NOWHERE TO GO?
Surveillance, Privacy Rules and Trade Talks

Roderick Abbott (with Hosuk Lee-Makiyama)
Roderick Abbott (roderick.abbott@ecipe.org) is a Senior Adviser, Member of the Steering Committee and Advisory Board at the European Centre for International Political Economy (ECIPE), former Deputy Director General at DG Trade, European Commission and at the World Trade Organization

INTRODUCTION
In early 2013, Edward Snowden, the former National Security Agency (NSA) contractor, contacted several people who were civil liberties activists and former journalists, including Glenn Greenwald, a former Guardian journalist; Laura Poitras, a filmmaker; and Barton Gellman, a former journalist with the Washington Post. These contacts led to face-to-face meetings in Hong Kong towards the end of May 2013 and the first revelations about American surveillance systems were published in early June.¹

Since then, the Snowden story continues to roll along and fascinates the media, the intelligence and political communities, and the public at large. Perhaps the least important part of it is the fact that Snowden has become a refugee without a passport, currently granted asylum in Russia, and in short of other options. The United States has asked Hong Kong, Russia and other countries to return him to US jurisdiction, and officially considers him a felon who has stolen secret government data, and a criminal who violated his official secrets oath. There is a lively debate in Washington whether he is a ‘whistle blower’ or a traitor, a civil liberties hero or a feckless burglar who broke the law.²

This policy brief will analyse different threads that run through the story, as it has affected millions of global citizens and many areas of public policy – including

SUMMARY
This policy brief outlines the chronology of the developments since Edward Snowden leaked the documents on large-scale electronic surveillance, including PRISM and Tempora programmes, the policy implications and the public’s response. It concludes that the nature of the debate has shifted from a legal and constitutional issue about US surveillance, to a global concern. The revelations have led to divergent attitudes towards surveillance operations, with Britain and other Anglophone countries on one side, and others in Europe and Brazil and in Asia judging intelligence activity more critically (but at times disingenuously). There is also a growing opposition from telecom companies and Internet providers in the US to being forced to pass on the personal data collected during their commercial operations to the government.

At this stage, the gulf between security needs and the privacy rights of individuals, both Americans and others, is as wide as ever. However, European attempts to promote data privacy rules as a safeguard against electronic surveillance proved to be unsuccessful, as the rules were not designed for that purpose and comes at disproportionately high costs. So were attempts to leverage on TTIP negotiations, especially as Europe is the demandeur of that FTA – not the US. Data privacy rules are also regulatory barriers in the eyes of trade negotiators, proven by the EU’s own offensive stance in its prior FTAs.
intelligence co-operation, security and global trade – as the impact of his revelations has spread far and wide beyond the United States.

DOMESTIC SURVEILLANCE BY PROXY?

The US laws prohibit ‘eavesdropping’ of the communications of its own citizens – whether by voice (telephone) or by electronic means, including the Internet or social media. However, it has become clear first that ‘incidental’ monitoring of American residents did occur as agencies listened to their calls and messages to foreign residents, and later that indirect data collection of American messages had taken place through programmes run by the British intelligence agency, and shared with the NSA.

As an exception to the basic rule, monitoring is permitted when a special warrant is issued. However in the period following 9/11 and the passage of the Patriot Act, ‘warrantless’ interceptions clearly occurred. In addition the Foreign Intelligence Surveillance Act (FISA) mandated the creation of a new court, Foreign Intelligence Surveillance Court (FISC) – the Supreme Court responsible for security issues – which met and took decisions in secret, issued frequent orders to network suppliers such as Verizon, Apple, Google and Yahoo, and Facebook, requiring them to make data available.

The early revelations disclosed surveillance programs monitoring all telephone and Internet communications of American residents, both calls and messages to each other and to those living abroad. We learned about the PRISM and Tempora programmes, among many others, and we learned about the USA Patriot Act of 2001 (adopted in a rush after the 9/11 attacks). Gradually we got to know about the powers conferred by the FISA legislation, and the existence of the largely secret court of FISC was revealed and its powers analysed.

It was at first denied that there was any surveillance of US citizens, but such denials were not sustainable, neither from Obama, nor from intelligence figures in the Congress. The Director of National Intelligence, James Clapper had said “the NSA does not collect data on millions of Americans”; and the President was quoted: “Nobody is listening to your telephone calls”. It rapidly became clear that Americans were in fact being swept up in the tapping of foreigners, and that GCHQ, the British signals intelligence agency, was monitoring American messages and sharing the results with the NSA.


The NSA is responsible for foreign intelligence, i.e. monitoring terrorist activities and containing risks of terrorist attacks. The role has become vastly more important after the 9/11 attacks in New York, and the reach of its surveillance activities has increased accordingly. The public reactions appeared within just a few days after Snowden’s revelations – many arguing that the NSA’s use of section 215 of the Patriot Act went beyond the letter of the law (despite its ambiguities), or the actual intentions of the US Congress when the act was passed in 2011 immediately following 9/11. Furthermore, claims were made that the use of section 1881a of the FISA Amendments Act, 2008 could be unconstitutional.

This forceful early attack on the programme may well indicate that a high level of dissatisfaction with the decisions of the FISC had been building up for some time. The initial response of the intelligence community (and its defenders – the chairs of Intelligence Committees, in Congress) made counterclaims that the programmes were necessary for national security, and the facts were admitted as little as possible. Those defending the intelligence community from the President down were accused of misleading Congress in their efforts to justify the policy as necessary to keep Americans safe.

It took some time before there was any admission of the scale of data collection – the “bulk hoovering” of millions of messages on a daily basis – a lateness that may have further undermined the public’s confidence: a Pew Centre poll (quoted in the Economist) shows that the 53% disapprove of NSA surveillance, while 40% approve, “although when there is a Democrat in the White House, Democrats are much keener to support what America’s spies are doing […] and vice versa”.


Moreover, journalists were quick to investigate the workings of the FISC, and its powers to compel Internet providers and phone companies to provide a mass of data. These powers had been considerably widened after the 9/11 attacks and the range of targets under surveillance had also been significantly increased, and the Court appeared to be issuing or approving court orders on a wholesale basis.

During July there was gradually a shift in attitudes in the Congress, leading to the drafting of bills to rein in the surveillance programme and rising pressure on President Obama for a general review of the situation and for changes in the system. While some spokesmen continued to defend the programme in its entirety (Mike Rogers, chair of the House Intelligence committee even accused Snowden of having been a Russian spy), publications traditionally close to the Democratic party published articles with titles like “The NSA; They know more than you think”. This reinforced the shift in public perceptions. On January 15th, new reports emerged about the technical ability of the NSA to monitor computers even if they were not linked to the Internet. In response, the President Obama had set up an advisory group of former NSA officials to make recommendations on changes, but some may argue that the need to address the issue was slow in coming.

If the public opinion at home appears divided, so are also the courts: a year after Snowden’s meeting with the journalists, the jury is literally still out on the legality of the NSA’s practices. One US federal judge has ruled that NSA surveillance is “significantly likely” to be unconstitutional, while another disagreed and has found them to be within the law. The question is apparently not new: details have also emerged of the 1971 burglary of an FBI office detailing the illegal surveillance activities directed at US citizens, civil rights activists and protest groups, which illustrated a long standing state of confusion about the legality of the surveillance programmes.

SURVEILLANCE ON EUROPE, ENEMIES, ALLIES, AND TRADING PARTNERS (OR ALL ABOVE)

The first revelations were rapidly escalated to uncover the extent of European surveillance on American and European citizens, including the Tempora programme, managed by GCHQ in the UK in conjunction with the NSA. Later published accounts revealed that American and British intelligence agencies had been monitoring the conversations of world leaders attending a G20 Summit in London in April 2009, that EU diplomatic premises in New York and Washington had been bugged, and that private communications of ‘friendly’ leaders from ‘allied’ countries – Der Spiegel reported that Chancellor Merkel’s personal phone had been tapped; Communications of President Dilma Rousseff of Brazil and former Prime Minister Ehud Olmert of Israel had also been regularly intercepted and monitored. In Europe, politicians asked pointed questions about who were the friends or foes, or perhaps which leaders were actually worthy of the spying effort.

At an early date the media began to report on the trade policy implications of the surveillance situation. Initially this was in the context of reports that Ecuador might offer asylum to Snowden (as they had done for Julian Assange), and the US may then threaten to withdraw trade benefits by revoking Ecuador’s GSP duty-free market access. More importantly, the reports risked derailing the first round of negotiations for the EU-US trade agreement, the Transatlantic Trade and Investment Partnership (TTIP). Reports from around capitals culminated in an NYT Editorial entitled “Listening in on Europe isn’t a good strategy [for the USA]”.

 Presidents Obama, Van Rompuy and Barroso launched the TTIP negotiations in March 2013, with much political muscle and media fanfare. France, supported by non-trade EU officials (such as the European Parliament President Martin Schulz and the Justice Commissioner Viviane Reding), urged a delay while explanations were sought; Germany and other remaining Commissioners wanted to move forward as planned. Trade analysts also warned against leveraging these negotiations against the NSA, almost immediately after Snowden’s first revelations. Once a compromise was brokered, trade talks could begin as scheduled with separate talks about surveillance in parallel.

In a later twist the German government warned the UK not to use its diplomatic facilities for surveillance
purposes; articles appeared which highlighted the British contribution (through GCHQ) and suggested that they had as much, if not, more data collected as the NSA. The NYT reported in December that ‘in monitoring more than 1000 targets in upwards of 60 countries between 2008 and 2011 the US and British agencies’. Other reports said that Australian embassies had monitored calls and Internet messages in the Asian region. Subsequently articles appeared reporting on the long history of swapping of intelligence among European countries, which suggested that governments had known about such monitoring (but perhaps had not grasped the new scale of global data capture) and were largely complicit or engaging in hypocritical protests. The existence of the “Five Eyes” partners – the US, the UK, Canada, Australia and New Zealand – that cooperated in collecting intelligence and in sharing the results was widely known. In effect, Europe was divided into three different circles, depending on their level of intelligence co-operation with the US, with practically little unity or common interests between the EU member states.

IMPLICATIONS ON THE GLOBAL ECONOMY

The EU was in midst of a legislative process for a new data privacy regulation, the General Data Privacy Regulation (GDPR), to replace the prior directive from 1995 that predated the Internet, and was asymmetrically enforced in different Member States. Given the origins of the EU as a customs union and a Single Market, EU privacy rules have primarily focused on the free movement of data (which follows the freedom of establishment) rather than the citizens’ right to privacy. The view of privacy as a “fundamental right” was not established until the Charter of Fundamental Rights in 2001.

The proponents of GDPR often stress the change in the EU charters, and the need for an EU-wide harmonisation. In contrast, the opponents point to the fact that the GDPR only applies between private parties (i.e. businesses and consumers), while EU governments and agencies are explicitly exempt, or likely to be so. Furthermore, the protectionist features in GDPR restricts foreign telecom operators, Internet companies, and data processors to enter the Single Market – some impact assessments show that that GDPR is likely to hamper European GDP growth by at least -0.3%. The data privacy concerns and the Snowden affair have indeed created an uneasiness towards ‘big data’ and the digital economy dominated by US-invested firms. Commissioner Reding (with some support from Germany) urged that the ratification process of the GDPR should be speeded up, and that the ‘Safe Harbour’ framework (a self-certification process allowing US firms to operate in the EU) should be reviewed, improved or revoked. In the context of TTIP, market access for Internet services and privacy rules are politically sensitive for Europe. However, the new defensive stance on its privacy rules in trade talks is a reversal from previous positions of the EU, who had negotiated free movement of data in its FTAs since its 2011 agreement with the Republic of Korea.

Other countries have also forcefully responded to the revelations. Brazil has threatened to stop all Brazilian data being transferred out of the country (and offering domestic email services via the national postal office). Overall, the US business estimates that US cloud computing industry stands to lose up to $35 billion from loss of consumer confidence. As a result, companies like Microsoft have offered to its users the option to have their data stored outside the United States. Further signs that data providers were not happy with the position started to emerge in August, with stories that firms closed down their services rather than provide data and further stories of companies and individuals that challenged the NSA’s letters or orders. This illustrates the impact of Snowden’s revelations – but also the participation, or even complicity, of the commercial actors. Companies are obliged or coerced to provide personal data to the intelligence agencies of one jurisdiction, while obliged to protect the same data in another. NSA and GCHQ had also been able to access company data directly by tapping in to the fibre-optic cables that carried their traffic, and this led to embarrassment of the companies and to fears that the integrity of the ‘open’ Internet would be compromised. However, the story does not seem to come an end – later reports fuelled suspicions that NSA activity could be re-directed towards industrial espionage. Also, the NSA seems to have also cracked secure encryption tools, adding to the growing discomfort.
CONCLUSION

Six months after the first revelations emerged, it is still difficult to know where (or if) this story will end. There have been further new developments in recent weeks, new secret technology used by the NSA to access computers and a Presidential review. Anything may come next. Obama received a report from his advisory panel, with recommendations for changes to the surveillance programs; and on January 20th he made a major speech promising that there would be changes in the system, but leaving many details of the new policy to be worked out by intelligence agencies and the Congress. The full and complete picture may never be known, but already a few preliminary conclusions can be drawn:

• First, the nature of the debate has shifted from a legal and constitutional issue about US surveillance, of primary concern to Americans, to a problem which is in effect now a global concern. Reactions to President Obama’s proposals are very different according to the listeners.

• Second, and linked to that, there is growing emphasis on the role played by GCHQ in Britain, which has been largely running a joint operation with the NSA. This leads to divergent attitudes towards surveillance operations, with Britain and other Anglophone countries on one side and others in Europe and Brazil and in Asia, judging intelligence activity more critically (but at times disingenuously).

• Third, there is growing opposition from telecom companies and Internet providers in the US to being forced to pass on the personal data collected during their commercial operations to the government – it belongs to them and its seizure affects their reputation and the security of their customers.

• Fourth, the gulf between security needs and the privacy rights of individuals, both Americans and others, is as wide as ever. Should Snowden be prosecuted as an outlaw, or commended for opening an overdue debate on security issues – which needed to be reviewed and probably rebalanced?

• Fifth, attempts to promote data privacy rules as a safeguard against electronic surveillance proved to be unsuccessful as these rules were not designed for that purpose and comes at disproportionately high costs. So were attempts to leverage on TTIP negotiations, especially as Europe is the demandeur of that FTA – not the US. Data privacy rules are also regulatory barriers in the eyes of trade negotiators, proven by the EU’s own offensive stance in its prior FTAs.

ENDNOTES

1. See Charlie Savage, “The leak source carrying a Rubik’s Cube”, 12 June 2013; The New York Times, editorial, 6 June, 2013 “President Obama’s Dragnet”; also The New York Times, 18 June 2013 revealing that companies such as Verizon, and Internet providers and social media websites such as Facebook were all supplying messages and call date to the NSA and the FBI.

2. See Reuters, “U.S. revokes Snowden’s passport: official source”, 23 June 2013; The New York Times editorial, “No Act of Treason”, 14 June 2013 citing John Boehner, Speaker of the House and Dianne Feinstein, chair of the Senate Intelligence Committee both using terms such as “traitor” and “act of treason”.


4. See articles in The New York Times by Shane, Scott, 18 June 2013; Savage, Charlie and Mazzetti, Mark, 12 June 2013 and editorial 6 June 2013; Tempora programme (managed by the British GCHQ) reported in e.g. Storm, Darlene, Computer World, 8 July 2014.


17. On compromise talks see The New York Times, e.g. Smale, Alison, “Europeans link trade talks to U.S. surveillance”, 4 July 2013; Eddy, Melissa, “Allies have long history of swapping intelligence” and “Merkel defends intelligence alliance with U.S.”, 10 and 12 July 2013; For the ‘Five Eyes’ group see the article cited in footnote 4 supra.


19. See EU–South Korea Free Trade Agreement, Art. 7.43.


21. Companies such as Lavabit and Silent Circle who shut down were mentioned; legal challenges were made by Calyx Internet Access and the Electronic Frontier Foundation. A coalition with Yahoo, Google and Microsoft aboard has appealed to the administration to be able to be more transparent than FISC orders permitted.

BIBLIOGRAPHY

News reports with initial revelations
Greenwald, Glenn, MacAskill, Ewen, “NSA Prism program taps in to user data of Apple, Google and others”, The Guardian, 7 June 2013.

Gellman, Barton, Markon, Jerry “Edward Snowden says motive behind leaks was to expose ‘surveillance state”, The Washington Post, 9 June 2013.


Other news reports


*Articles*


The European Centre for International Political Economy (ECIPE) is an independent and non-profit policy research think tank dedicated to trade policy and other international economic policy issues of importance to Europe. ECIPE is rooted in the classical tradition of free trade and an open world economic order. ECIPE’s intention is to subject international economic policy, particularly in Europe, to rigorous scrutiny of costs and benefits, and to present conclusions in a concise, readily accessible form to the European public. We aim to foster a “culture of evaluation” — largely lacking in Europe — so that better public awareness and understanding of complex issues in concrete situations can lead to intelligent discussion and improved policies. That will be ECIPE’s contribution to a thriving Europe in a world open to trade and cross-border exchange.

LATEST PUBLICATIONS:

Nowhere To Go? Surveillance, Privacy Rules and Trade Talks
ECIPE Policy Brief No. 01/2014
By Roderick Abbott

Trade and Logistics: A “Bali Package” for the EU
ECIPE Bulletin No. 01/2014
By Erik van der Marel

The Internationalization of the Renminbi and the Rise of a Multipolar Currency System
ECIPE Working Paper No. 01/2014
By Miriam Campanella

Labour-Market Integration of Immigrants in OECD-Countries: What Explanation Fit the Data?
ECIPE Occasional Paper No. 04/2013
By Andreas Bergh

What now for EU-Ukraine relations?
ECIPE Bulletin No. 11/2013
By Michal Krol

One Year after Russia’s WTO Accession: Time for Reform
ECIPE Bulletin No. 10/2013
By Erik van der Marel

A Multilateral Legal Assistance Protocol: Preventing Fragmentation and Re-territorialisation of the Internet
ECIPE Policy Brief No. 09/2013
By Hosuk Lee-Makiyama

A Trans-Pacific Partnership worth its weight in gold - but what is taking so long?
ECIPE Bulletin No. 09/2013
By Lisa Brandt

Is e-commerce really the threat to European way of life – or did domestic populism trump the Single Market?
ECIPE Bulletin No. 08/2013
By Hosuk Lee-Makiyama

Why Are Services Commitments in RTAs Stronger than in the GATS? Trade Policy Implications for TTIP
ECIPE Bulletin No. 07/2013
By Erik van der Marel

The Case for an EU-China investment agreement
ECIPE Bulletin No. 06/2013
By Michal Krol

Argentina, the Expropriation of Repsol YPF, and the Case for Improved Investment Protection Accords
ECIPE Policy Brief No. 08/2013
By Fredrik Erixon, Lisa Brandt

Who’s Afraid of China’s High-Tech Challenge?
ECIPE Policy Brief No. 07/2013
By Guy de Jonquières

Biofuels Reform in the European Union: Why New ILUC Rules will Reinforce the WTO Inconsistency of EU Biofuels Policy
ECIPE Occasional Paper No. 03/2013
By Fredrik Erixon

Solar Panels, Telecommunication Equipment – and the “Modernisation” of EU Trade Defence Policy
ECIPE Bulletin No. 05/2013
By Fredrik Erixon

China’s Rise: Perceptions and Misperceptions
ECIPE Policy Brief No. 06/2013
By Krishnan Srinivasan