Technological Sovereignty: Missing the Point?

An Analysis of European Proposals after June 5, 2013

by TIM MAURER, ROBERT MORGUS, ISABEL SKIERKA, MIRKO HOHMANN

Following reports of foreign government surveillance starting in June 2013, senior officials and public figures in Europe have promoted proposals to achieve "technological sovereignty". This paper provides a comprehensive mapping and impact assessment of these proposals, ranging from technical ones, such as new undersea cables, encryption, and localized data storage, to non-technical ones, such as domestic industry support, international codes of conduct, and data protection laws. This analysis shows that most technical proposals will not effectively protect against foreign surveillance. In addition, some proposals could negatively affect the open and free Internet or lead to inefficient allocation of resources. Finally, proposals tend to focus on the transatlantic dimension, neglecting the broader challenge of foreign surveillance and promising ideas like the expansion of encryption tools. Ultimately, the security of data depends primarily not on where it is stored and sent but how it is stored and transmitted.

This paper is part of a joint project by New America's Open Technology Institute and the Global Public Policy Institute (GPPi) called "Transatlantic Dialogues on Security and Freedom in the Digital Age". For more: www.digitaldebates.org

November 2014

TRANSATLANTIC DIALOGUES

ON SECURITY AND FREEDOM IN THE DIGITAL AGE

Acknowledgements

The authors would like to thank the members of the Steering Committee for the project Transatlantic Dialogues on Security and Freedom in the Digital Age (go to www.digitaldebates.org for more) as well as the participants of our workshop hosted in Washington, DC, on September 18, 2014, for their valuable input and feedback (see Annex 4). The authors also owe a special debt of gratitude to Scott Janz, an intern at New America's Open Technology Institute, and Joanna Bronowicka, an intern at the Global Public Policy Institute, for their outstanding help throughout the process of building the report. The authors also thank Lucas Stratmann for his research help; Dan Staples and Seamus Tuohy for their technological expertise; Stefan Heumann and Jonah Force Hill for their constructive criticism; Krystle Wong and Esther Yi for their editing; and Oliver Read for ensuring a thorough editing and polished layout.

All views, errors or omissions are solely the authors' responsibility.

This report has been funded with the assistance of the European Union. The contents of this report are the sole responsibility of New America and GPPi, and can in no way be taken to reflect the views of the European Union.

Table of Contents

Executive Summary

European government officials and public figures have promoted a variety of proposals for gaining "technological sovereignty" in response to the media reports that began emerging in June 2013 on foreign surveillance. Our research identified proposals from over a dozen countries in Europe that range from the construction of new undersea cables to stronger data protection rules made by top decision-makers and other public figures. The current German government's coalition agreement, for example, explicitly states that it will "take efforts to regain technological sovereignty."[1] Some of these statements and proposals qualify as simple posturing to address political pressure. Others have been more seriously debated publicly.

This report finds that many of the proposals do not effectively protect against foreign surveillance. Moreover, some of them, especially technical proposals forcing localized data storage or routing, are likely to negatively affect a free and open Internet. Other proposals attempt to use the political window of opportunity to redirect limited resources and funding for political purposes, leading to suboptimal investments and policy outcomes. The specific impact often depends on how a proposal is implemented. That's why Europe needs to focus more on its responsibility to ensure globally an open, free, and secure Internet. Actively promoting proposals for greater control within Europe will limit Europe's ability to present itself as a global advocate of a free and open Internet. Without greater nuance, other governments could use the proposals to justify their own actions, including those that do not protect, but violate, human rights.

Many technological sovereignty proposals were advanced with the goal of securing data and privacy. The majority of proposals focus on the physical location of data as a security mechanism. But data privacy and security depend primarily not on where data is physically stored or sent, but on how it is stored and transmitted. Moreover, the debate thus far has focused narrowly on the transatlantic dimension, but the problem of data privacy and security is much bigger. The proposals most likely to protect against any foreign surveillance focus on the use of encryption tools. These deserve greater attention from policymakers. The debate on the use of encryption tools includes discussing the local government's ability to conduct domestic law enforcement efforts, which has been the subject of an emerging and important debate in the United States and the United Kingdom.[2]

The goal of this report is to provide a more nuanced, technically informed analysis of these proposals, in the hope that it will lead to a more productive discussion. The main contribution of this paper is a systematic mapping and impact assessment of existing proposals, using the Organisation for Economic Cooperation and Development (OECD) Principles for Internet Policy-Making and a traffic-light system to visualize the proposals' impact. The mapping and impact assessment provide a more detailed analysis of technical proposals that could have long-lasting effects on the architecture of the Internet. This assessment can serve as a toolbox for policymakers, so that they can better assess the nature, feasibility, and viability of the proposals. Europe has a responsibility to lead by example in ensuring an open, free, and secure Internet. This report strives to advance this goal.

Introduction

In the months following the 2013 reports revealing surveillance by foreign governments, European government officials and public figures have promoted a variety of measures for gaining "technological sovereignty." The current German government's coalition agreement, for example, explicitly states that it will "take efforts to regain technological sovereignty." [3] The term remains vague and undefined. In this report, it is used in the same way as policymakers have used it: an umbrella term for a spectrum of different technical and non-technical proposals, ranging from the construction of new undersea cables to stronger data protection rules. Many of them are not new but have developed greater political traction over the past year.

After scrutinizing the proposals, this report finds that many of them do not significantly enhance protection against foreign surveillance from any country. For example, new undersea cables are expensive but can be tapped as easily as existing cables.[4] Moreover, some of the proposals are likely to negatively affect a free and open Internet. For instance, nationalized or bordered routing directly opposes the original construction of the Internet, which was designed to allow data to flow by way of the most efficient route at that particular moment. Other proposals attempt to use the political window of opportunity to redirect limited resources and funding for political purposes, leading to suboptimal investments and policy outcomes. In short, many proposals will not effectively protect against foreign surveillance, and they distract from more promising ideas like the broader use and enhanced quality of encryption. A full impact assessment of selected proposals is outlined in this study.

The German government has been most vocal in Europe about its intentions to safeguard technological sovereignty. In its recently adopted Digital Agenda, Germany calls for the preservation and expansion of "Germany's autonomy and authority over information and telecommunication technology."[5] Calls for technological sovereignty resonate strongly with German telecommunications companies and hardware manufacturers, which would be tasked with implementing national routing, e-mail, or hardware solutions. Similar pan-European suggestions include a "European" or a "Schengen" cloud that requires all data for citizens of the European Union (EU) or Schengen area to be stored and processed inside the respective geographical area and to be subject to local data protection laws.[6]

Our research identified additional proposals from over a dozen countries in Europe. For example, in February 2014, French President François Hollande and German Chancellor Angela Merkel discussed a "European communication network," in which data would be routed through European servers as much as possible. The EU is also promoting alternatives to United States-based communication infrastructure. In February 2014, EU President Herman Van Rompuy and Brazilian President Dilma Rousseff agreed to lay a new undersea cable between Europe and Brazil, circumventing the US.[7] Similarly, Finnish Minister of Education, Science and Communication Krista Kiuru called for a new cable between Finland and Germany that circumvents Sweden, whose national intelligence agency, the National Defence Radio Establishment, has conducted bulk collection of data and provided access to Baltic undersea cables to other intelligence agencies.[8]

Research on the implications of these technological sovereignty proposals remains nascent. A growing body of literature examines the growth of "data localization" policies, meaning the "laws and guidelines which limit the storage, movement, and/or processing of digital data to specific geographies, jurisdictions, and companies."[9] Such proposals were the focus of attention in early 2014, because they were part of Brazil's debate over its Internet Bill of Rights, "Marco Civil da Internet." The term "technological sovereignty" remains vague. As it is used by European policymakers, it resembles terms like "data sovereignty," which has been defined as "a spectrum of approaches adopted by different states to control data generated in or passing through national [I]nternet." It is a subset of "cyber sovereignty," which is "the subjugation of the cyber domain to local jurisdiction."[10]

The main contribution of this paper is a comprehensive, systematic mapping and impact assessment of existing technological sovereignty proposals.[11] It builds upon existing literature,[12] but our approach differs by distinguishing between types of proposals, technical or non-technical, and by considering whether they achieve their purported goal of protecting against foreign surveillance. This paper goes beyond analyses focused solely on data localization requirements[13] by providing a comprehensive overview of the proposals that have been advanced under the umbrella of technological sovereignty. We use the term "technological sovereignty" as an umbrella term for the wide assortment of European proposals, ranging from technical ones, such as new undersea cables, encryption, and localized storage, to non-technical ones, such as local industry support, international codes of conduct, and data protection laws.

As Harvard professor Joseph Nye has pointed out, Internet fragmentation is already a reality. The question is: What type of fragmentation undermines a free and open Internet, and how can further fragmentation of this kind be averted?[14] Accordingly, this study focuses on the effect of technical proposals on the open architecture of the Internet. The second chapter presents an analytical framework for classifying technical and non-technical proposals, which is explained in greater detail in Annex 1. Subsequently, it examines the proposals' political traction and salience in current public debates. The impact assessment in the third chapter provides a more detailed analysis of technical proposals, which could have long-lasting effects on the Internet architecture, whereas non-technical proposals are arguably easier to reverse. Using the 2011 OECD Principles for Internet Policy-Making, this paper analyzes the proposals' implementation in an environment of limited resources and their impact on the Internet. Of the 14 OECD principles, we focus on the principles relating to the preservation and promotion of human rights, transparent and accountable governance, economic benefits, and Internet security.

This impact assessment was developed to serve as a toolbox for policymakers, so that they can better assess the nature, feasibility, and viability of the proposals. We hope that the framework will be a helpful model for policy- and decision-makers as more empirical research becomes available, even if the reader does not fully agree with our assessment of the proposals.

Ultimately, our goal is to provide a more nuanced, technically informed analysis of these proposals, in the hope that it will lead to a more productive discussion. Proposals

that do not achieve their stated goals or whose unintended negative consequences outweigh their benefits should be discarded. This will pave the way for focusing on the more promising proposals. Today, only a third of the world's population uses the Internet. Another two billion people are projected to gain access over the next five years.[15] Europe has a responsibility to lead by example in ensuring an open, free, and secure Internet now and in the future. This study hopefully contributes to that end.

Analytical Framework for Classifying the Proposals & The Proposals' Political Traction

We marry our political analysis with the scholarship of Internet governance expert Laura DeNardis, who writes, "arrangements of technical architecture are also arrangements of power."[16] The Internet is a meta-network, composed of a constantly changing collection of individual networks and devices that communicate with each other through the Internet Protocol (IP). Through technical features, the physical and software architecture, or code, shapes human behavior on the Internet and beyond. Because the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. This architecture constitutes a powerful tool for actors to further their interests. According to Stanford law professor Barbara van Schewick, policymakers who traditionally used the law can now use Internet technologies to bring about desired political or economic effects.[17] Building upon this scholarship, we designed a framework for classifying the proposals based on what part of the Internet they impact. (A snapshot from the full list of proposals and their sources, dates, and classifications starts on p. 11 with more details on the framework and methodology outlined in Annex 1.)

We began this research by collecting the proposals and statements of European political decision-makers, as well as those of stakeholders from the private sector and academia, made after June 5, 2013, the day on which the first wave of articles about foreign government surveillance was published. It is important to bear in mind that while these proposals were advanced in response to the surveillance affair, they address different dimensions of a complex problem, namely the protection of:

1. Government secrets;
2. Individual citizens' privacy;
3. Industry secrets.

An additional complexity is the fact that policymakers have been using the political attention to suggest new industrial policies aimed at supporting the European Information Technology (IT) sector through major public investments and IT sector-specific subsidies.

Upon completing the collection phase of research, we divided the proposals into two groups: technical and non-technical, with further details visualized in Annex 1.

Technical proposals are based on the type of technological change proposed: new undersea cables, national e-mail, localized routing and storage, and encryption. New undersea cables, for example, refer to suggestions to directly connect Latin America and Europe, avoiding data transfer through the United States. Likewise, national

e-mail was suggested in Germany as a means of avoiding contact with American servers whenever possible. Localized routing goes a step further than national e-mail, in the sense that it would encompass all data, not just e-mail data, and route it solely through local servers. However, localized does not necessarily mean that the data is concentrated in one country. For example, localized could encompass the entirety of the European Union. Finally, there have been calls for improving encryption, making existing encryption more accessible to the general public, and extending it to mobile devices.

Non-technical proposals are sorted based on the changed mechanism: institution, law, norm, transparency, and business. The idea to establish a single EU Data Protection Agency exemplifies how actors consider institutions as a means of addressing a given challenge. A wide variety of laws have been proposed, and some implemented, ranging from changes to the US-EU Safe Harbor agreement[18] to domestic data protection laws. There are also several proposals aimed at increasing trust – not through regulation, but through the establishment of common norms, like a "no-spying" agreement between the US and European partners.[19] Another non-technological category is composed of proposals aimed at increasing transparency of how governments and businesses handle the data of citizens and customers. Proposals to advance the national production of hardware and software mainly originate in Germany, such as the "IT Security Made in Germany" brand or the production of an IT-Airbus in cooperation with France. Ideas like these fall into the business cluster, though there are technical components to the proposals. Generally, these non-technical proposals impact non-technical factors that shape the Internet, like laws, norms, markets, and institutions.

Proposals' Political Traction

Some proposals have gained more political traction than others over the past year and a half. Classified as having high political traction are proposals that have been widely discussed, that have been implemented, or are likely to be implemented. Other proposals have been discussed, but their implementation remains uncertain. These are classified as having medium political traction. Some proposals have been barely discussed or were discussed and discarded, and these are classified as having low political traction. (For a full list of proposals, see Annex 2.)

A number of proposals with the highest political traction are close to implementation. The German government, for example, is debating whether to exclude foreign companies from government contracts if they cannot guarantee that data will not be shared with another government. This action has been accompanied by a general shift of government services from foreign to local companies.[20] Similarly, proposals for strengthening data protection standards in Europe have gained much political traction. The EU's institutions will most likely adopt the European Data Protection Regulation in 2015.[21] Additional proposals in Germany for developing an "IT Security Made in Germany" brand have garnered attention from politicians. Among the technical proposals, new undersea cables have also been seriously debated.[22] Brazilian and Finnish initiatives to lay new undersea cables circumventing the US and Sweden, respectively, will be implemented in the next two years.[23] A local e-mail service proposed by Deutsche Telekom and United Internet in Germany has been implemented, though experts and media outlets have criticized the proposal for providing a false sense of security.[24] Nonetheless, polling suggests that more than half of Germans have found the initiative "helpful," raising questions about perceived

versus actual security.[25] Because of its implementation, it is included in the bucket of high political traction.

The majority of proposals have gained some political traction, but their implementation remains uncertain. To date, no steps have been taken to legally mandate localized data storage. Instead, policymakers have turned to the promotion of localized storage as a best practice and voluntary data security standards. For example, the European Commission issued the Cloud Service Level Agreement Standardisation Guidelines,[26] and the Steering Board of the European Cloud Partnership suggests common, non-binding security and encryption standards for European cloud providers storing data on European soil.[27] Growing demand for European or national cloud options has led companies like SAP, Hewlett-Packard, Microsoft, and Oracle to offer local cloud solutions.[28]

Another bucket of proposals with medium political traction are calls for stronger encryption. Several experts have called for the development of more easily accessible encryption tools,[29] and the European Parliament has called on the European Commission to "strengthen the protection of confidentiality of communication ... by way of requiring state-of-the-art end-to-end encryption of communications."[30] Major technology companies like Apple and Google have also begun offering encryption by default,[31] and the Internet Engineering Task Force (IETF) has resumed work on building encryption by default into HTTP 2.0 after the initial surveillance reports, a project it had previously decided against in March 2012.[32]

Other proposals have not gained, or no longer have, significant traction. Proposals to locally route data traffic – whether on a national, Schengen, or pan-European scale – were intensely debated but no longer have substantial political traction. Another initiative to provide secure SIM data and cryptophones for government and corporate customers met limited demand.[33] A legal "no spying" agreement between governments to limit surveillance was discussed but not implemented.[34]

Snapshot of Mapping

This is a snapshot from the full list of proposals. The entire mapping can be found in Annex 2.

Technical Proposals

TYPE OF PROPOSAL	SUMMARY	PROPOSING ACTORS	COUNTRY OR REGION	TIME RANGE	DIMENSION	DATA TYPE	LAYER	POLITICAL TRACTION
National e-mail	Route all e-mails within Germany on German servers and cables[35]	Private: Deutsche Telekom	Germany	8/1/2013	Code	Motion + Meta	Application	High
Undersea cables	Lay a new fiber-optic submarine cable between Latin America and Europe; lay a new fiber-optic cable between Finland and Germany, circumventing Sweden[36, 37]	Public: Herman Van Rompuy (President of the European Council), Krista Kiuru (Finnish Minister of Education, Science and Communication)	EU, Finland	12/11/2013-2/24/2014	Code	Motion	Physical	High
Localized data storage	Create a European or a Schengen cloud; create a European or Schengen zone for data[38, 39, 40, 41]	Public: France, Germany; Private: Green, Deltalis, Quantique (Switzerland), EuroCloud (Poland)	France, Germany, Poland, Switzerland	6/27/2013-5/14/2014	Code, Market, Norm, Law	Rest + Meta	Data at rest	High-Medium
Localized routing	Data streams should flow within a geographically restricted zone; inter-Schengen data traffic should be routed within the Schengen zone.[42, 43, 44, 45, 46, 47]	Public: German government; Private: Deutsche Telekom, Atos	France, Germany	10/12/2013-7/27/2014	Code, Norm, Law	Motion + Meta	Protocol (Content, Application, Physical)	Medium

Impact Assessment

The following impact assessment can serve as a toolbox for policymakers as they focus on the most promising proposals while discarding those that do not achieve their stated goals or whose negative consequences outweigh their benefits. The assessment examines whether the proposals actually achieve their purported goals of making data more secure in response to the surveillance debate, and then assesses the proposals' broader implications for the Internet, using the 2011 OECD Principles for Internet Policy-Making.[48]

The OECD principles provide concise guidance for policymakers crafting Internet policy, and they were designed to "help preserve the fundamental openness of the Internet while concomitantly meeting certain public policy objectives."[49] Given that the OECD member countries, as well as multiple other stakeholders, agreed upon these principles, they offer a useful anchor for transatlantic cooperation. We identified eight out of the 14 principles that are relevant to technological sovereignty and grouped them into four categories that constitute the foundation for our impact assessment of the proposals:

Human Rights:
- OECD #1: Promote and protect the global free flow of information.
- OECD #9: Strengthen consistency and effectiveness in privacy protection at a global level.

Governance – Open Internet:
- OECD #2: Promote the open, distributed, and interconnected nature of the Internet.
- OECD #8: Ensure transparency, fair process, and accountability.

Economic:
- OECD #4: Promote and enable the cross-border delivery of services.
- OECD #11: Promote creativity and innovation.

Security:
- OECD #13: Encourage cooperation to promote Internet security.
- OECD #14: Give appropriate priority to enforcement efforts.

For a full list and explanation of the principles, see Annex 2.

We use a simple traffic-light system for the impact assessment. A green light means that the proposal would have a positive impact on the principle. A yellow light means that the impact on the principle is either neutral or depends on the proposal's implementation. A red light denotes that the policy proposal is at odds with the principle. Some principles did not apply to a proposal.

Technical Proposals

		OECD Principles							
		BUCKET 1: HUMAN RIGHTS		BUCKET 2: GOVERNANCE		BUCKET 3: ECONOMIC		BUCKET 4: SECURITY	
Technical Proposals	**Political Traction**	OECD #1	OECD #9	OECD #2	OECD #8	OECD #4	OECD $#11	OECD #13	OECD #14
National e-mail	High	🔴	🟡	🔴	🟡	🔴	🟡	🟡	🟢
Undersea cables	High-Medium	🟡	🟡	🟡	N/A	🟢	🟡	🟡	🟢
Localized routing	Medium	🔴	🟡	🔴	🟡	🔴	🟡	🟡	🟢
Localized data storage	Medium	🔴	🟡	🔴	🟡	🔴	🟡	🟡	🟢
Expand encryption tools	Medium	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟡
More-secure encryption standards	Medium	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟡

BUCKET 1: HUMAN RIGHTS
OECD #1: Promote and protect the global free flow of information
OECD #9: Strengthen consistency and effectiveness in privacy protection at a global level

BUCKET 2: GOVERNANCE – OPEN INTERNET
OECD #2: Promote the open, distributed, and interconnected nature of the Internet
OECD #8: Ensure transparency, fair process, and accountability

BUCKET 3: ECONOMIC
OECD #4: Promote and enable the cross-border delivery of services
OECD #11: Promote creativity and innovation

BUCKET 4: SECURITY
OECD #13: Encourage co-operation to promote Internet security
OECD #14: Give appropriate priority to enforcement efforts

🔴 The proposal is at odds with the principle.

🟡 The proposal either has a neutral impact on the principle or the impact depends on the proposal's implementation.

🟢 The proposal has a positive impact on the principle.

N/A The principle does not apply to the proposed policy.

Non-Technical Proposals

		OECD Principles							
		BUCKET 1: HUMAN RIGHTS		BUCKET 2: GOVERNANCE		BUCKET 3: ECONOMIC		BUCKET 4: SECURITY	
Non-Technical Proposals	**Political Traction**	OECD #1	OECD #9	OECD #2	OECD #8	OECD #4	OECD $#11	OECD #13	OECD #14
Companies unable to provide legal guarantee excluded from federal contracts	High	N/A	🟢	🔴	🟡	🔴	🟡	🟡	🟢
Shift government services from foreign to local companies	High	🟡	🟡	🔴	🟡	🔴	🟡	🟡	🟢
EU Data Protection Authority	High-Medium	N/A	🟡	N/A	🟡	N/A	N/A	N/A	🟡
EU Data Protection Directive	High- Medium	🟡	🟢	🟡	🟡	🟡	🟡	🟡	🟡
"IT Security Made in Germany" brand	High- Medium	N/A	🟡	🔴	🟡	🔴	🟡	🟡	🟢
Increase funding for small businesses	Medium	N/A	🟡	🟡	N/A	🟡	🟢	🟡	🟡
Encryption key governance	Low	🟡	🟡	N/A	🟡	N/A	N/A	🟡	🟡
Single committee for all digital issues	Low	N/A	N/A	N/A	🟡	N/A	N/A	N/A	N/A
Legal code of conduct between intelligence agencies	Low	N/A	🟡	N/A	🔴	N/A	N/A	🟡	🟡
Transparency on government access to data	Low	🟡	🟡	N/A	🟢	N/A	N/A	🟡	🟡

BUCKET 1: HUMAN RIGHTS
OECD #1: Promote and protect the global free flow of information
OECD #9: Strengthen consistency and effectiveness in privacy protection at a global level

BUCKET 2: GOVERNANCE – OPEN INTERNET
OECD #2: Promote the open, distributed, and interconnected nature of the Internet
OECD #8: Ensure transparency, fair process, and accountability

BUCKET 3: ECONOMIC
OECD #4: Promote and enable the cross-border delivery of services
OECD #11: Promote creativity and innovation

BUCKET 4: SECURITY
OECD #13: Encourage co-operation to promote Internet security
OECD #14: Give appropriate priority to enforcement efforts

🔴 The proposal is at odds with the principle.

🟡 The proposal either has a neutral impact on the principle or the impact depends on the proposal's implementation.

🟢 The proposal has a positive impact on the principle.

N/A The principle does not apply to the proposed policy.

National E-mail

Goals achieved?

The alleged benefit of initiatives like "E-Mail Made in Germany" is that e-mails would be secure from foreign surveillance. However, while using Secure Sockets Layer encryption increases security, the SSL encryption of data in transit that E-Mail Made in Germany offers is not a new advancement.[50] The latest version of this encryption was issued in 2008 and has been implemented by many e-mail providers long before Deutsche Telekom and United Internet made their announcement.[51] In addition, the security protocol, SSL, is vulnerable to man-in-the-middle attacks, which intelligence agencies have used to intercept e-mail traffic in the past.[52] Lastly, while e-mails in transit are secured through SSL, this security does not extend to the storage of the data on servers. In short, a national e-mail service as proposed is unlikely to protect against foreign surveillance.

Broader implications for the Internet, using the OECD Principles for Internet Policy-Making

- **Human Rights:** The proposed national e-mail service is unlikely to protect against foreign surveillance. Instead, localization proposals negatively affect the free flow of information, while it enhances domestic state and private actors' control over data.[A] Therefore, the impact on privacy depends on the local government's respect for privacy. Furthermore, governments outside of Europe, namely authoritarian regimes with poor human rights records, could rhetorically use Germany's localized e-mail efforts to justify their own actions, weakening Germany and Europe's human rights foreign policy.

- **Governance – Open Internet:** Forcing localized e-mail routing will have a negative impact on the open and interconnected nature of the Internet by forcing traffic to remain within geographic borders and national territories.

- **Economic:** Localized routing and national e-mail undermine the promotion of the cross-border delivery of services.

- **Security:** Whether national e-mail proposals increase or decrease Internet security depends on whether the local company uses a lower or higher security standard than the foreign provider. Given that the current encryption standard proposed for these initiatives is not higher than the standard used by most providers, the new service will not improve security. Instead, national e-mail could make law enforcement easier, since data is stored within national borders and subject to national data protection laws, which usually contain enforcement exceptions.[53]

Conclusion: The national e-mail service proposed is unlikely to protect against foreign intelligence agencies. Instead, it undermines the nature of the open and interconnected Internet and sets a precedent for authoritarian governments to reference, which would

A Given that the ordinary citizen is likelier to be the target of surveillance from domestic rather than foreign government agencies, this proposal could actually enable more surveillance as a whole. In addition, national e-mail services could provide a one-stop-shop for intelligence and law enforcement agencies and for storing data on a limited number of servers in a finite number of locations.

undermine European human rights and foreign policy. Last but not least, this example highlights the risk of promoting proposals that give users a false sense of security by claiming enhanced security features without actually significantly enhancing security.

Undersea Cables

Goals achieved?

The main goal of constructing new undersea cables is to better protect against foreign surveillance. However, a direct cable link from Brazil to Europe, for example, will not prevent the cable from being tapped by a government with the capability to do so.

Broader implications for the Internet, using the OECD Principles for Internet Policy-Making

- **Human Rights:** New undersea cables will not prevent foreign governments from tapping new cables. The effect on the free flow of information depends on the domestic laws of the countries that the new cables connect to.

- **Governance – Open Internet:** In principle, new undersea cables contribute to a more distributed and interconnected Internet as long as the cables remain connected to the global Internet and come without restrictions.

- **Economic:** The government-driven construction of new undersea cables is a case of a politically motivated investment that might risk the inefficient allocation of limited resources. New undersea cables do promote and enable the cross-border delivery of services by providing a new avenue through which data can flow.

- **Security:** New undersea cables will offer more capabilities to law enforcement agencies of the countries that the new cables connect to, by providing them with access to the data flowing through the cables. Therefore, and in light of the above, it provides a false sense of security to Internet users.

Conclusion: New undersea cables do not make data more secure and thus should be discarded as a policy option for protecting against foreign surveillance. Laying new cables for this reason creates a false sense of security for Internet users. More and new undersea cables can increase the resiliency of the Internet overall, which has been a secondary goal and has been advanced to justify new cables. However, this investment is not the most efficient way of allocating resources to maximize resilience, as the original goal was to protect against surveillance.

Localized Routing

Goals achieved?

Proposals for localized European or Schengen routing suggest the protection of individual Internet users' data from surveillance by foreign intelligence agencies.[54] The idea is that as long as intra-European data traffic is exclusively routed through European or national infrastructure and Internet Exchange Points, citizens' data will

be secure.[55] Such measures may raise the technical hurdle for intercepting data for certain foreign surveillance agencies, but may also in fact lower the legal hurdle for many intelligence agencies.[B] At the same time, localized routing may also make it easier for domestic intelligence and law enforcement to access and control more European Internet traffic than before, and domestic agencies may still pass the data on to foreign intelligence agencies that they cooperate with.

Broader implications for the Internet, using the OECD Principles for Internet Policy-Making

- **Human Rights:** Localized routing is unlikely to protect against foreign surveillance but will negatively affect the free flow of information by potentially enhancing domestic state and private actors' ability to control the free flow of information. Such a policy would in turn help authoritarian regimes with poor human rights records to justify their own actions to increase their control, weakening Europe's human rights foreign policy.

- **Governance – Open Internet:** Forcing localized routing distinguishes the local network from the global Internet, negatively impacting the open and interconnected nature of the Internet. The implementation of this proposal would require changes to the routing protocols and IP address allocation system, thus affecting basic principles of the Internet's architecture.

- **Economic:** Localized routing undermines the promotion of the cross-border delivery of services.

- **Security:** Localized routing would make law enforcement easier, since data is localized within national borders and subject to national data protection laws, which usually contain enforcement exceptions.[56]

Conclusion: Localized routing as proposed by France and Germany and private companies like Atos and Deutsche Telekom is unlikely to protect against surveillance by foreign intelligence agencies. Instead, it undermines the open and interconnected Internet, sets a precedent for authoritarian governments to reference, which undermines European human rights and foreign policy, and, like national e-mail initiatives, provides a false sense of security to Internet users.

Localization of Stored Data

Goals achieved?

European proposals to store data locally would require commercial cloud providers to relocate their servers. In Europe, the extension of localized data storage requirements

B For example, the US legal authority under which US intelligence and law enforcement agencies collect data outside of the US is Executive Order 12333. How the intelligence community interprets EO 12333 is largely unknown, though it is more permissive than Section 702 of the FISA Amendments Act, which permits law enforcement agencies to collect data within the US. For more on this subject, see: Tye, John. 2014. "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans." The Washington Post. July 18. <http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html>.

to privately owned data is a new development. Similar proposals to localize data of all citizens previously emerged in other parts of the world, namely China, Russia, and Iran.[57] Importantly, while the location of servers affects the legal protections of the data, it does not necessarily affect the ownership of or access to the data. For example, if data is held within EU territory, it is subject to EU data protection laws. This does not mean, however, that data is owned by parties exclusively subject to European law or rendered inaccessible for domestic or foreign intelligence services. Therefore, the security of data from foreign intelligence agencies depends not on where it is stored, but on comprehensive security practices, modern technology, and qualified security personnel.[58]

Broader implications for the Internet, using the OECD Principles for Internet Policy-Making

- **Human Rights:** The localized data storage proposals would limit the free flow of information, without achieving the goal of improving privacy protection. Confining data to a limited geographical area may render it legally easier for access by foreign or domestic intelligence agencies. It is the security measures, not the location of the server on which data is stored, that increases data security and privacy.

- **Governance – Open Internet:** Localized data storage would harm the open and distributed nature of Internet, by forcing the "nodes" to be located in specific geographic areas, where their operations might be suboptimal from a global perspective.

- **Economic:** Requirements to store data locally would impede cross-border delivery of services. Article 4 of the EU-US Information and Communication Technology (ICT) Trade Agreement[59] discourages this approach.[C] Requiring localized data storage will raise costs and barriers to entry, which in turn risks hampering innovation.[60]

- **Security:** Data security depends on factors beyond the physical location of servers. As for enforcement efforts: Locally stored data could be used to identify and prosecute conventional criminal activities.

Conclusion: Localized storage of data in a European or Schengen zone, as proposed by governments and companies across Europe, is unlikely to protect users' data from surveillance. Security of stored data depends not on its geographical location, but on the actual security of the technology used to store the data, encryption among them. In addition, it provides a false sense of security to users. Moreover, it risks increasing costs and barriers to entry, particularly for smaller foreign companies, which harms innovation.

C The EU-US ICT Trade Agreement urges governments not to impose local infrastructure requirements, stating, "Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services."

Expansion of Encryption Tools

Goals achieved?

While encryption may not protect individuals against sophisticated, targeted surveillance by intelligence agencies, the widespread use of encryption would significantly raise the cost of surveillance generally. The more individuals encrypt their communications, the more difficult and costly it will become for intelligence agencies to decrypt those communications. Encryption can be applied to all layers of the Internet – to the physical layer (cable or radio communications), the protocol layer (i.e, Hypertext Transfer Protocol (HTTP) or Transmission Control Protocol (TCP)), and the application layer (e-mail, www, mobile). Thus, encryption can protect both data in motion through end-to-end encryption of communications, as well as data at rest through encryption of devices at the end nodes. The different forms of encryption tools proposed in Europe attempt to deliver better privacy through various means:

1. End-to-end encryption of mobile voice communication through the use of crypto phones can be an effective tool for protecting government and business secrets and individuals' private data.

2. End-to-end encryption can also be applied to e-mail, instant messaging, cloud storage, and radio. Existing tools are often difficult and cumbersome to use, so engineers at the IETF and major US software companies are working on making encryption more easily accessible to the wider public.[61] It is possible for data encrypted from end-to-end to be accessed by intelligence or law enforcement agencies, but only through measures targeted at specific users and with much greater difficulty.

3. Large key sizes used in any type of encryption can also strengthen the privacy of users. Large key sizes mean that it will take longer to crack encryption, and it will be more expensive, forcing intelligence agencies to rely on more computing power in order to decrypt the data.

Broader implications for the Internet, using the OECD Principles for Internet Policy-Making

- **Human Rights:** Better and more widely accessible encryption has a positive effect on the protection of users' privacy without hindering the free flow of information. Encryption can prevent, or raise the cost, of surveillance, because existing methods of breaking or circumventing encryption focus on identified end nodes.

- **Governance – Open Internet:** Encryption has no negative impact on the open, distributed, and interconnected nature of the Internet. Different forms of encryption can be applied to various layers of the Internet while preserving its decentralized structure andstrengthening the capacity of actors within the existing frameworks.

- **Economic:** As long as encryption is promoted globally and encryption tools can be imported and exported without national restrictions, proposals to enhance encryption efforts can promote innovative, easier-to-use technologies. Encryption

and privacy protection have become central to the new business strategies of existing and emerging companies.[62]

- **Security:** Encryption strengthens overall Internet security, as well as individual and collective efforts for self-protection. But law enforcement and counterterrorism agencies point to a tension between data privacy and security. Some have consequently advocated for a "golden key" to encrypted devices and communications, which should be provided to or stored with a third party, such as a trusted authority under the state's jurisdiction. However, such backdoors and keys stored elsewhere constitute a risk for Internet security, since they could be exploited by criminals.[63]

Conclusion: Encryption enhances the protection of both data in motion and at rest, but not necessarily of metadata. It can be used to protect government, business, and individuals' data alike. Wider use of end-to-end encryption would make any surveillance significantly more difficult and costly. Encryption does not necessarily protect against the collection of metadata, targeted surveillance, and law enforcement, but significantly increases the cost of surveillance. The use of encryption tools has no negative impact on the free flow of information and strengthens overall Internet security, while hampering law enforcement and counterterrorism efforts.

Spotlight: "IT Security Made in Germany"

In addition to assessing the aforementioned technical proposals, we are putting a spotlight on the non-technical proposals for a subsidized local IT industry because they have been a focus in the debate but carry a significant risk of misperception. "IT Security Made in Germany" will not be more secure per se. Whether or not services and products will be more secure depends on the security standard and expertise, as well as the policies of the German government regarding backdoors. Depending on its implementation, "IT Security Made in Germany" might actually be less secure.

Goals achieved?

Initiatives such as "IT Security Made in Germany" suggest that domestically produced services and items are more secure and trustworthy than those produced abroad.[64] However, like the location of data storage and routing, it is not the location of production and supply chains that guarantees protection from surveillance or espionage, but the actual security standards. Locally produced security products can include as many, if not more, vulnerabilities than those of foreign companies. While this measure will make it harder for foreign intelligence agencies to build in backdoors, it does not prevent local intelligence or law enforcement agencies from doing so. Any backdoor will increase the general insecurity of these products.[65] These proposals, often labeled as especially secure, risk providing a false sense of security to customers, depending on their implementation.

Broader Implications for the Internet, using the OECD Principles for Internet Policy-Making

- **Human Rights:** This proposal may have a positive or negative impact on the protection of privacy. If the security standard is of lower quality, or if German intelligence agencies contract with companies to build backdoors, it will have a negative impact, and vice versa.

- **Governance – Open Internet:** The proposal does not have a direct impact on governance structures or on the promotion of the open nature of the Internet.

- **Economic:** The government-driven production of domestic hardware and software risks promoting protectionism, which can negatively impact competition, stifle innovation, and increase prices worldwide and other parts of the domestic industry.

- **Security:** This proposal has the potential to increase or decrease Internet security, depending on the security standards of the new technologies. Domestic IT products may enhance the capabilities of local law enforcement agencies, as producers may be obligated to build in access for law enforcement and intelligence agencies.

Conclusion: Homegrown hardware and software manufacturing as proposed by initiatives like "IT Security Made in Germany" is unlikely to protect against foreign surveillance. This policy is a government-induced regulation, which can lead to a decline in competition, innovation, and quality, as the European technology sector lags behind that of other countries and risks isolating itself.[66]

Conclusion

This in-depth analysis of the technological sovereignty proposals reveals several trends. First, it is unlikely that most technical proposals proposed to date will effectively protect data against foreign surveillance. Only a limited number of proposals might achieve that – namely encryption – and they have not been at the center of attention in the European debate. Second, some proposals could in fact have a negative effect on the open and free Internet, or at least lead to an inefficient allocation of limited resources. Moreover, the specific impact often depends on how the proposals are implemented and remains uncertain without further research. Third, the proposals tend to be narrowly focused on the transatlantic dimension and generally neglect the larger challenge and the new technological reality.

Data privacy and security depend primarily not on where data is physically stored or sent, but on how it is stored and transmitted. A critical fact often ignored in the debate thus far is that the governments exposed by media reports since June 5, 2013 are unlikely to be the only countries with such technical surveillance capabilities. The proposals most likely to protect against any foreign surveillance focus on encryption tools. These deserve greater attention and scrutiny if the goal is to protect against foreign surveillance. At first blush, restricting data from flowing through the physical infrastructure of other countries might seem like an effective measure for protecting against government surveillance. However, this is a false hope, given the many ways to gain access to data, ranging from tapping undersea cables to manipulating encryption standards to employing targeted malware. Moreover, the laws in some countries lower the legal barrier for intelligence agencies to collect and analyze data if the data is collected outside of the intelligence agency's home country. In other words, measures forcing data to remain within a country's borders might lower the legal threshold for foreign intelligence agencies to conduct surveillance in the first place. In short, proposals focused on simply avoiding certain countries geographically misunderstand current technological and legal realities and risk wasting important resources that could be used to effectively make data more secure.

The specific impact of proposals often depends on the details of their implementation, which remain unknown to date. On the surface, a proposal might appear to have a positive impact. For example, new undersea cables may increase resilience or lead to greater investment and growth. However, this was not the primary goal, and the politically motivated action is likely to lead to an inefficient allocation of limited resources. As another example, increasing funding for small businesses and establishing an "IT Security Made in Germany" brand will only increase data security if those companies produce, and are capable of producing, products and services with higher security standards than those of foreign companies. So far, the implementation of these proposals do no suggest that they offer significantly more secure services, in some cases providing instead a false sense of security.

Calls for technological sovereignty have not been limited to Europe. In Brazil, data localization proposals were hotly debated. In China, government offices are prohibited from using the Windows 8 operating system, and Cisco and IBM are under scrutiny.[67] The Australian government has banned China's Huawei from participating in building

its National Broadband Network. And the United States has not been immune from this trend, as portrayed by Congress's creation of a cyberespionage review process to limit government procurement of Chinese IT equipment in 2013.[68] Meanwhile, the British government has been a pioneer in trying to address cyber security risks and balancing them with a commitment to open markets. It established the Huawei Cyber Security Evaluation Centre (HCSEC) in 2010 to test Huawei products sold to British telecommunications companies, after similar concerns of foreign surveillance from Chinese telecommunications equipment firm Huawei.[69] HCSEC has been subject to several reviews,[70] and National Security Adviser Sir Kim Darroch found that while concerns regarding operational independence were not ungrounded, HCSEC had been achieving its objectives. Although HCSEC is an interesting model of addressing security risks while maintaining a commitment to open markets and free trade, it is hard to scale and does not provide a universal solution to the broader problem.

The European countries promoting technological sovereignty proposals have a responsibility to protect an open, free, and secure Internet and should not risk having other countries use these proposals to justify their own restrictive measures. Therefore, it is paramount for leaders in Europe to quickly and publicly discard proposals that were made in the spur of the moment and that do not make data more secure and instead risk undermining an open and free Internet. This will allow them to focus on the more promising proposals, to help move the debate in a more productive direction, and to ensure that the Internet remains open and free, as well as secure.

Annex 1: Methodology

Step 1: Dividing proposals into two general categories – technical and non-technical

A first review of the proposals revealed that they could be clustered into two general groups: technical and non-technical proposals. We then grouped technical proposals based on the type of technological change proposed: new undersea cables, national e-mail, localized routing, encryption, and localized data storage. These proposals directly affect the technical architecture of the Internet. Non-technical proposals are those that affect the Internet in other ways – for example, calls for new laws or for more transparency, which could affect the technical architecture but indirectly so.

Step 2: Applying Lessig's four dimensions for governing the Internet

To add more nuance, we applied Harvard Law Professor Lawrence Lessig's framework, which provides a nuanced conceptualization of the ways in which behavior on the Internet is constrained, or governed. He identifies four elements that shape behavior in cyberspace: (1) architecture, which corresponds with our category of technical proposals, as well as (2) laws, (3) social norms, and (4) markets, which help analyze the non-technical proposals in greater detail.[71] Some proposals do not focus on the means of governing the Internet but instead on the actor that governs, which is not part of Lessig's framework. Therefore, we included "institution" as an additional variable in our analytical framework for classifying proposals – for example, recommending the creation of a single committee on digital issues.

Figure 1: Lessig's Four Dimensions

NON-TECHNICAL CONSTRAINTS
Law:* The constraint that "regulates by sanctions imposed ex post" facto. Law is the most prominent of the constraints.
Norm:* The constraint that is built on understandings or expectations of how one ought to behave. Norms have no centralized norm enforcer, but are understood be everyone within a given community.
Market:* The constraint that regulates by price. Through this device, "market sets opportunities, and through that range of opportunities, it regulates."
Institution: The actor involved in governing cyberspace.
TECHNICAL CONSTRAINT
Architecture:* The constraint of the "world as I find it." In cyberspace this means that actual "software and hardware that constitutes cyberspace as it is."

* Source: Lessig, Lawrence (1998) The Laws of Cyberspace. Harvard Law School.

Lessig focuses on the law as a first dimension, which regulates by threatening "ex post sanction[s] for the violation of legal rights." He notes that it is the most prominent of the regulatory dimensions, but it is just one of the four.[72] The second dimension, norms, constitutes the "set of understandings [that] constrain behavior." The enforcer of the regulation is what differentiates norms from law. In the case of law, the state regulates. For norms, the threat of sanctions comes from the community.[73] The market dimension regulates by "pricing structures" that "constrain access."[74] The fourth regulatory device is what Lessig calls "architecture." Architecture dictates what behavior is possible or impossible.[75] Together, these dimensions govern the decisions of actors in real space.

Among Lessig's most important contributions is his discussion of the fourth dimension – architecture. What Lessig refers to as "architecture" in real space, he calls "code" in cyberspace, or "the software and hardware that constitutes cyberspace as it is – the set of protocols, the set of rules, implemented, or codified, in the software of cyberspace itself, that determine how people interact, or exist, in this space."[76] Code "sets the terms upon which [actors] enter, or exist, in cyberspace." For actors not versed in methods of code manipulation,[D] code is not an optional dimension. While actors are able to break norms and laws and manipulate the device of price, actors do not "choose whether to obey the structures that [code] establishes ... Life in cyberspace is subject to code."[77] Although laws, norms, and markets can shape how we use the Internet, the technical architecture of cyberspace equally influences how laws, norms, and markets develop.

For the purposes of this study, proposals encompassed by Lessig's constraint of law are those that explicitly or tacitly suggest legislative change. Social norm proposals are those that suggest mass behavioral changes without a guiding law or centralized enforcement. Proposals comprising the constraint of market are those that attempt to shape behavior based on price, whether by making a foreign service more expensive or a local one less expensive. These proposals, most of which are classified as non-technical by this report, affect markets, law, norms, or institutions, as they seek to alter the choices people make, given the actual constraints of cyberspace. Some technical proposals, like the data location proposals, are choice-based as well and seek to constrain decisions through norms, laws, or markets. However, the majority of technical proposals fall under code.

Step 3: Integrating different types of data – data in motion, data at rest, and metadata

To elevate the level of technical acumen informing this debate, it is important to note that several types of data exist: data in motion, data at rest, and metadata. Governance proposals depend on what type of data is to be governed.

The data we access on the Internet is stored on servers. When this data is inactive – meaning, it is not being changed or in motion – it is classified as data at rest. Data at rest can be the text, music, or video files we store in the cloud, or the data that is the content of a webpage stored on a company server.

Data in motion is data that traverses the physical infrastructure of the Internet. Because the Internet is a global network of computing devices, from laptops and PCs

D Hackers, for example.

to smart phones, data must flow from the host device or server to the device trying to access it. The easiest way to explain this phenomenon is to picture an e-mail sent from one user to another. The sender generates the data that then travels over the cables and wires that make up the physical infrastructure of the Internet, until it reaches the intended recipient. The same process happens when a user tries, for example, to access content through a webpage or download videos from a server. The route taken by the data depends on a number of factors, ranging from physical constraints like bandwidth to contractual considerations like peering agreements. Nonetheless, data is generally routed through what technologists refer to as the "cheapest" route. This ensures that the data reaches its recipient quickly and keeps Internet speeds high for everyone.

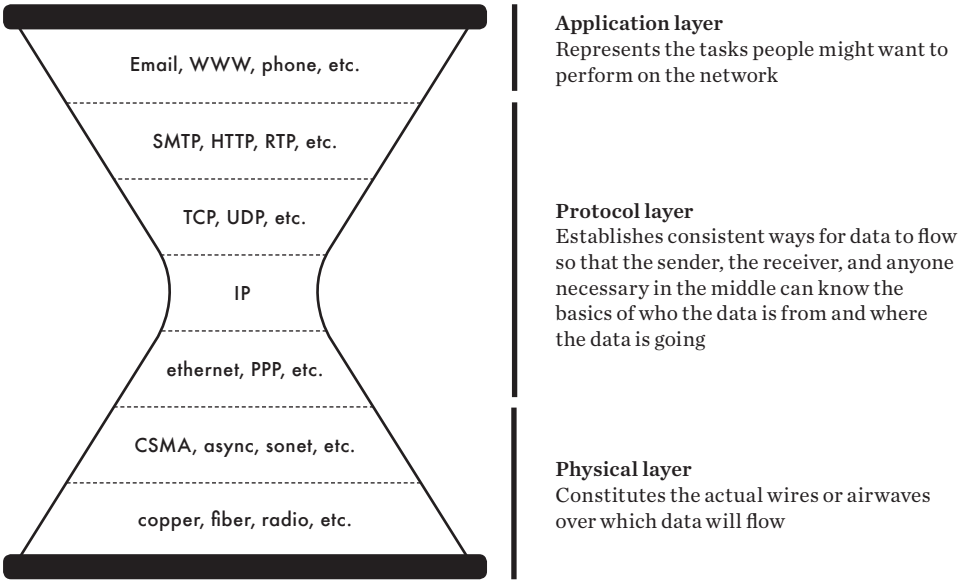
Metadata, simply put, is the data about data. Two types exist. Structural metadata "indicates how compound objects are put together."[78] This type of metadata is mostly used to present complex items. Structural metadata takes two separate streams of data, identifies them, and then ensures that they are properly synchronized for presentation. In other words, structural metadata ensures that the visual stream of the latest movie you are watching is synchronized with the audio stream. The second type of metadata is descriptive metadata, which "describes a resource for purposes such as discovery and identification."[79] This is the conceptualization of metadata. Descriptive metadata allows users to query databases and to identify data based on relevant criteria. It should be noted that even encryption does not necessarily protect metadata from surveillance. Figure 4 visualizes how the proposals are clustered.

Step 4: Zooming in on data in motion – the Hourglass Model

Several models exist to illustrate the intricacies of the technical architecture that underlies the Internet. Internet expert and Harvard law professor Jonathan Zittrain built upon those and the work of many other scholars by combining the technical and social components of the Internet with his interpretation of the Hourglass Model, which highlights the centrality of the IP for the Internet's coherence and interoperability.

At the bottom is the physical layer, or "the actual wires or airwaves over which data will flow."[80] Undersea and fiber-optic cables – and phone lines, in some cases – are categorized by this layer. Next is the protocol layer, which "establishes consistent ways for data to flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of whom the data is from and where the data is going."[81] This layer includes the limited IP, as well as the HTTP and the Simple Transportation Management Protocols (STMP). The IP layer is the narrowest layer in the hourglass model, signifying that it is, for the time being, the least elastic feature of the Internet, but also the layer on which the rest rely for communication. While we can build new cables and add more end-user devices, we are constrained by a finite number of IP addresses. Moving up the Hourglass, we find the application layer, "representing the tasks people might want to perform on the network."[82] E-mail clients and websites, for example, make up this layer. Resting atop the Hourglass are Zittrain's final two layers: the content layer, which is the actual information exchanged through the other layers, and the social layer, "where new behaviors and interactions among people are enabled by the technologies underneath."[83] These layers and the implications they carry apply directly to the proposals that we classify as technical proposals.

Figure 3: The Hourglass Model



Source: Zittrain, Jonathan (2008) *The Future of the Internet and How to Stop It*. Yale University Press. p. 67-68.

The Hourglass model offers an additional level of analysis for data in motion proposals to identify which layer they impact.

Figure 4: Visualizing the break-down of the proposals

All Proposals by Type	
TECHNICAL PROPOSALS (= LESSIG'S ARCHITECTURE)	NON-TECHNICAL PROPOSALS
Metadata Data at Rest Data in Motion (Hourglass Model)	Law Law/Norm Law/Norm/Market Market Institution

The architecture constraint in real space is the constraint of code in cyberspace. As the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. That's why the technical proposals are a specific focus of this paper.

Annex 2: Complete List of Technological Sovereignty Proposals

Technical Proposals

TYPE OF PROPOSAL	SUMMARY	PROPOSING ACTORS	COUNTRY OR REGION	TIME RANGE	DIMENSION	DATA TYPE	LAYER	POLITICAL TRACTION
National e-mail	Route all e-mails within Germany on German servers and cables[84]	Private: Deutsche Telekom	Germany	8/1/2013	Code	Motion, Meta	Application	High
Undersea cables	Lay a new fiber-optic submarine cable between Latin America and Europe; lay a new fiber-optic cable between Finland and Germany, circumventing Sweden[85, 86]	Public: Herman Van Rompuy (President of the European Council), Krista Kiuru (Finnish Minister of Education, Science and Communication)	EU, Finland	12/11/2013-2/24/2014	Code	Motion	Physical	High
Localized data storage	Create a European or a Schengen cloud; create a European or Schengen zone for data[87, 88, 88, 89]	Public: France, Germany; Private: Green, Deltalis, Quantique (Switzerland), EuroCloud (Poland)	France, Germany, Poland, Switzerland	6/27/2013-5/14/2014	Code, Market, Norm, Law	Rest, Meta	Data at rest	High-Medium
Localized routing	Data streams should flow within a geographically restricted zone; inter-Schengen data traffic should be routed within the Schengen zone[91, 92, 93, 94, 95, 96]	Public: German government;Private: Deutsche Telekom, Atos	France, Germany	10/12/2013-7/27/2014	Code, Norm, Law	Motion, Meta	Protocol (Content, Application, Physical)	Medium
Expand encryption tools	End-to-end encryption of communication data; encryption of end devices[97, 98, 99]	Public: European Parliament, Stefan Katzenbeisser (Technische Universität Darmstadt), Mark Manulis	Germany, UK	11/23/2013 - 2/24/2014	Code, Norm, Market	Motion, Rest	Protocol (Content, Application, Physical) + Data at rest	Medium
More-secure encryption standards	Require proof of security and key sizes equivalent to 128-bit symmetric security or more[100]	Public: ENISA	EU	10/31/2013	Law	Motion, Rest	Protocol (Content, Application, Physical) + Data at rest	Medium
Mobile encryption tools	End-to-end mobile voice encryption;[101, 102] secure SIM Data for corporate customers[103]	Private: Thomas Kremer (Deutsche Telekom), Björn Rupp (GSMK)	Germany	9/9/2013 - 3/12/2014	Code	Motion, Rest	Protocol (Content, Application, Physical) + Data at rest	Medium-Low

Non-Technical Proposals

CODING	SUMMARY	PROPOSING ACTORS	COUNTRY OR REGION	TIME RANGE	DIMENSION	DATA TYPE	POLITICAL TRACTION
Companies unable to provide legal guarantee excluded from federal contracts	Exclude any company that cannot guarantee that foreign services or authorities will not obtain any of their data from federal contracts[104]	Public: German government	Germany	3/16/2014	Law	Motion, Rest	High
Shift German government services from foreign to local companies	The German government will shift all services provided by Verizon to Deutsche Telekom[105]	Public: German government	Germany	6/27/2014	Market	N/A	High
EU Data Protection Authority	Establish a single EU Data Protection Authority[106]	Public: Jacob Kohnstamm (Chairman, Dutch Data Protection Agency)	Netherlands	5/8/2014	Law	N/A	High-Medium
EU Data Protection Directive	Establish EU-wide data protection laws, GDPR; conduct a comprehensive review of the legal framework for data protection[107, 108, 109, 110, 111, 112]	Public: Peter Hustinx (European Data Protection supervisor, Jan Philipp Albrecht (Member of the European Parliament), Dimitrios Droutsas (Member of Parliament, Greece), Polish government	Belgium, Germany, Greece, Poland	10/23/2013-3/11/2014	Law	N/A	High-Medium
“IT Security Made in Germany”	Establish an "IT Security Made in Germany" brand[113]	Private: Deutsche Telekom	Germany	1/1/2014	Norm, Market	N/A	High-Medium
Increase funding for small businesses	Improve funding for small businesses to compete with US companies on privacy[114]	Private: Christian Knorst (technology law specialist)	Germany	12/3/2014	Market	N/A	Medium
Safe Harbor agreement reforms	Proposals range from strengthening agreement to suspension of Safe Harbor agreement[115, 116, 117]	Public: EP and EU at EU-US Summit	UK, EU	11/6/2013-3/26/2014	Law	N/A	Medium
Encryption Key Governance	Encryption keys should be held by a public entity, and should be held by a third party, not the cloud service provider[118, 119]	Private: David Hernandez Montesinos (Gloria Transmedia), Gastone Nencini (Trend Micro Italia)	Italy, Spain	11/14/2013-4/29/2014	Law	Motion, Rest	Low
Single committee for all digital issues	Establish one committee responsible for all digital issues[120]	Public: Marietje Schaake (MEP)	Netherlands	5/20/2014	Law	N/A	Low
Legal Code of Conduct between intelligence agencies	Establish rules, transatlantic code of conduct regarding technological spying[121, 122, 123]	Public: Manuel Valls (Prime Minister, France), Wolfgang Ischinger (Chairman, Munich Security Conference), Jean-Claude Juncker (European Commission President)	France, Germany, Luxemburg	10/22/2013-1/20/2014	Law, Norm	N/A	Low
Transparency on government access to data	Explore increased transparency on government access to data in order to rebuild trust[124]	Public: European Commission	EU	10/15/2013	Law, Norm	N/A	Low

Annex 3: OECD Principles

Full OECD Communiqué on Principles for Internet Policy-Making available at:
http://www.oecd.org/internet/innovation/48289796.pdf

Principle 1: Promote and protect the global free flow of information.
Principle 2: Promote the open, distributed, and interconnected nature of the Internet.
Principle 3: Promote investment and competition in high-speed networks and services.
Principle 4: Promote and enable the cross-border delivery of services.
Principle 5: Encourage multi-stakeholder cooperation in policy development processes.
Principle 6: Foster voluntarily developed codes of conduct.
Principle 7: Develop capacities to bring publicly available, reliable data into the policymaking process.
Principle 8: Ensure transparency, fair process, and accountability.
Principle 9: Strengthen consistency and effectiveness in privacy protection at a global level.
Principle 10: Maximize individual empowerment.
Principle 11: Promote creativity and innovation.
Principle 12: Limit Internet intermediary liability.
Principle 13: Encourage cooperation to promote Internet security.
Principle 14: Give appropriate priority to enforcement efforts.

Annex 4: Steering Committee and Workshop Participants

Steering Committee of the Transatlantic Dialogues on Security and Freedom in the Digital Age

Thomas Bagger
Head of Policy Planning, German Federal Foreign Office

Ansgar Baums
Director Corporate Affairs, Hewlett-Packard Germany

Natalie Black
Deputy Director, Office of Cyber Security and Information Assurance, United Kingdom Cabinet Office

Paul Cornish
Oxford Martin Fellow, The Global Cyber Security Capacity Centre; Professor of Strategic Studies, University of Exeter

Myriam Dunn Cavelty
Head of the New Risk Research Unit, Center for Security Studies, ETH Zurich

Martha Finnemore
Professor, George Washington University

Roger Hurwitz
Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT

Gustav Lindstrom
Head of the Emerging Security Challenges Programme, Geneva Center for Security Policy

Kristin Lord
President and CEO, IREX

Cheri McGuire
Vice President, Global Government Affairs & Cyber Security Policy, Symantec Corporation

Joseph Nye
Harvard University Distinguished Service Professor; former Dean of the Kennedy School

Thomas Rid
Professor, King's College London

Marietje Schaake
Member of the European Parliament

Wendy Seltzer
Policy Counsel to the World Wide Web Consortium; Visiting Fellow with Yale Law School's Information Society Project

Ian Wallace
Visiting Fellow in Cybersecurity with the Center for 21st Century Security and Intelligence, Foreign Policy program at the Brookings Institution

Non-Steering Committee Participants of the September 18, 2014 Workshop Hosted at New America

Joanneke Balfoort
Deputy Head, Political Department,
Embassy of the Kingdom of the Netherlands
in Washington, DC

Kevin Bankston
Policy Director, New America's
Open Technology Institute

Thorsten Benner
Director, Global Public Policy Institute

Alan B. Davidson
Director, New America's
Open Technology Institute;
Vice President, New America

Scott Janz
Intern, New America's
Open Technology Institute

Danielle Kehl
Policy Analyst, New America's
Open Technology Institute

Matthew Noyes

Oliver Read
Editor and Communications Manager,
Global Public Policy Institute

Norbert Riedel
Commissioner for International Cyber Policy,
German Federal Foreign Office

Marion van Ruiten
Political Officer, Political Department,
Embassy of the Federal Republic of Germany,
United States

Anne-Marie Slaughter
President and CEO, New America

Dan Staples
Associate Technologist, New America's
Open Technology Institute

References

1 German Government. 2013. “Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode.” <http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=2820F3157BAD69B7313E63020CF9944C.s4t2?__blob=publicationFile&v=2>.

2 The Brookings Institution. 2014. “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” *The Brookings Institution*. Oct. 16. <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi>; Street, Jon. 2014. “Eric Holder: Apple, Google Not Giving Law Enforcement Access to Encrypted Data Is ‘Worrisome.’” *The Blaze*. Oct. 1. <http://www.theblaze.com/stories/2014/10/01/eric-holder-apple-google-not-giving-law-enforcement-access-to-encrypted-data-is-worrisome/>; Hosko, Ronald T. 2014. “Apple and Google’s new encryption rules will make law enforcement’s job much harder.” *The Washington Post*. Sept. 23. <http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/>.

3 German Government. 2013. “Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode.” <http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=2820F3157BAD69B7313E63020CF9944C.s4t2?__blob=publicationFile&v=2>.

4 Built Invisible. 2014. “Messages in the Deep: The Remarkable Story of the Underwater Internet.” *Built Invisible*. <http://builtvisible.com/messages-in-the-deep/>.

5 German Government. 2014. “Digitale Agenda 2014 – 2017.” *Die Bundesregierung*. p. 4. <http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf>.

6 The Schengen area is the border-free zone shared among 26 countries in Europe. For more information, see: European Commission Home Affairs. 2013. “Schengen Area.” *European Commission*. <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm>.

7 Mari, Angelica. 2014. “High expectations for Brazil undersea cable to Europe.” *ZDNet*. Feb. 12. <http://www.zdnet.com/high-expectations-for-brazil-undersea-cable-to-europe-7000026264/>.

8 Finish Ministry of Transport and Communications. 2014. “Minister Kiuru on Submarine Cable Decision: Finland to be a Safe Harbour for Data.” *Finish Ministry of Transport and Communications*. May 20. <http://www.lvm.fi/pressreleases/4402744/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data>; The Local. 2013. “Swedish spies ‘breaking surveillance laws.’” The Local. Sept. 9. <http://www.thelocal.se/20130909/50134>; Wittes, Benjamin. 2013. “Mark Klamberg on EU Metadata Collection.” Lawfare Blog. Sept. 29. <http://www.lawfareblog.com/2013/09/mark-klamberg-on-eu-metadata-collection/>.

9 Chander, Anupam and Uyen P. Le. 2014. “Breaking the Web: Data Localization vs. the Global Internet.” UC Davis Legal Studies Research Paper No. 378; Hill, Jonah Force. 2014. “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders.” Lawfare Research Paper Series 2, no. 3. <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>.

10 Polatin-Reuben, Dana and Joss Wright. 2014. “An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet.” USENIX. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

11 A comprehensive list of proposals can be found in Annex 1I.

12 Chander, Anupam and Uyen P. Le. 2014. “Breaking the Web: Data Localization vs. the Global Internet.” *UC Davis Legal Studies Research Paper No. 378*; Hill, Jonah Force. 2014. “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders.” *Lawfare Research Paper Series 2, no. 3.* <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>; Polatin-Reuben, Dana and Joss Wright. 2014. “An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet.” *USENIX*. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

13 Chander, Anupam and Uyen P. Le. 2014; Hill, Jonah Force. 2014.

14 New America. 2014. “Digital Borders and Technological Sovereignty: Breaking or Saving the Internet as We Know It?” *New America*. Sept. 19. <http://www.newamerica.net/events/2014/digital_borders_and_technological_sovereignty>.

15 The Broadband Commission for Digital Development. 2014. “The state of Broadband in 2014: broadband for all.” *Broadband Commission Report*. < http://www.broadbandcommission.org/Documents/reports/bb-annualreport2014.pdf>

16 DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press, p. 9.

17 van Schewick, Barbara. 2010. *Internet Architecture and Innovation*. Cambridge: MIT Press.

18 The Safe Harbor agreement is the process developed by the US Department of Commerce that allows US companies to more easily comply with EU Directive 95/46/EC, the initial EU Data Protection Directive from 1998. When the directive went into force in 1998, "it became clear that it actively threatened data flows between the two largest trading partners on earth." Thus, the Safe Harbor agreement, which is unique to the US and EU, is "voluntary self-certification system for transmitting data from the EU to the United States." For more on the Safe Harbor, see: Dowling, Jr., Donald C. 2009. "International Data Protection and Privacy Law." White & Case. p. 12. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

19 O'Donnell, John and Baker, Luke. 2013. "Germany, France demand 'no-spy' agreement with U.S." Reuters. Oct. 24. <http://www.reuters.com/article/2013/10/25/us-eu-summit-idUSBRE99N0BJ20131025>.

20 Bloomberg News. 2014. "German government cancels Verizon Communications Inc deal in wake of NSA spy scandal." *Financial Post Tech Desk*. June 27. <http://business.financialpost.com/2014/06/27/german-government-cancels-verizon-communications-inc-deal-in-wake-of-nsa-spy-scandal/?__lsa=512f-ffa4>.

21 TaylorWessing. 2014. "When will there be a new EC data protection Regulation?" *TaylorWessing*. Nov. <http://www.taylorwessing.com/globaldatahub/article_2014_ec_regulation.html>.

22 Bundesverband IT-Mittelstand. 2012. "Software Made in Germany." *Bundesverband IT-Mittelstand*. <http://www.software-made-in-germany.org/>; *European Parliament*. 2014. "Motion for a European Parliament Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." European Parliament. Feb. 21. Paragraph 97. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

23 Emmot, Robin. 2014. "Brazil, Europe plan undersea cable to skirt U.S. spying." Reuters. Feb. 24. <http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224>; Nielsen, Nikolaj. 2014. "Brazil champions undersea cable to bypass US." *EUObserver*. Feb. 14. <http://euobserver.com/justice/123260>.

24 Heise Online. 2014. "E-Mail made in Germany: Vollständig umgesetzt, dennoch unzureichend." Apr. 29. <http://www.heise.de/netze/meldung/E-Mail-made-in-Germany-Vollstaendig-umgesetzt-dennoch-unzureichend-2179269.html>.

25 Ibid.

26 European Commission. 2014. "Cloud Service Level Agreement Standardisation Guidelines". <https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>.

27 European Cloud Partnership Steering Board. 2014. "Establishing a Trusted European Cloud." <http://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/Report-Establishing-trusted-cloud-Europe.pdf>.

28 In January 2014, IBM announced that it would invest more than $1 billion in the construction of 15 new data centers around the world, but the only European data center was to be constructed in the UK. Salesforce.com, conducted a similar initiative, but only in the UK. In September, Oracle announced that it would open two data centers in Germany for German companies that would like to store their data in Germany. With its "Cloud 28+" initiative, Hewlett Packard called for a common Cloud space for Europe. Similarly, Microsoft Germany announced that it was planning to develop Cloud technology that would be offered only within Germany. It wants data to be kept within Germany's own borders and hosted by a data center, which would be subject to German or European law. For more on this story, see: *Deutsche Welle*. 2014. "While NSA 'maps' the Internet landscape, German tech companies want Cloud cover." Deutsche Welle. Sept. 14. <http://www.dw.de/while-nsa-maps-the-internet-landscape-german-tech-companies-want-cloud-cover/a-17921351>.

29 Waidner, Michael. 2014. "Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014." June 26. <https://www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf>.

30 European Parliament. 2014. "Motion for a European Parliament Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." *European Parliament*. Feb. 21. Paragraph 95. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

31 Vance Jr., Cyrus R. 2014. "Apple and Google threaten public safety with default smartphone encryption." *The Washington Post*. Sept. 26. <http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html>.

32 Jackson Higgins, Kelly. 2013. "NSA Leaks Bolster IETF Work On Internet Security." *DarkReading*. Nov. 14. <http://www.darkreading.com/risk/nsa-leaks-bolster-ietf-work-on-internet-security/d/d-id/1140891>.

33 Greis, Friedhelm. 2014. "Telekom dementiert Abschaffung des Merkel-Handys." *Golem.de*. Oct. 8. <http://www.golem.de/news/simko-3-telekom-dementiert-abschaffung-des-merkelphones-1410-109703.html>.

34 Epstein, Jennifer. 2014. “U.S. doesn’t have ‘no-spy agreement’ with foreign countries, Obama says.” *Politico*. Feb. 11. <http://www.politico.com/story/2014/02/nsa-spying-foreign-countries-103382.html>; Oltermann, Philip. 2014. “US will not enter bilateral no-spy deal with Germany, reports media.” *The Guardian*. Jan. 14. <http://www.theguardian.com/world/2014/jan/14/us-not-entering-no-spy-agreement-germany-media>.

35 Deutsche Telekom. 2013. “Deutsche Telekom, WEB.DE and GMX launch ‘E-mail made in Germany’ initiative.” *Deutsche Telekom Media*. Aug. 9. <http://www.telekom.com/media/company/192834>.

36 European Council: The President. 2014. “Press Statement by the President of the European Council, Herman Van Rompuy, following the 7th EU-Brazil Summit.” *The European Council*.<http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/141144.pdf>.

37 Ronnholm, Antton. 2014. “Minister Kiuru on submarine cable decision: Finland to be a safe harbor for data.” *Finnish Ministry of Transport and Communications*. Apr. 20. <http://www.lvm.fi/pressreleases/4402744/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data>.

38 Iwankiewicz, Maciej W. 2013. “The Polish Approach to EU Cloud Computing Strategy.” *EuroCloud*. July 5. <http://www.eurocloud.org/the-polish-approach-to-the-eu-cloud-computing-strategy/>.

39 Deutscher Bundestag. 2013. “Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.” *German Bundestag*. Nov. 15. <http://dip21.bundestag.de/dip21/btd/18/000/1800059.pdf>.

40 Juskailian, Russ. 2014. “For Swiss Data Industry, NSA Leaks Are Good as Gold: here’s how the Swiss promise to keep your data safe.” *Technology Review*. Mar. 18. <http://www.technologyreview.com/news/525546/for-swiss-data-industry-nsa-leaks-are-good-as-gold/>.

41 Le Maire, Bruno. 2014. “Bruno Le Maire: Pour un Cloud europeen.” *Slate*. May 14. <http://www.slate.fr/tribune/87057/bruno-le-maire-cloud-europeen>.

42 Berke, Jürgen. 2013. “Telekom will innerdeutschen Internetverkehr ubers Ausland stoppen.” *Wirtschafts Woche*. Oct. 12. <http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html>.

43 Schäfer, Louisa. 2013. “Deutsche Telekom: ‘Internet data made in Germany should stay in Germany.’ Interview with Philipp Blank.” *Deutsche Welle*. Oct. 18. <http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891>.

44 Gaugele, Von Jochen, Kade, Claudia, Malzahn, Claus Christian and Vitzthum, Thomas. 2014. “Dobrindt will mit ‘Netzallianz’ an die Weltspitze.” *Die Welt*. Jan. 12. <http://www.welt.de/politik/deutschland/article123774038/Dobrindt-will-mit-Netzallianz-an-die-Weltspitze.html>.

45 Thombansen, Hannah. 2014. “Video-Podcast der Bundeskanzlerin #2/2014.” *Bundesregierung*. Feb. 15. <http://www.bundesregierung.de/Content/DE/Podcast/2014/2014-02-15-Video-Podcast/links/download-PDF.pdf;jsessionid=0BC9A500E8D948E37C285341160692B2.s4t1?__blob=publicationFile&v=3>.

46 Breton, Thierry. 2013. “Atos CEO calls for ‘Schengen for data.” *Thierry Breton’s blog*. Sept. 2. <http://www.thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html>.

47 von Altenbockum, Jasper und Lohse, Eckart. 2014. “Verfassungsschutz-Präsident ‘Wir werden unsere Abwehr verstärken.’” *Frankfurter Allgemeine Zeitung*. July 28. <http://www.faz.net/aktuell/politik/inland/interview-mit-hans-georg-maassen-abwehr-verstaerken-13067331.html>.

48 OECD. 2011. “Communiqué on Principles for Internet Policy-Making.” *OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth*. June 29. p. 3. <http://www.oecd.org/internet/innovation/48289796.pdf>.

49 Ibid.

50 E-mail Made in Germany. 2014. “E-mail made in Germany.” *E-mail made in Germany.* <http://www.e-mail-made-in-germany.de/>.

51 Dierks, T. and E. Rescorla. 2008. “The Transport Layer Security (TLS) Protocol Version 1.2.” *Internet Engineering Task Force Network Working Group*. <http://tools.ietf.org/html/rfc5246>.

52 Vaughn-Nichols, Steven J. 2013. “How the NSA, and your boss, can intercept and break SSL.” June 8. <http://www.zdnet.com/how-the-nsa-and-your-boss-can-intercept-and-break-ssl-7000016573/>.

53 Dowling, Jr., Donald C. 2009. “International Data Protection and Privacy Law.” *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

54 Deutsche Telekom. 2013. “Data Privacy and Security Report.” 2013. p. 4-5; p. 12-13. <http://e-paper.telekom.com/data-privacy-report-2013/#/2>; Claus, Ulrich. 2014. “So würde Europas Schengen-Internet funktionieren.” *Die Welt*. Mar. 31.<http://www.welt.de/politik/deutschland/article126343060/So-wuerde-Europas-Schengen-Internet-funktionieren.html>.

55 Beuth, Patrick. 2013. “Telekom denkt über deutsches Internet nach.” *Zeit Online*. Oct. 14. <http://www.zeit.de/digital/internet/2013-10/telekom-national-routing>.

56 Dowling, Jr., Donald C. 2009. "International Data Protection and Privacy Law." *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

57 Jonah Hill (2014), p.3; Chander, Anupam and Le, Uyen P. 2014. "Breaking the Web: Data Localization vs. the Global Internet." *Emory Law Journal*. April 23. <http://ssrn.com/abstract=2407858>.

58 Bob Butler, Irving Lachow, Jonah Force Hill. 2014. "Cloud computing under siege." *Few.com*. Sept. 12. <http://fcw.com/articles/2014/09/12/cloud-under-siege.aspx>; European Cloud Partnership Steering Board. 2014. "Establishing a Trusted European Cloud." p.19.<http://www. kowi.de/Portaldata/2/Resources/horizon2020/coop/Report-Establishing-trusted-cloud-Europe.pdf>.

59 The European Commission. 2011. "European Union-United States Trade Principles for Information and Communication Technology Services." *The European Commission*. <http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf>.

60 Plaum, Alexander. 2014. "The impact of forced data localisation on fundamental rights." *Access Now*. April 4.. <https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights>.

61 Protalinski, Emil. 2014. "Gmail now always uses an HTTPS connection and encrypts all messages moving internally on Google's servers." *The Next Web*. Mar. 20. <http://thenextweb.com/google/2014/03/20/gmail-now-uses-encrypted-https-connection-check-send-email/>; Armasu, Lucian. 2014. "Huge: Cloudflare's Free SSL Service Brings Encrypted-By-Default Web Closer Than Ever." *Tom's Hardware*. Sept. 29. <http://www.tomshardware.com/news/cloudflare-security-encryption-ssl-https,27780.html>; Perey, Juan Carlos. 2014. "Microsoft makes email encryption for Office 365 easier." *Tech Central.ie*. Oct. 6. <http://www.techcentral.ie/microsoft-makes-email-encryption-office-365-easier/#ixzz3Ix0eOXHl>; O'Neill, Patrick Howell. 2014. "Tor executive director hints at Firefox integration." *The Daily Dot*. Sept. 29. <http://www.dailydot.com/politics/tor-mozilla-firefox/>; Meyer, David. 2014. "Pretty Easy Privacy project aims to make encryption easier for regular people to use." *Gigaom*. Oct. 6. <https://gigaom.com/2014/10/06/pretty-easy-privacy-project-aims-to-make-encryption-easier-for-regular-people-to-use/>.

62 Peterson, Andrea. 2014. "Privacy is tech's latest marketing strategy." *The Washington Post*. Sept. 26. <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/26/privacy-is-techs-latest-marketing-strategy/>.

63 Schneier, Bruce. 2014. "Stop the hysteria over Apple encryption." *CNN*. Oct. 31. <http://edition.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/>.

64 Deutsche Telekom. 2013. "Data Privacy and Security Report." p. 4-5; p. 12-13. <http://e-paper.telekom.com/data-privacy-report-2013/#/2>; Infineon. 2014. "Data Security is a Prerequisite for Succesful 'Industrie 4.0' Implementation: Infineon and Deutsche Telekom Demonstrate Security Technology 'Made in Germany' at IT Summit 'Nationaler IT-Gipfel 2014.'" <https://www.infineon.com/cms/en/about-infineon/press/press-releases/2014/INFCCS201410-002.html>.

65 Timberg, Craig. 2014. "Police want back doors in smartphones, but you never know who else will open them." *The Washington Post*. Oct. 2. <http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/02/police-want-back-doors-in-smartphones-but-you-never-know-who-else-will-open-them/>.

66 Rinke, Andreas. 2013. "Europa träumt vom IT-Airbus." *N-TV*. Aug. 11. <http://www.n-tv.de/wirtschaft/Die-Folgen-des-NSA-Skandals-Europa-blaest-zur-IT-Aufholjagd-article11151961.html>; Deutsche Wirtschaft Nachrichten. 2013. "Politische Idee eines IT-Riesen in Europa ist Unsinn." Nov. 28. <http://deutsche-wirtschafts-nachrichten.de/2013/11/28/sap-politische-idee-eines-it-riesen-in-europa-ist-unsinn>.

67 Tiezzi, Shannon. 2014. "In Cyber Dispute With US, China Targets IBM, Cisco." *The Diplomat*. May 28. <http://thediplomat.com/2014/05/in-cyber-dispute-with-us-china-targets-ibm-cisco/>.

68 Rogers, Mike and Dutch Ruppersberger. 2012. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Permanent Select Committee on Intelligence. Oct. 8. <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf>.

69 Intelligence and Security Committee. 2013. "Foreign Involvement in the Critical National Infrastructure: The Implications for National Security." UK: TSO Ltd., p. 4; BBC News UK. 2011. "GCHQ Chief Reports 'Disturbing' cyber-attacks on UK." BBC.com. Oct. 31. <http://www.bbc.com/news/uk-15516959>.

70 Intelligence and Security Committee. 2013. *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security*. UK: TSO Ltd.; Sir Darroch, Kim. 2013. A *Review by the National Security Adviser on the Operation of the Huawei Cyber Security Evaluation Centre (HCSEC)*. National Security Adviser. Dec. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266487/HCSEC_Review_Executive_Summary_FINAL.PDF>.

71 Lessig, Lawrence. 2006. "Code v2." p. 124. <http://codev2.cc/>.

72 Ibid.

73 Ibid.

74 Ibid.

75 Ibid.

76 Lessig, Lawrence. 1998. "The Laws of Cyberspace." *Presented at the Taiwan Net '98 Conference*. p. 4.

77 Ibid.

78 National Information Standards Organization. 2004. *Understanding Metadata*. NISO Press, p. 1-2. <http://marciazeng.slis.kent.edu/metadatabasics/types.htm>.

79 Ibid.

80 Zittrain, Jonathan L. 2008. *The Future of the Internet – And How to Stop It*. New Haven: Yale University Press, Chapter 4, p. 67-100.

81 Ibid.

82 Ibid.

83 Ibid.

84 Deutsche Telekom. 2013. "Deutsche Telekom, WEB.DE and GMX launch 'E-mail made in Germany' initiative." *Deutsche Telekom Media*. Aug. 9. <http://www.telekom.com/media/company/192834>.

85 European Council: The President. 2014. "Press Statement by the President of the European Council, Herman Van Rompuy, following the 7th EU-Brazil Summit." *The European Council*.<http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/141144.pdf>.

86 Ronnholm, Antton. 2014. "Minister Kiuru on submarine cable decision: Finland to be a safe harbor for data." *Finnish Ministry of Transport and Communications*. Apr. 20. <http://www.lvm.fi/pressreleases/4402744/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data>.

87 Iwankiewicz, Maciej W. 2013. "The Polish Approach to EU Cloud Computing Strategy." *EuroCloud*. July 5. <http://www.eurocloud.org/the-polish-approach-to-the-eu-cloud-computing-strategy/>.

88 Deutscher Bundestag. 2013. "Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit." *German Bundestag*. Nov. 15. <http://dip21.bundestag.de/dip21/btd/18/000/1800059.pdf>.

89 Juskailian, Russ. 2014. "For Swiss Data Industry, NSA Leaks Are Good as Gold: here's how the Swiss promise to keep your data safe." *Technology Review*. Mar. 18. <http://www.technologyreview.com/news/525546/for-swiss-data-industry-nsa-leaks-are-good-as-gold/>.

90 Le Maire, Bruno. 2014. "Bruno Le Maire: Pour un Cloud europeen." *Slate*. May 14. <http://www.slate.fr/tribune/87057/bruno-le-maire-cloud-europeen>.

91 Berke, Jürgen. 2013. "Telekom will innerdeutschen Internetverkehr ubers Ausland stoppen." *Wirtschafts Woche*. Oct. 12. <http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html>.

92 Schäfer, Louisa. 2013. "Deutsche Telekom: 'Internet data made in Germany should stay in Germany.' Interview with Philipp Blank." *Deutsche Welle*. Oct. 18. <http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891>.

93 Gaugele, Von Jochen, Kade, Claudia, Malzahn, Claus Christian and Vitzthum, Thomas. 2014. "Dobrindt will mit 'Netzallianz' an die Weltspitze." *Die Welt*. Jan. 12. <http://www.welt.de/politik/deutschland/article123774038/Dobrindt-will-mit-Netzallianz-an-die-Weltspitze.html>.

94 Thombansen, Hannah. 2014. "Video-Podcast der Bundeskanzlerin #2/2014." *Bundesregierung*. Feb. 15. <http://www.bundesregierung.de/Content/DE/Podcast/2014/2014-02-15-Video-Podcast/links/download-PDF.pdf;jsessionid=0BC9A500E8D948E37C285341160692B2.s4t1?__blob=publicationFile&v=3>.

95 Breton, Thierry. 2013. "Atos CEO calls for 'Schengen for data.'" *Thierry Breton's blog*. Sept. 2. <http://www.thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html>.

96 von Altenbockum, Jasper and Lohse, Eckart. 2014. "Verfassungsschutz-Präsident 'Wir werden unsere Abwehr verstärken.'" *Frankfurter Allgemeine Zeitung*. July 28. <http://www.faz.net/aktuell/politik/inland/interview-mit-hans-georg-maassen-abwehr-verstaerken-13067331.html>.

97 European Parliament. 2014. "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." Feb. 21. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

98 Ward, Mark. 2014. "Can Europe go its own way on data privacy?" *BBC Technology*. Feb. 17. <http://www.bbc.com/news/technology-26228176>.

99 Schutz, Colin. 2014. "Tech Companies Are Trying to Make NSA-Proof Encrypted Phones and Apps." *Smithsonian Magazine*. Feb. 24. <http://www.smithsonianmag.com/smart-news/tech-companies-are-responding-nsa-revelations-encrypted-phones-and-apps-180949874/?no-ist>.

100 ENISA. 2013. *Algorithms, Key Sizes and Parameters Report*. European Union Agency for Network and Information Security Agency. Oct. 29. <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report>.

101 Sawall, Achim. 2013. "Simko 3 zugelassen." *Golem.de*. Sep. 9. <http://www.golem.de/news/simko-3-zugelassen-hintertueren-lassen-sich-bei-smartphones-nicht-ausschliessen-1309-101467.html>.

102 Deutsche Telekom. 2013. "Data Privacy and Data Security: Report 2013." *Deutsche Telekom AG*. <http://www.telekom.com/dataprotection>.

103 Gandhe, Shreyas. 2014. "Vodafone Germany starts rolling out SIM card based encryption." *Neowin.net*. Mar. 12. <http://www.neowin.net/news/vodafone-germany-starts-rolling-out-sim-card-based-encryption>.

104 Obermaier, Frederik and Struz, Benedikt. 2014. "German Plans to Ban Tech Companies That Play Ball With NSA." *Sueddeutsche.de*. May 16. <http://international.sueddeutsche.de/post/85917094540/germany-plans-to-ban-tech-companies-that-play-ball-with>.

105 Bloomberg News. 2014. "German government cancels Verizon Communications Inc deal in wake of NSA spy scandal." *Financial Post Tech Desk*. June 27. <http://business.financialpost.com/2014/06/27/german-government-cancels-verizon-communications-inc-deal-in-wake-of-nsa-spy-scandal/?__lsa=512f-ffa4>.

106 Out-law.com. 2014. "Dutch regulator questions likelihood of June agreement on data protection reforms." <http://www.out-law.com/en/articles/2014/may/dutch-regulator-questions-likelihood-of-june-agreement-on-data-protection-reforms-/>.

107 Pfeifle, Sam. 2013. "Data Protection and Privacy Commissioners Release Resolutions on Tracking, Profiling, International Cooperation." *Privacy Association*. Sept. 25. <https://privacyassociation.org/news/a/data-protection-and-privacy-commissioners-release-resolutions-on-tracking-p/>.

108 European Pariliament. 2014. "Data protection: 'Be careful who you trust, exercise your rights, ask questions.'" *European Parliament News*. Jan. 28. <http://www.europarl.europa.eu/news/en/news-room/content/20140127STO33808/html/Data-protection-Be-careful-who-you-trust-exercise-your-rights-ask-questions>.

109 European Parliament. 2013. "Interview: bringing data protection rules up to date." *European Parliament News*. Nov. 3. <http://www.europarl.europa.eu/news/en/news-room/content/20140310STO38525/html/Interview-bringing-data-protection-rules-up-to-date>.

110 European Parliament. 2013. "Interview: bringing data protection rules up to date." *European Parliament News*. Nov. 3. <http://www.europarl.europa.eu/news/en/news-room/content/20140310STO38525/html/Interview-bringing-data-protection-rules-up-to-date>.

111 The Council of the European Union. 2014. "Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data." *The Council of the European Union*. May 28. <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT>.

112 Ministry of Administration and Digitization, Poland. *Polish contribution on Digital Agenda ahead of the European Council of 24-25 October 2013*. Government of Poland. Oct. 23. <https://mac.gov.pl/files/wp-content/uploads/2013/10/Polish-contribution-on-Digital-Agenda.pdf>.

113 Deutsche Telekom. 2014. *Data Privacy and Data Security: Report 2013*. Deutsche Telekom AG. p. 11. <http://www.telekom.com/dataprotection>.

114 Out-law.com. 2013. "European 'IT Airbus' could lead to competition concerns, says expert." *Out-law.com*. Dec. 3. <http://www.out-law.com/articles/2013/december/european-it-airbus-could-lead-to-competition-concerns-says-expert/>.

115 Council of the European Union. 2014. *EU-US Summit Joint Statement*. Council of the European Union. Mar. 26. <http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/141920.pdf>.

116 External relations. "Moraes: EP is looking not only into NSA allegations but also at EU's own backyard." *European Parliament News*. Nov. 6. <http://www.europarl.europa.eu/news/en/news-room/content/20131106STO23912/html/Moraes-EP-looks-not-only-into-NSA-allegations-but-also-at-EU%27s-own-backyard>.

117 Departament Spoleczenstwa Informacyjnego, Poland. "Analiza Program 'Bezpieczna Przystan' ('Safe Harbour')." *Ministry of Administration and Digitization, Government of Poland*. Apr. 10. <https://mac.gov.pl/files/raport_ewaluacyjny_stosowania_programu_safe_harbour_-_dsi_mac.pdf>.

118 Martin, Javier. 2013. "Buscando un guardian para la nube." El Pais Sociedad. Nov. 14. <http://sociedad.elpais.com/sociedad/2013/11/14/actualidad/1384383731_820058.html>.

119 Badalucco, Giuseppe. 2014. "La sfida del cloud dopo il datagate." *Data Manager Online*. Apr. 29. <http://www.datamanager.it/rivista/la-sfida-del-cloud-dopo-il-datagate-55515.html>.

120 Schaake, Maritje. 2014. "European Parliament should create a Committee on Digital Affairs." *MarietjeSchaake.eu*. May 20. <http://www.marietjeschaake.eu/2014/05/european-parliament-should-create-a-committee-on-digital-affairs/>.

121 Zeit Online. 2014. "Juncker für verbindliches No-Spy-Abkommen." *Zeit Online*. Jan. 21. <http://www.zeit.de/news/2014-01/21/geheimdienste-juncker-fuer-verbindliches-no-spy-abkommen-21112007>.

122 To the Tick. 2013. "France Summons US Ambassador in Snowden Affair." *To the Tick*. Oct. 21. <http://www.tothetick.com/france-summons-us-ambassador-in-snowden-affair>.

123 Deutsche Telekom. 2014. *Data Privacy and Data Security: Report 2013*. Deutsche Telekom AG. <http://www.telekom.com/dataprotection>.

124 Heath, Ryan. 2013. "What does the Commission mean by secure Cloud computing services in Europe?" *European Commission Memo*. Oct. 15. <http://europa.eu/rapid/press-release_MEMO-13-898_en.htm>.

www.digitaldebates.org