We can never be completely certain that no one is watching.

The global architecture of the Internet that has beautifully facilitated access to knowledge, economic growth, and freedom of expression has at the same time weakened the liberty of individual privacy. This is a fundamental - perhaps existential - problem for modern information systems. The right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights. Focused on the sanctity of privacy in the home, it extends to correspondence and communication. And in the information age - when our whole lives are gradually migrating online - the digital application of privacy rights becomes very broad.

The network of networks that supports the Internet spans the globe and optimizes the storage and processing of Internet data for cost and efficiency -- not privacy. All of that data passes through a server and a switch somewhere -- often outside the country. In short, the globalization of communications has taken control over the right to privacy outside the power of the nation state to protect. The most powerful nation states have turned this vulnerability into a strength to combat new threats to national security, authorizing spy agencies to use surveillance technologies to build a massive communications dragnet.

This was an open secret long before Edward Snowden made it public. Very few people knew exactly how it was done. But after 9/11, most close observers of either technology markets or intelligence agencies understood the high probability that all forms of electronic surveillance that are possible, legal and affordable are likely happening. This is not exclusively an American business, but rather the practice of many nations. The muted and often contradictory reactions of many governments to the exposure of National Security Agency (NSA) programs indicates the scope of probable cooperation between allied intelligence services.

Nonetheless, the shift from an open secret to a published secret is a game changer. It is a game changer because it exposes the gap between what

governments will tolerate from one another under cover of darkness and what publics will tolerate from other governments in the light of day. Those governments that were complicit with the NSA are scrambling to re-align themselves with their voters. Meanwhile, Washington is building up its arsenal of justification. Major commercial actors on both continents are preparing offensive and defensive strategies to battle in the market for a competitive advantage drawn from Snowden's revelations. And citizens are organizing to demand sweeping change. Left unresolved, we risk that the logic of intelligence agencies -- which operate with a maxim of "trust no one" -- will begin to contaminate other areas of political, governmental and social cooperation among nations.

To untangle this knotty dilemma, we have to start with a comprehensive review of how we got where we are and the nature of the challenges we face. We must assess a series of novel policy problems inherent to the relationship between law and technology in modern signals intelligence. Few have taken a comprehensive view of the top-down and bottom-up political and economic forces that must be engaged in any workable solution. And almost no one has identified a path forward towards an international standard that can realign both governments and publics around a trusted regime that balances liberty and security in the digital world. With humility before the scope of the task, we seek to address all of these issues in turn.

Background

Surveillance as a tool of law enforcement and intelligence gathering is, of course, nothing new. And within appropriate limits, it is a powerful tool to detect, expose, and thwart criminals and threats to national security. According to intelligence sources, over 80 percent of information about terrorist threats comes from signals intelligence. Threats to public safety and national security are very real, and the interception of communications is a necessary and indispensable tool for law enforcement. Though many Europeans are very critical of NSA practices, the EU is dependent on American intelligence capabilities in much the same way it relies on American military power more generally to pursue common international security objectives.

Over the years, the nature of surveillance has changed dramatically. The original form required an evidence-based court order to intercept the communications of an individual suspect. Surveillance was authorized if it was necessary to apprehend the suspect and the infringement on liberty was proportionate to the nature of the crime or intelligence purpose. No other individuals were implicated in this infringement on privacy, except those who communicated with the suspect. Today, this logic is reversed. We intercept huge quantities of communications from millions of people and then search the resulting database for information related to suspects. Few would dispute that there are legitimate purposes for some kinds of surveillance. But, the infringement on the liberty of the innocent in the practice of mass surveillance has not been weighed against these legitimate purposes in the court of public opinion. There has been very little public debate in any country over whether this is justified or acceptable. When these issues do make headlines - e.g. "warrantless wiretapping" and the Echelon scandal - public reactions have been negative.

Two factors influenced this logical shift in intelligence practices: new technology and the attacks of September 11, 2001. The terrorist attacks dramatically expanded the threat profile for national security - not just for the US, but for all allied nations focused on Al Qaeda. The targets were no longer conventional military assets, but thousands of individuals scattered around the globe plotting lethal attacks on civilians. To counter this threat, intelligence agencies developed and deployed new technologies to intercept electronic communication on an unprecedented scale. And simultaneously, they operationalized new tools to store, sort, and analyze these mountains of information. On a mission to find individuals like the unassuming young migrants to Germany who would later sit in the cockpits of hijacked airplanes, the needed breadth and depth of intelligence activities were almost limitless.

This was a paradigm shift. The old logic of "necessary and proportionate" was stretched to meet the new demands. To find shadowy terrorists in lawless corners of the world, the necessity of using all potential tools of surveillance was clear. And the scale of the atrocities on 9/11 left few in doubt that whatever infringements on privacy were needed to capture perpetrators were proportionate to the crime. In other words, after 9/11, there was a dramatic change to the discussion over how to define necessary and proportionate. Nearly every increase in technological capability to collect, process, and operationalize intercepted communications was welcome. And though restrictions were placed on these capabilities - it was not a lawless free-for-all - the scope of operations expanded steadily. This increase in the capabilities of American intelligence over the last decade was not the work of power-hungry spies. It was the work of a national security system maximizing its effectiveness under the law in a post-9/11 world. What distinguishes American intelligence work from that of other nations is not this logic, but rather resources, threat perception, and a firm belief in superior technology. This evolution must be understood in that context.

These programs moved well beyond the interception of mass quantities of "upstream" data on telephone and Internet networks. They solicited and compelled the partnership of Internet companies that store and process large quantities of information from the commercial market. The now notorious "Prism" program is one example, although its reputation far exceeds its scope of impact compared to other collection methods. More insidious, the NSA reportedly worked to compromise the most common cryptographic standards. Firms that promised privacy through encryption quietly handed the keys to the NSA under legal compulsion (or voluntarily) or had them stolen. According to the Snowden documents, the implementations of encryption in common services like HTTPS, Voice-over-IP, and 4G wireless networks have all been secretly unwound. Only the specially modified devices of high ranking government officials - such as the German Chancellor - can hope to have trustworthy security. For everyone else in the mass market, it is mostly a fiction.

And let us be clear that this was not just the United States. Many countries developed these capabilities to some extent. Each implemented policies with a focus on reducing risks for its own citizens. Looking back now, we can see that the secret programs to increase surveillance to improve national security almost certainly achieved that outcome. But these practices also opened vulnerabilities. The backdoors built into secure systems can be used by anyone with the

skill to find them. And the pursuit of criminals in big data inevitably sweeps innocents into the mix and jeopardizes public trust in a government that would undermine personal privacy without a word of public debate.

Novel Policy Problems

The NSA is the undisputed champion of the surveillance world. Just as Silicon Valley companies dominate the Internet marketplace, American agencies dominate the business of electronic surveillance. It requires huge resources to fulfill this mission, and only a few countries can afford to maintain and staff the infrastructure. But the same legal and logical principles that guide the NSA programs apply in many other nations on a smaller scale, but with similar methods. Most notably, the Snowden documents make clear that the British Government Communications Headquarters (GCHQ) is not only a close and highly capable partner but a paid subsidiary of the NSA. Much less is known about the practices of other European intelligence services, but several (including the German Bundesnachrichtendienst [BND]) are known to be in close cooperation with the NSA.

Aiming at our goal of identifying the elements of a new international (or at least transatlantic) standard to contain surveillance practices within a new legal framework, we need to compare the laws governing foreign intelligence surveillance between the US and the largest EU powers and assess the novel policy problems of mass surveillance that must be addressed. This dual approach will enable the identification of a baseline of law and policy today as well as the elements of a new standard that would recoup lost trust. And of course, implicitly, we will see the distance between them that must be bridged.

A comprehensive review of national surveillance laws is beyond our presents scope, but we can draw basic conclusions that will suffice for our purposes here. Though it may come as a surprise to many European citizens, the laws used to authorize surveillance programs in EU countries are comparable to those in the US. Foreigners are legitimate targets for surveillance under broadly defined national security purposes. In many cases, this is not limited to counter-terrorism but applies to foreign intelligence information more generally as it relates to public safety. Typically, local citizens are protected by a higher standard of privacy, but they are not exempt from surveillance. Intelligence agencies gain access to the telecommunications networks that physically cross their territory. And the companies that own the upstream networks and data storage/processing facilities are required by law to cooperate. There are no clear minimum standards of operational protection, even inside of Europe. And there is broad cooperation among intelligence services, including the exchange of data. The extent of interaction and the standards of practice for filtering and deleting data prior to exchange remain largely unknown. We may learn more as the remainder of Snowden's documents are released in the news cycles ahead. But for now, we can focus on the novel policy problems that both the US and Europe face with the broad understanding that we are all basically in the same boat.

Locating the Act of Infringement on Liberty

Since 9/11, a quiet shift has occurred in the relationship between surveillance law and technology. This change was driven by the nature of the current generation of surveillance technology. And it fundamentally altered the definition of the act of infringement - the

moment that personal liberty is violated for the sake of common security. Is it the moment a communication is intercepted? Or is it the search and analysis that occur during the processing of the intercepted data and the subsequent actions taken?

The logic of the last generation of wiretapping places the act of infringement at the point of interception. But based on the Snowden documents' depiction of NSA and GCHQ activities, it is clear that we have pushed that back to the act of processing. Mere interception is no longer considered an infringement of rights. This is a critical distinction. If interception was infringement, it would not be legally viable to conduct mass surveillance.

Here is how this works. Let us say an intelligence analyst is searching for communications between two suspected terrorists hiding out in Berlin and Seattle. Under the old standard, he would seek a method to intercept all communications between those individuals by placing a tap on the specific Internet or telephone lines tied to their accounts. Or, he would bring a court order for that specific data to the email or telephone provider. Of course, he would need cooperation from another national law enforcement agency to get both ends of the communication in this manner. Under the new standard, he can attempt to gather ALL of the email and phone calls coming in/out of Berlin (or in/out of Seattle) and store it in a database. He might not even need cooperation from a partner spy agency, depending on what international lines he has tapped on a permanent basis. Or he could also ask the email or telephone provider to give him everything they have that might be related to the suspects in Berlin or Seattle for a period of days or weeks or months. Then, he can go to this database at his leisure and use powerful processing tools to search through all of this data to find what he wants. The analyst's chances of finding the suspects are undoubtedly higher. And he might even find information that he was not looking for, but which is useful in his investigation. But at what cost?

Perhaps 99 percent of the data that he has collected from this torrent of global communications is irrelevant to the investigation. Few would dispute the importance of pursuing the 1 percent - but what about the rights of the 99 percent that get swept up in the process? In order to justify the act of mass surveillance, what the analyst has done as a matter of law and morality is shifted the moment of infringement of liberty from interception to processing. Inevitably, he will have intercepted huge quantities of communications that have nothing to do with the investigation and should not have been captured. To justify this, he has simply pushed back the moral red line of surveillance and declared that the inadvertent collection of your data requires no legal justification as long as he deletes it later. Only when he processes that data and uses it for some law enforcement or intelligence purpose has he infringed on your rights. Is it necessary to make this shift? Is it proportionate to the crime of the suspected terrorists? Who decides? Because these activities are all classified, it has not been subject to much scrutiny.

Minimization Practices

The intelligence agencies address this dilemma through "minimization practices." That is - they delete some of the data that they should not have collected and stored in the first place. For example, these agencies are never meant to use communications data transmitted between their own citizens and should delete it immediately if discovered before it is processed for intelligence purposes. But - if they find something of

intelligence value in this data before they delete it - then they do NOT delete it, whether it was related to the initial target or not. The NSA's minimization standards have now been published. But even those specific standards do not provide certainty about which data is deleted and whether it is all deleted before it is searched if it was legally off limits in the first place. For example, the rules governing raw data collected directly off of the Internet appear to be slightly different than for data compelled in bulk from a company. And we have other documents suggesting that much of it is not deleted before it is searched and sorted to some degree; and in some cases (such as with the Israelis), the raw data is shared with other intelligence agencies before it is minimized. (The NSA disputes the significance of the documents detailing these circumstances, but the government has not offered a counter-narrative with similar levels of detail.)

Long story short - the logic of "minimization" is at least partly contradictory. Intelligence agencies intercept huge quantities of communications data in search of a few targets. They are meant to delete everything they were not supposed to collect in the first place. But before they delete it, if they find anything constituting foreign intelligence value in the data they were not meant to collect, then they go ahead and keep that too. If they only minimize what they did not want anyway - that is not minimization, it is just sorting. It seems likely that they delete a lot of obviously irrelevant or off-limits data before they search it. But we simply do not know exactly because the oversight of these programs is classified.

And here is the real hypothetical mind-bender: the current problem of infringing on everyone's rights in order find the terrorists is a function of the power and the limits of technology. We are collecting everything, storing and searching because it is technically possible and certainly more effective to do so. But currently, it is *not* technically possible to search ALL of the data flowing across the entire Internet in real time and pick out ONLY very specific targets such as email addresses or keywords. That can only be done after it is stored and searchable. But someday, it might be possible to set up a filter that makes it unnecessary to intercept all the data and store it for later processing. In other words, if signals intelligence agents had an even more powerful and intrusive technology than they do today, but it was more precise - they would be able to take the moment of infringement back to the original standard of interception.

The key conclusion here is that there is a certain amount of technological path dependency to any reform effort. Technology has shaped the reason policy-makers and intelligence agency directors have declared that surveillance no longer means merely intercepting data but rather involves the processing of that data. Policy-makers had to make this shift in order to accommodate a more effective technology to achieve their goals. And similarly, the nature of the minimization practices stems from this basic technological requirement to intercept and store all of the data. Since we have to have all the data to find the bad guys, would it not be irresponsible if we did not go ahead and look for other bad guys we can see in the data even if we were not looking for them in the first place? Or is that an unacceptable step onto the slippery slope towards Big Brother government?

Compulsory Private Sector Cooperation

The combination of novel policy problems we must disentangle contains one more key element. This problem involves the role of the private sector. Because so much of the Internet and telephone data in the world is carried, stored and processed by private sector companies, they are now complicit in the practices of mass surveillance. The now-notorious Prism program involves many of the biggest brand names on the Internet. When compelled by law enforcement with a valid court order, they have no lawful choice but to provide the data requested and to disclose nothing about the request. This is a common practice in many nations. But because most of the largest Internet service providers are American companies, the US gains access to foreign data stored by American companies in far greater quantities than would be possible anywhere else.

Naturally, other governments have begun to put pressure on these companies to disclose exactly how (and how much) information about their citizens is being transmitted by American companies to American intelligence agencies. But the policy problem is this: if a European government passed a law that Internet service providers operating in their countries are forbidden to pass data to US law enforcement, they place these companies in a contradiction. They are still American companies and subject to US law. In these circumstances, they cannot be in compliance with the law in both countries. [More recent proposals to place consumer warning labels on data processing that might happen outside the EU are an attempt to circumvent this problem, but likely will lead to the same contradictions between national laws.] The same contradiction applies for any country that would pass laws to govern the companies governed outside their control. In other words, a disagreement about policy between two governments cannot be easily solved by market regulations. But if not that - then what?

Reactionary Forces - Political and Economic

Throughout the summer of Snowden, we have seen a variety of reactions. We can group these into two categories:

1) *political* - government to government demands for policy change as well as public pressure on national governments to stop foreign surveillance;

2) *economic* - proposed regulations to limit exposure to surveillance by privileging domestic firms, restricting foreign-owned firms, as well as changes in consumer behavior in the market.

Political Pressure

Up to now, most governments have shied away from a thorough discussion of the NSA documents in order to avoid revealing their own intelligence activities operating on similar principles. Political oversight of intelligence services are conducted with very limited resources. And so these agencies are the last island of absolute sovereignty for the nation state. If politicians do not seek an international agreement to protect the right to private communications, the agencies certainly will not do so on their own. The price of operating under laws that permit unlimited surveillance of foreign citizens is the vulnerability of your own citizens to the same treatment by others.

Now that the facts of this situation are public, the damage done is enormous. It includes the erosion of trust between allied nations, the concerns of millions of citizens about total surveillance, and increased fears in the marketplace about economic espionage. In short, the scale of the surveillance programs has

shredded the trust in the security and integrity of the Internet itself.

Most of the political responses from governments have criticized Washington and London and called for an end to their surveillance practices. But few have held up their own systems as exemplars to follow. And without a new standard to follow, these efforts are unlikely to bear fruit.

The best of them - and the bar is very low - is the German/American announcement of negotiations to construct a mutual "No Spy Agreement." According to statements from German government officials, the agreement would require the NSA to respect German law and the rights of German citizens in any surveillance activities conducted in Germany. The deal would also prohibit any economic espionage against German companies. Such a pact could serve as a model that could be applied between other states as well.

However, this announcement should be viewed with some skepticism. It was unveiled in the weeks prior to a German election in which the government was well served to deflect this issue. It was negotiated by the intelligence agencies (BND and NSA) and the specifics were not disclosed. Further, it was announced with a declaration that the NSA had not broken any German laws to date. Moreover, there is no evidence that the US has ever conducted industrial espionage against Germany. In short, the "No Spy Agreement" appears to propose an agreement to end problems which it simultaneously declares are not occurring.

Meanwhile, the pressure rises from the bottom. Citizen-led protests against NSA overreach continue. Media coverage has been almost uniformly negative in Europe. The outrage was sufficient to propel the issue into the talking points of all parties contesting the German elections. Senior officials in the EU have also taken up the cause. Neelie Kroes, European Commissioner for Digital Agenda, and Viviane Reding, European Commissioner for Justice, Fundamental Rights and Citizenship, have both been vocal in their demands that Washington atone for its sins or face political consequences. The most common demands from Brussels for policy change in Washington are largely focused on calls for transparency and an accounting of exactly what European data has been collected, by whom, in what ways, and for what purposes. Looming in the background is the possibility that Europe will cancel key agreements over data sharing with the US - such as SWIFT banking data and the "safe harbor" for US commercial data services. And of course, the much-heralded Transatlantic Trade and Investment Partnership negotiations have just begun and mass surveillance is likely to play a turbulent role in those discussions. It appears that the political conflicts over surveillance practices are playing out in economic policy.

Economic Pressure

No law made in Europe can hold American intelligence agencies accountable. The only targets for political backlash that lie within European jurisdiction are American technology companies that have been exposed as cooperating with the NSA.

Two approaches to economic policy-making have emerged in response to Snowden:
1) restricting and regulating the activities of American technology companies in Europe; and
2) creating incentives for technological

sovereignty over data storage and transport on the Internet.

Neither of these digital Maginot lines are likely to stop the NSA from intercepting European communications. But both may get the attention of the US government and focus policymakers on a political solution that would reduce surveillance of European citizens. However, these policies are not without significant risks for European political and economic interests.

The first idea has multiple potential applications. The simplest proposal is for Brussels or a number of member states to pass laws that require all foreign companies that provide data storage or processing in European markets to refrain from passing that data to other governments - or at least to provide transparent notification when it happens. Another proposal is to terminate existing agreements that permit American technology companies to do business in Europe despite the fact that they do not specifically comply with EU law. Policies like these would certainly hold Silicon Valley's feet to the fire, though not in a particularly productive way. These companies would all remain subject to US law that requires the cooperation that Europe would prohibit. Assuming that these firms would not abandon their European customers (which would certainly be extremely unpopular), it would put their lawyers in a tough spot but it is not a game-changer for the NSA. Moreover, European intelligence and law enforcement agencies also rely on these companies to provide data and may seek to protect those interests. The potential benefits of restoring trust with such a policy would be undermined by the absence of real results.

The second idea - technology sovereignty - has more teeth. Proposals include new regulations that require that all data that is stored or processed for European consumers be stored and processed inside Europe. Another option would be rules requiring or incentivizing the routing of all domestic voice and data traffic to remain as much as possible on wires located inside the country. The German Interior Minister, Hans-Peter Friedrich, suggested that any German citizen with concerns about American espionage should avoid using Internet services that send data over US networks. Chancellor Angela Merkel also mentioned a Germany-only routing solution in response to questions about NSA spying.

Layered onto these political suggestions are the enthusiastic responses of European Internet and telecommunications companies. In August, Deutsche Telekom and United Internet announced a new offer of "Made in Germany" email using SSL/TLS encryption. Subsequent stories based on Snowden documents revealed that some common SSL implementations have been compromised by the NSA. However, the German system does not appear to be among them, and it retains the confidence of Deutsche Telekom leadership. The company has more recently announced it will begin routing email traffic to and from certain German email systems on paths that avoid international networks and surveillance. The specific design of these services is to circumvent US and UK network access.

Home grown and guaranteed security in data storage, hardware manufacture, cloud computing services and routing are all a part of a new discussion about "technological sovereignty." It is both a political response and a marketing opportunity. If enough customers (especially enterprise clients and government buyers) took their business away from American service providers, it could translate into a significant shift

in revenue in the digital marketplace. For this reason, even if political Europe decides at some point that it is better to set this issue aside to protect their own interests in security policy, it is quite likely that national economic actors will not let it go.

American technology companies are now in a lose-lose situation. Their public image in Europe is badly bruised by the Snowden revelations. And yet they are still compelled to comply with US law, even as they face the possibility of increased regulation in foreign markets. At a recent conference in Silicon Valley, Facebook CEO Mark Zuckerberg expressed what many of his peers may be thinking: "The government blew it." The Washington justification that they only spy on foreigners is no help for global Internet companies. Facebook has joined several other high tech firms in a suit against the government that petitions for the right to release more information about the number and nature of the information requests they get. These companies - long seen as punching bags in European politics - are ironically well positioned as allies for EU political leaders seeking to push for reform in Washington. These companies may not be overly concerned with commercial data privacy – but they have no desire to be seen as the handmaidens of the NSA or any other intelligence service.

They are desperate to restore their credibility in the market before consumer behavior begins to shift to non-American alternatives. They have good reason to worry. A recent study by the Information Technology & Innovation Foundation projects that the US cloud computing industry will lose more than $20 billion in the next three years because of the NSA scandal. That is just one of many industry segments that will feature the same trend. Political and economic leaders across Europe are not only predicting this outcome - they are encouraging it. Nationalism is being wielded as an economic weapon against the perception that globalization of technology markets is responsible for their security problems. Few leaders are currently weighing these concerns against the social and economic benefits this same global network has delivered.

So far, we have not seen major changes in consumer behavior in response to the Snowden revelations and the naming of names among American companies that are cooperating with the NSA. Several factors likely explain this stasis, some of which could change in the future. The least likely to change is the simple reality that many consumers do not care about the NSA, or at least not enough to be even slightly inconvenienced in their online activities. But as people become more educated about the nature of modern surveillance and their options to thwart it, we may see more consumers looking for alternatives. The problem is that even if there were broader consumer knowledge about the need for end-to-end encryption to ensure privacy, there are not any commercially successful, user-friendly solutions to add this level of security onto popular Internet services like email, social networking, and instant message. That could change and probably will as clever entrepreneurs toss a stream of new products into the market branded as NSA-busters.

Consequences

If there is no political solution to set new international standards to govern mass surveillance, we should expect the combination of political and economic reactions to achieve at least some of their stated goals in Europe. These

are powerful political arguments backed by organized public outrage and domestic industry giants that see market opportunity.

A major shift in Europe towards technological sovereignty will have very serious consequences for the global Internet as well as the European digital economy. And though it may result in a higher degree of protection against foreign surveillance in the short term, it is not likely to shut out determined electronic espionage from the US (or others) without a political agreement.

But technological isolation carries significant shortcomings. The most popular idea - requiring local data storage in Europe - would certainly press the pain button for American technology firms. The costs of replicating server infrastructure through the EU would be very high. And European companies might benefit from the initial shake-up. But, short of cutting American companies out of the market altogether, the end result will retain the major vulnerabilities to American law and exposure to data collection.

Meanwhile, these policies could easily trigger similar local data storage requirements in other countries or regions around the world. Brazil has been very vocal about its intentions to move in this direction. If many countries took this path, the result would be a balkanization of the Internet. It would no longer be possible to host a website or Internet service in one location and make it available to a global market. Every national market for every digital company would require its own dedicated budget for infrastructure before product launch. Many companies would choose to limit product offerings to only the most lucrative markets. Ironically, the only companies in the world with the resources to afford these infrastructure costs are the very American firms that Europe seeks to restrict. The pushback against these policies from the European digital companies with market ambitions outside of Europe would be significant and justified. And these are the companies often extolled by Brussels as future growth centers of the European economy.

Policies encouraging local routing of Internet traffic may also have unintended consequences in addition to the benefits of avoiding contact with international exchange points that might be compromised by spy agencies. The architecture of the Internet is not designed for national routing and significant changes to routing patterns would have unknown impact on overall network functionality. Even if the EU blunts this problem by making a regional agreement, such policies will likely encourage similar activity in other nations. But the purposes of national routing do not typically tend towards protecting civil rights, but rather the opposite. The localization of Internet traffic will intensify opportunities for national surveillance, censorship, and the kind of political persecution of online dissidents that the West has fought for years. Furthermore, these kinds of centralized routing practices would introduce vulnerabilities of their own that might be exploited by the intelligence agencies they are designed to thwart.

Of course, none of these consequences are guaranteed. The effects could be less dramatically negative. But in any scenario it is unlikely that economic reactions will change the law and motives for surveillance programs. Given the risks, it would be sensible to make an aggressive attempt at a political solution before falling back on economic and technological nationalism as a response to foreign surveillance.

A Path Forward

We have taken a long path to come to our proposal: a call for a strong but pragmatic international standard for surveillance operations in the Internet age. Our purpose in outlining the full scope of the problem - from origins to initial reactions - is not to convey pessimism, but to lay out the context in which any viable solution must be conceived. Our conclusion is that any effort that might succeed will have to combine political and economic forces that support reform. And sustainable change will require pressure from citizens and consumers as well as leadership from governments and boardrooms.

We believe solutions will begin with the US and Europe - especially between NATO allies. If we can go to war together on the strength of common commitments to liberalism and democracy, we can surely develop a common standard for intelligence operations and hold one another to it. The problem of mass surveillance cannot be solved at the national level. The integrity of secure communications is broken because global information networks are only as private as the least secure link on the paths between us. But that cannot justify the balkanization of the Internet. Walling off the information networks the connect the world is a mistake - both politically and economically. The consequences of a global shift towards technological sovereignty would be severe and still it would likely fail to solve the espionage problem. The current political momentum pushing towards that outcome should motivate us to find an alternative. If we can establish a transatlantic zone of common values, legal standards, and operational practices, we will have a chance of restoring some of the trust that has been lost in the Internet.

Market Response

Before we describe a framework for a possible political solution, it is worth spending some attention on market forces. The political process to build a new international policy for foreign intelligence surveillance will be painfully slow. But the market reactions will not. And what happens in the market will influence the outcomes of the political debate. For that reason, we must look at where this pressure will appear and what form it may take in the short term. Here are a few examples of changes we expect to see or which we believe should be encouraged.

Brussels-San Francisco Alliance: The reaction of companies under pressure for complicity in government surveillance is a push for transparency. Some of the major Silicon Valley giants are publishing as much information about surveillance as the law allows and petitioning for the authority to do more. Ironically, Europe's most valuable allies in the effort to press Washington for policy reforms may be the Silicon Valley companies that are the current focus of their anger. An argument made together by European political leaders and American CEOs about the consequences of failure to reform foreign surveillance practices would be a potent force. Europe could set a standard of transparency in intelligence cooperation for companies operating in the EU and gain eager allies in the private sector.

Security By Design: The starting gun for a new "crypto arms race" was fired by Edward Snowden. His disclosures triggered a frenzy of activity to design new products and services that are NSA-proof. The private sector will play a large role in developing new technologies that seek to provide more security and trust in the Internet marketplace. On the hardware side, this activity

might include new kinds of customized PCs, smartphones, servers, and routers. New cryptographic software tools are also likely to be in high demand, particularly if they can be used to augment already popular services. But we should be mindful that if secure software becomes widespread, the pressure to take backdoors for surveillance into the hardware layer will increase.

Crypto Savvy Consumers: With the right combination of public and private sector leadership, consumer outrage over the NSA could be channeled into increased digital literacy. Most people have no idea how the Internet works despite its integration into their everyday lives. The Snowden story sets off alarm bells for people, but it does not give clear guidance for what to do. Insert here a battalion of wily marketing gurus and public service NGOs, and we may see a boom in consumer demand for strong encryption. Technical literacy does not magically make the average person immune to foreign surveillance, but it does improve the probability of security and privacy on the Internet without waiting for a political solution.

Policy Reforms

Real change will only be achieved with a political settlement. There are no market regulations or new products that can hold governments accountable to the balance between liberty and security. To reach agreement on an international standard for surveillance practices, we will need to see movement in three areas:

1) Increased transparency about national surveillance practices;
2) Negotiated agreement of a new standard for foreign intelligence collection;
3) Specific reforms/oversight in each nation to bring current practices up to the new standard.

The process we propose is straightforward and its logic is pragmatic. We do not suffer from illusions that this could done on a global scale. But there could be agreement on common standards for the interception of communications between nations that share common concern about the privacy of one another's citizens. The way forward is not a magic formula of technical solutions or digital Maginot Lines around national Internets. The only answer is a steady march through difficult politics. We would like to offer novel policy ideas, a clever diplomatic coup, or brilliant concept for a technical fix. But there is nothing like that available. We suggest here a sequence of steps to guide the process. It is simple and straightforward, as it must be to have a chance of success.

First – nations must decide about mass surveillance in a public debate. As nations, we have to answer openly the central question that Snowden forces: should mass surveillance of any kind be permissible under the law of democratic societies to protect common security at the expense of individual privacy? As a practical matter virtually all nations will decide in favor of some forms of mass surveillance with restrictions. Once this Rubicon has been crossed, the tough choices begin as we seek the legal barriers that will establish a new balance between security and liberty that accounts for the power of new technology.

If mass surveillance is legal in certain cases, the heart of the debate is about how to restrict these practices in a credible way without rejecting the secrecy necessary for success. The FISA court, the G-10 Commission, and other such methods in different nations are the current practice. They are not adequate. National leaders must reengage the core question: How should surveillance

practices be constrained by law to certain circumstances and subject to rigorous oversight?

The new rules will have to account for the nature of modern surveillance and justify the infringement on personal liberty in pursuit of common security using the standards of necessity and proportionality. These judgments must be hard and fast, because upon this base democratic societies will distinguish "legitimate" surveillance from the repressive operations of authoritarian governments. Intelligence systems that collect and store data without clear and enforceable limits--such as some of the NSA and GCHQ programs reported in the Snowden documents--cannot be justified. Further, the moment of infringement on privacy rights must be once again fixed to the act of intercepting data, not processing it. Total digital surveillance crosses the same moral line as total visual surveillance. And it follows that we cannot demand intelligence agencies to have perfect information. As societies, we accept a reduction in security in order to preserve individual freedom. This is an age-old dilemma that requires modern recalibration in an open, public process within each nation.

Second – international organizations must begin a process of deliberation. The national debates will inevitably run parallel with an international process that seeks a common standard for all nations that share the ideals of liberty and democracy. The right to privacy is enshrined in international human rights accords, but we must now make them specific and transparent with respect to digital surveillance policy in order to have a chance of regaining the trust of citizens. Many different international organizations will play a role in convening these discussions – some of them inter-governmental and some of them multi-stakeholder. We do not believe these forums are likely to resolve the problem, but they will shed light on it and provide forums for engagement and valuable comparative analysis of the thorniest legal and technical issues.

The elements of the new standard will have to address each of the novel policy problems we have discussed here. This will not be easy even inside of continental Europe. Many of the European intelligence agencies have similar practices to the NSA (albeit at a lesser scale) and operate on similar legal frameworks. Setting a new standard will mean acknowledging the status quo, measuring the distance to the new standard, and making the necessary changes to cross that gap. International organizations will provide a platform to deliberate the balance of rights and obligations of governments, companies, and citizens of all countries participating in the process.

Third - Europe will go first. The goal of this work should be a transatlantic agreement. But the process will likely begin within the EU where the political will to make changes is higher. As EU Commissioner Neelie Kroes put it in a recent interview with *Der Spiegel*: "The Snowden Affair has shown us all that we must finally wake up." But she also rightly pointed out that the EU can hardly lecture Washington on espionage when its own members states are spying on each other. Despite broad-based public demand for change and the privacy protections set forth in the European Convention on Human Rights (ECHR), there is no clear minimum standard of operational privacy extended between European states. How can Europe even dream about a common politics if it is not united around protecting basic rights of citizens? The British are perhaps the outliers in the scope of their

intra-EU surveillance, but they are hardly alone. For example, when the German BND forwards data to the NSA, they may filter out Germans and protect the constitutional rights of their own citizens, but that does not hold for other Europeans.

A European standard begins by extending the same protections to all European citizens that are provided to the citizens of each nation. For the UK, and maybe France, the unification of the EU around a common policy will be a hard sell. But it will be a necessary starting point. This will mean very strict limits on surveillance. How strict? We suggest these circumstances should be carefully circumscribed around targeted investigations into national security issues such as terrorism, WMDs, or organized crime. Political and economic espionage would be prohibited. This standard could be pegged to the privacy protections in Article 8 of the ECHR, but to date, there are no explicit stipulations for what that would mean in practice. It may well be that European intelligence agencies are already in violation of the law measured against this standard. The court has not ruled on the question. And even if it did, it is not clear that governments would comply without a political negotiation. To set this framework, the EU could clarify that the national security exception to Article 8 does not permit unrestricted bulk collection.

The EU process should be set in motion by agreement among European heads of state. The negotiations should be conducted by a working group including representatives from intelligence agencies, data protection authorities, foreign ministries, parliamentary oversight committees, and the European Commission. Engagement with civil society leaders as well as industry players in this process will be essential to ensuring buy-in and trust at its conclusion.

Fourth – Europe should present a unified policy to Washington. If Europe can set standards among its member states that represent real changes, it will be well positioned to take a leadership role at the international level. European leaders can argue the case that if the same restrictions and protections from foreign surveillance can be shared among all EU citizens, they can be shared with the US and other traditional allies. The EU will likely enjoy the backing of other states with strong views on surveillance such as Brazil. EU engagement with Washington will inevitably play out in a parallel context with other critical transatlantic priorities such as the Transatlantic Trade and Investment Partnership, NATO security policies, and international counter-terrorism measures. They may be formally separated, but they will be politically linked by a common need for trust and accountability.

If the US agrees to a new standard, it will then carry the weight of both the political and economic support of the West. From there, it will become an attractive club for other countries to join, because it will carry both political and economic advantages for digital products and services. We do no underestimate the level of difficulty in achieving this outcome – but we see no other path more likely to accomplish the goal.

One important point of critical sensitivity between the EU and the US is the firm prohibition on economic espionage. Here we do not mean industrial espionage – spying with the purpose of handing intelligence to domestic companies for commercial advantage, such as the Chinese have long done. Little evidence exists to suggest industrial espionage is an issue between

the US and Europe. As of today, there is no proven case even among Snowden's documents. Furthermore, US intelligence leaders have repeatedly declared that this would be illegal under American law. However, that doesn't mean that there is no economic espionage designed to glean information about market activity that informs political decision-making. For example, former CIA director James Woolsey publicly acknowledged over a decade ago that US intelligence spies on European businesses for the purpose of uncovering bribes paid to other governments. As he wrote, rather sarcastically in the Wall Street Journal: "Yes, my continental European friends, we have spied on you." Part of the deal on surveillance must be an end to this type of surveillance as well as clear policy answers to the reasons Woolsey felt justified in doing it.

Fifth – new surveillance standards must include rigorous policies of oversight and enforcement. This is perhaps the greatest challenge because it requires trust. No state will allow an international organization to control oversight of intelligence practices. And therefore each nation must have transparent and effective enforcement mechanisms in place. We propose a mix of oversight between judicial and legislative instruments in coordination with the government's own management of intelligence agencies. In the US, this would require strengthening Congressional oversight and the FISA court review process. In Germany, it would require establishing judicial oversight and broadening the capabilities of the G-10 Commission.

Elements of the New Standard

We cannot predict the results of these negotiations – either at the national or international level. But we can conclude by identifying key ingredients and a possible framework for agreement. Through the conduct of this process, governments and their publics must take up the central moral, legal and technical questions that will inform the boundaries for surveillance practices. Given the complexity of some of these problems, we should begin with concrete, simple steps.

The lowest hurdle may be an agreement to halt economic espionage and political espionage conducted against allied embassies. The disclosures about NSA targeting EU delegations strike Europeans as the behavior of an enemy, not an ally. If bugging an Embassy is permissible, we must assume that all communications among national political leaders are in bounds, regardless of their bearing on national security interests. The political cost of these disclosures to mutual trust far exceeds any benefit of continuing the practice. It raises the question of whether the NSA conducted these risky operations with the full knowledge of political leaders in the White House. President Obama pointed to the need for review and reform in his comments at a press conference at the G-20 in St. Petersburg.

> "And what I've said is that because technology is changing so rapidly, because these capabilities are growing, it is important for us to step back and review what it is that we're doing, because just because we can get information doesn't necessarily always mean that we should. There may be costs and benefits to doing certain things, and we've got to weigh those."

An appealing recommendation for how to begin this process of introspection and negotiation of the larger issues of restrictions and control comes

from former BND chief Hansjörg Geiger. In the wake of the Snowden disclosures, he called for an "Intelligence Kodex" - a new set of rules for intelligence practices that would be adopted by NATO countries and inside the EU as a starting point. Geiger's Kodex would prohibit political and economic espionage and limit surveillance to urgent matters of national security, such as counter-terrorism and WMDs. Consider the Geiger Kodex in combination with a legal argument from German judge and G-10 Commission member, Dr. Berthold Huber. Responding to the Snowden Affair and the apparent absence of privacy standards that apply to foreign citizens, Huber argued in a law journal that German law (perhaps unique among Western nations) contains constitutional privacy protections that extend not only to German citizens, but to anyone. He points to specific sections of Germany's basic protection of privacy rights that do not distinguish between Germans and non-Germans. Though it appears the German government has not interpreted the law in this way, if it chose to do so, it would be a step towards establishing a new standard of privacy against which only limited exceptions would be reasonable.

The combination of what Geiger and Huber suggest is not new. In fact, it was the framework for a solution to the last major transatlantic dispute over surveillance - a program known as Echelon. At the end of the second Clinton administration, the European Parliament completed a report accusing the NSA and its partner intelligence agencies of conducting global surveillance of telecommunications. The final report of the European Parliament on the Echelon investigation from July 11, 2001 offers a similar proposal to what we describe here. The basic idea would require all parties to make rules respecting privacy and security of foreign citizens at the same standards they require for their own citizens. The report concludes with a set of strong recommendations that could easily be mistaken for a post-Snowden framework, including:

> "The Member States are called upon to aspire to a common level of protection against intelligence operations and, to that end, to draw up a code of conduct based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services. A similar code of conduct should be negotiated with the USA."

This foundational proposal was swept aside by the disaster of 9/11 and the subsequent decade of the war on terror. But just as Mr. Obama speaks about ending the war on terror, he must revisit the idea of a transatlantic pact on foreign surveillance that resets the balance between liberty and security. The process will require a degree of transparency that will not come easily to the shadow world of intelligence agencies. But without this level of clarity, it will be nearly impossible to restore any degree of trust back into the digital communications marketplace. The threshold for trust between nations is the expectation that the citizens of allied nations will be given the same rights as we give our own citizens. Such a move would mark a decisive change.

About the Authors

Georg Mascolo was a Public Policy Scholar with the Wilson Center's Global Europe Program and is now a visiting scholar at the Weatherhead Center for International Affairs at Harvard University. He is a journalist and former Editor-In-Chief of *Der Spiegel* and has written about surveillance since 1990.

Ben Scott is Senior Advisor to the Open Technology Institute at the New America Foundation and directs the European Digital Agenda program at the Stiftung Neue Verantwortung in Berlin. Previously, he served as an advisor on technology issues at the US Department of State.

OPEN TECHNOLOGY INSTITUTE

Wilson Center

Main Office
1899 L Street, NW
Suite 400
Washington, DC 20036
Phone 202 986 2700
Fax 202 986 3696

New America NYC
199 Lafayette St.
Suite 3B
New York, NY 10012

New America Foundation

WWW.NEWAMERICA.NET