Prague SECONOMICS Discussion Papers
2013/7

Drawing the line between security and privacy. An analysis of security discourses in the US press, 2010-2013

Contribution to the SECONOMICS project and
Prague Graduate School in Comparative Qualitative Analysis 2013

Nikola Belakova

London School of Economics

Institute of Sociology
Academy of Sciences of the Czech Republic
Prague, December 2013

Editorial Board: Zdenka Mansfeldová, Petra Guasti, Jessie Hronešová
Copy-editing: Andrew Korb
Published by: Institute of Sociology, AS CR
Jilská 1, 110 00 Prague 1
Prague 2013

Contact: Press and Publications Department
Institute of Sociology, AS CR
Jilská 1, 110 00 Prague 1
tel.: 210 310 217
e-mail: prodej@soc.cas.cz

This publication has been completed with funding from project SECONOMICS: Socio economics meets security, an Integrated Project supported by the European Commission's Seventh Framework Programme for Research, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT.

ISBN 978-80-7330-243-6

SECONOMICS Consortium

SECONOMICS "Socio-Economics meets Security" (Contract No. 285223) is a Collaborative project) within the 7th Framework Programme, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT. The consortium members are:

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESSCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Prof. Julian Williams julian.williams@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Silvia Castellvi Catala silvia.castellvi@atosresearch.eu
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr Robert Coles Robert.S.Coles@ngrid.com
11	ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr

In this discussion paper series, the Prague *SECONIMICS* team intends to allow the broader academic community taking part in an on-going discussion about risks and threats as well as trade-offs between them and security. This research focus stems from the fact that until now, social scientists have primarily studied threats and risks through the perspective of social psychology by conducting the so-called "risk assessment" analyses, especially looking at the concept of "risk perception". This research thus aims to probe these concepts in order to broaden our understanding of the multivariate study of risks and threats in social sciences by adding some context-dependent and temporal aspects.

Table of contents

1. Introduction

Recently, leading international media uncovered the US and UK intelligence agencies' covert efforts to undermine Internet security. The investigative reports based on secret documents leaked by Edward Snowden and published by the *Guardian, New York Times, and ProPublica*, have confirmed the suspicions of independent security experts that the US National Security Agency (NSA) has been undermining Internet security standards. Millions of people use email, online banking, and have their medical records stored online. All of those services have now been compromised, allowing the spy agencies to gather private information that many of us have deemed sacred. Such intrusion into our privacy has reportedly been done in the name of counter-terrorism and foreign intelligence gathering. These revelations have once again highlighted our vulnerability when using the latest technologies. The reports have also underscored how often modern societies are faced with the dilemma of where to draw the line between privacy and security.

The story brought to light another, perhaps less apparent issue. Concluding its report, the *Guardian* wrote that "intelligence officials asked the *Guardian, New York Times* and *ProPublica* not to publish this article, saying that it might prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read." The three news organisations responded by removing some "specific facts but decided to publish the story because of the value of a public debate about government actions that weaken the most powerful tools for protecting the privacy of internet users in the US and worldwide".[1] These last few sentences highlight the power the news media have over public opinion and public debate. The news is a construct. It is not, as some journalists like to say, a mirror held up to reality' (Patterson 2000, 241). What information media organisations select thus considerably influences how informed the public is about specific security threats and government policies and their impact for society and them individually.

This report explores the coverage of three security-related issues in US news media between 2010 and 2013 as part of a larger endeavour to better understand the role the press plays in shaping the public's views about security risks and the related trade-offs. This research was conducted within the framework of the SECONOMICS 'Socio-Economics meets Security' project. SECONOMICS investigates the trade-offs between security and possible restrictions of personal liberties considered from the perspective of individuals and their acceptance of adopted measures. This report is a direct product of the SECONOMICS Graduate School **in Comparative Qualitative Analysis** that took place in Prague between 13

[1]Ball, James, Julian Borger and Glenn Greenwald. 2013. "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security." *Guardian*, 5 September 2013. Web. Accessed 13 September 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

and 18 May 2013. The Graduate School explored the role of the media and social media in influencing citizen's risk perception and attitudes in a comparative perspective. The resulting national reports, which analyzed the press coverage of 3D body scanners, Stuxnet, and CCTV cameras, examined these topics using qualitative textual analysis. This report first introduces the US news media landscape. It then outlines the methodology employed and puts the US case study into context of recent security threats the country faced. After discussing the findings of the qualitative data analysis of US newspapers, this report presents some tentative conclusions about the role media coverage has played in the public discussions about the security-privacy dilemma in the US.

2. Media landscape in the United States

To better understand the media coverage of our selected topics, it is vital to assess it in the context of the US media environment. The US media have been characterised as being 'among the freest' and 'most commercial' in the world (Patterson 2000, 244).[2] The core guarantee of freedom of speech and the press is provided by the US Constitution's First Amendment, which was inspired by fear that government could utilise the press 'to suppress opposition and maintain itself in power' (Graber and Holyk 2011). The founding fathers of the United States believed that the media could not perform their democratic functions properly unless they were free from government control of news content. While press freedom has come under pressure at various times in the country's history, the right of journalists to be free of state control has been upheld and expanded by numerous court decisions. Beginning with the seminal judgment in *The New York Times v. Sullivan* (1964), requiring officials to prove 'actual malice' on the part of the press (see e.g. Patterson 2000, 242), the courts have granted the media an extensive protection from libel and defamation suits that involve commentary on public figures.[3]

The media are also 'almost completely free of government censorship.' National security interests can be a reason for restriction. The burden of proof, however, lies on the government (Patterson 2000, 242). In *The New York Times v. United States* (1971) the Supreme Court ruled that unless the government can provide compelling reasons for

[2]Between 2010 and 2013, the Freedom House Freedom of the Press Index rated the US press as 'free' with scores between 17 and 18 points. In this period, the US thus ranked between the 17th and 24th country in the world in terms of press freedom. The Freedom of the Press Index classifies the media as "Free," "Partly Free," or "Not Free." States scoring 0 to 30 are considered as having "Free" media; 31 to 60, "Partly Free" media; and 61 to 100, "Not Free" media. See Freedom House. 2013. "Freedom of the Press." Accessed 20 August, 2013. http://www.freedomhouse.org/report-types/freedom-press.

[3]Freedom House. 2013. "Freedom of the Press 2013 – United States." Web. Accessed 20 August 2013. http://www.freedomhouse.org/report/freedom-press/2013/united-states.

restriction, 'any system of prior restraints' on the press is unconstitutional. The Court decided that the Department of Justice, claiming it wanted to prevent harm to the war effort, could not block the publication of the Pentagon Papers (illegally obtained secret government documents revealing official deception about the progress of the Vietnam War). Until recently, one 'exception to judicial support for press freedom' included requests by prosecutors for information gathered by journalists, including material from confidential sources. As a result of this exception, several reporters who refused to identify sources ended up in prison for contempt of court.[4] One of the most widely publicised examples of this in recent years involved James Risen, a prize-winning *New York Times* journalist and author of several books about national security issues. The Justice Department has repeatedly sought to make Risen testify about information he may have received from a former Central Intelligence Agency (CIA) employee, while researching a book about the US efforts to disrupt the Iranian nuclear programme. The Department's attempts were restricted by a 2011 federal court decision, which stated that journalists are not to be called before grand juries unless the government has exhausted other means to gather the information in question, or if sufficient material for indictment has already been acquired,[5] restricting the exception.

Generally, the role of the state is relatively limited. State regulation of content tends to be minimal[6] with specific rules governing each industry. There are no industry-wide self-regulatory organisations in the US ((Hallin and Mancini 2004, 222–4). The print press sector is the least regulated with no rules prescribing specific content, as that would go against press freedom (Graber and Holyk 2011). Under federal law, radio and television airwaves are public property leased to private broadcasters, which decide on the content of programmes.[7] The Federal Communications Commission (FCC) regulates radio and television broadcasting, administering licenses and reviewing content to ensure it complies with legal requirements in relation to public service and local programming, or regarding limits on indecent or offensive material. Nonetheless, the FCC has been characterized as 'very superficial in its scrutiny of station performance' (Graber and Holyk 2011), and as implementing 'regulation by raised eyebrow' in the sense that it has shied away from issuing specific directives on programming (Hallin and Mancini 2004, 230). This hands-off attitude towards media policy 'reflects the belief that diverse owners will produce a broad array of views, sustaining a sound democracy' (Graber and Holyk 2011).

The US news media sector is largely privately owned with a relatively high ownership

[4]Freedom House. 2010. "Freedom of the Press 2010 – United States." Web. Accessed 20 August 2013. http://www.freedomhouse.org/report/freedom-press/2010/united-states.

[5]Freedom House. 2013. "Freedom of the Press 2013 – United States." Web. Accessed 20 August 2013. http://www.freedomhouse.org/report/freedom-press/2013/united-states.

[6]Ibid.

[7]Ibid.

concentration.[8] The authorities have kept small fragments of the radio and television spectra for public broadcasting in the effort to compensate for the shortcomings of privately controlled broadcast media (Graber and Holyk 2011). The Public Broadcasting Act of 1967 established the Public Broadcasting Service (PBS) for television, as well as National Public Radio (NPR) to focus on unprofitable programming neglected by private broadcasters, such as educational programmes. However, public broadcasting 'has remained weak by comparative standards' (Hallin and Mancini 2004, 229) since the government established public television only after commercial networks had become 'solidly entrenched' and able to lobby successfully 'against a strong public-sector component' (Patterson 2000, 246). The television market has traditionally been dominated by the 'big three' commercial networks – CBS, NBC, and ABC – and their affiliates. Their supremacy over news broadcasting is, however, diminishing as the cable networks like CNN, Fox News, and MSNBC with their popular 24/7 news formats are attracting sizable audiences and advertising revenues (Graber and Holyk 2011). The daily newspaper market, on the other hand, is 'geared toward local readership'[9] with an estimated 1,400 individual papers scattered throughout the US.

While print media generally provide the most of political information, news featured by television networks appeal to much broader sections of the public. In 2000, for instance, Patterson reported that three times as many US citizens relied on television as on newspapers as their key news source, followed by the radio in a distant third place (2000, 247). Nowadays, the Internet is the strongest rival for traditional news media.[10] 2010 was the first year the number of Americans who identified the Internet as their primary source of news exceeded the number of citizens relying on newspapers. A recent survey by the Pew Research Center revealed that the Internet was the third most frequently used news source for the 2012 US presidential campaign, after cable news networks and local television news, surpassing newspapers by far.[11]

Despite the large number of private news organisations and the absence of regulation, numerous commentators agree that the US media environment does not really provide an information-rich, open 'marketplace of ideas' conducive for robust public debate (e.g. Patterson 2000; Graber and Holyk 2011; Brown and Gitlin 2011). As a result of several intertwined factors, most Americans, to cite Patterson, 'receive a relatively uniform rendition of the news' (2000, 248). Structural constraints in news production considerably limit the spectrum of news stories and views provided to the general public. Since newsgathering in a country as vast as the United States is expensive, only a handful of media

[8]Ibid.
[9]Ibid.
[10]In 2012, approximately 81% of US citizens used the Internet. See ibid.
[11]Ibid.

organisations actually do it. The majority of news providers depend on wire services for non-local stories, or follow the stories first published by internationally-respected news organizations (Graber and Holyk 2011). In recent years, the quality of news and the ability of traditional news organisations to conduct investigative reporting and thus fulfill their watchdog function has further suffered as the news industry experiences, particularly newspapers, experience financial trouble, as a result of the rise of the Internet and the global economic crisis. According to the 2009 Pew Report on the State of the News Media, 'the problem facing American journalism is not fundamentally an audience problem or a credibility problem. It is a revenue problem—the decoupling… of advertising from news.'[12] According to the Newspaper Association of America, print newspapers' ad revenues fell by 55% between 2007 and 2012.[13] Virtually all outlets have been forced to cut back their newsgathering, personnel, and infrastructure over the past decade. Some competing media outlets have even started sharing resources, including journalists.[14] Focusing their resources on online editions, several newspapers have discontinued their print editions entirely, while others publish only a few times a week. Several television networks have reduced reporting teams, leaving a single person to function as reporter, editor, cameraman and producer (Graber and Holyk 2011). Despite some serious efforts in online journalism, many blogs devoted to public policy issues are often plagued with staunch partisanship. Instead of compensating for the general decline in traditional news coverage they contribute to further ideological polarisation (Brown and Gitlin 2011).

While in the past individually owned private media companies prevailed in the news media sector, large corporations and/or tycoons, often with no previous experience in journalism, have increasingly started to purchase unprofitable media outlets.[15] With the exception of the Hearsts, the owners of the *Times Union,* and the Sulzbergers, the owners the *New York Times*, few of America's newspaper families still hold on to the broadsheets founded by their ancestors. Even the Sulzbergers were forced to sell the *Boston Globe* at a loss to the owner of the Boston Red Sox baseball team, John Henry, in 2013. The most recent and perhaps the most prominent example of this trend is the acquisition of the struggling, high-quality newspaper, the *Washington Post,* by the founder of Amazon.com, Jeff Bezos, in

[12]Pew Research Centre for Excellence in Journalism. 2009. The State of the News Media 2009. Web. Accessed 20 August 2013. http://www.stateofthemedia.org/files/2011/01/COMPLETE-EXEC-SUMMARY-PDF.pdf.
[13]Launder, William Christopher S. Stewart and Joann S. Lublin. 2013. "Bezos Buys Washington Post for $250 Million." Wall Street Journal, 5 August 2013. Web. Accessed 10 October. http://online.wsj.com/news/articles/SB10001424127887324653004578650390383666794.
[14]Freedom House. 2013. "Freedom of the Press 2013 – United States." Web. Accessed 20 August 2013. http://www.freedomhouse.org/report/freedom-press/2013/united-states.
[15]Freedom House. 2013. "Freedom of the Press 2013 – United States." Web. Accessed 20 August 2013. http://www.freedomhouse.org/report/freedom-press/2013/united-states.

early August 2013.[16] Although Bezos promised that the newspaper's values would not change, some commenters were concerned about the phenomenon of tycoon-owners who could pursue corporate or political interests through their newspapers. Others, in contrast, were hopeful that Bezos could come up with a business strategy that would attract new readers while preserving the best characteristics of the *Post*.[17] Acknowledging challenges ahead, the Chairman of the Washington Post Company, which had owned the newspaper since 1933, praised Jeff Bezos's track record as a 'well-connected industry innovator with the patience to make difficult businesses profitable.'

Commentators agree that the commercialism in American press is another reason why 'newspapers and broadcast stations from coast to coast are likely to highlight the same national news stories and to interpret them in similar ways' (Patterson 2000, 248). As Graber and Holyk explain, 'most private owners are business entrepreneurs who are motivated by economic goals rather than public service aims.' The main source of revenue for the media has traditionally been advertising, which is contingent on the size and demographic composition of the audience. Hence, 'to attract the largest audiences, and thereby earn the largest advertising fees, programming is structured to suit audience preferences. The societal importance of news is secondary, as is the need to keep the public well informed enough to perform citizenship functions effectively' (2011). As Patterson argues, 'both television and newspaper stories have become shorter, more conflict-ridden, and more story-like' (2000, 247–8). To appeal to audiences, the media couch political issues in attractive entertainment formats. 'Soft news' prevails over 'hard news.' Soft news portrays human-interest stories that emphasise episodes in the lives of particular individuals or groups. Stories are framed in a way that the audience can identify with some of the actors in the story and empathise with them. Hard news, on the other hand, discusses societal problems in a more thematic, less personalised way. It reports events in a factual style, encouraging dispassionate analysis and general conclusions about the issues at hand. While soft news, with its focus on individual episodes in specific individuals' lives, fosters thinking in terms of specified contexts, thematic framing promotes a broader consideration of social issues and the seeking of society-wide solutions for issues (Graber and Holyk 2011).

US news media pride themselves on offering 'objective' coverage. They try to avoid personal interpretations and opinions, and instead provide opposing viewpoints in dialogue with each other. However, commentators agree that journalistic objectivity and political

[16]"Bezos buys the Post: The newspaper industry." 2013. *The Economist* (Online), 6 August 2013. *Proqest*. Web. Accessed 18 October 2013.

[17]"Lexington: Keeping the mighty honest." 2013. *The Economist*, 10 August 2013. Web. Accessed 18 October 2013. http://www.economist.com/news/united-states/21583274-new-wave-press-barons-should-not-allow-newspapers-become-niche-products-keeping?zid=293&ah=e50f636873b42369614615ba3c16df4a.

neutrality are declining as an aggressive and partisan interpretive style increasingly dominates reporting (Hallin and Mancini 2004; Brown and Gitlin 2011; Graber and Holyk 2011). Hallin and Mancini write that, historically in the Anglo-American model, 'the dominant form of professional practice came to be centered around the notion of "objectivity" – that is, fundamentally, the idea that news could and should be separated from opinion, including both the opinions of journalists and those of owners'. 'Compared with continental journalists, who give greater emphasis to commentary', US journalists nowadays still 'remain more oriented towards informational and narrative styles of writing'. However, according to Hallin and Mancini, 'the differences have diminished' (2004, 291; 207). In contrast, Patterson claims that interpretive reporting has 'become the dominant model of news coverage,' with journalists, previously 'the relatively passive voice behind the news,' becoming 'as active and visible as the newsmaker they cover.' According to Patterson, 'facts and interpretations are freely intermixed in news reporting. Interpretation provides the theme and the facts illuminate it. The theme is primary, the facts are illustrative' (2000, 249–250).

Journalists have also become increasingly aggressive and negative in their coverage of political news. Politics is reported not as 'an issue but a game in which individual politicians vie power' (Patterson, 253-4). Instead of proper investigative journalism, US media have been blamed for 'attack dog journalism' that uses politicians' opponents as a foundation for undermining their claims. Patterson explains that 'these attacks are circumscribed in that journalists seldom contest the values inherent in political conflicts. But they constantly question politicians' motives, methods, and effectiveness. This type of reporting may look like watchdog journalism, but in most instances it is not. It is ideological in its premise: politicians are assumed to act out of self-interest rather than from political conviction' (252). It has been suggested that the US media's preference for game-centred, negative news has intensified Americans' 'disenchantment with their political leaders and institutions,' and misled the public about social trends. For instance, a survey in 1996 found that US citizens incorrectly believed by a two-to-one margin that unemployment, inflation, the federal budget, and crime had risen during the past five years. As Patterson argues, when negative stories emphasising political scandal, wrongdoing and incompetence 'overwhelm positive ones, the public can hardly be faulted for thinking poorly about the performance of government and the condition of society' (2000, 263).

Hallin and Mancini maintain that 'it would make little sense to characterise American newspapers as Europeans commonly do theirs, by assigning them distinct locations on the political spectrum or distinct partisan sympathies.' They write that 'for the most part, American newspapers are not significantly differentiated in their political orientations.' Nonetheless, to characterise US journalism as neutral 'is not meant to imply that it is literally 'value free' or without a point of view. The point is that these media position themselves as

"catchall" media, cutting across the principal lines of division between established political forces in society' (2004, 208–210). In fact, the American political system 'is organised around two catchall, centrist parties, both committed to a liberal political culture that is essentially taken for granted' (2004, 239). According to Hallin and Mancini, the US news media thus essentially all have the same, centrist political leaning oriented towards the political 'mainstream.' A survey conducted by Patterson and Donsbach found in 1993 that American journalists placed all major news organisations within a small range in the middle of the political spectrum between the Republicans and Democrats. Hallin and Mancini therefore write that although 'on their editorial page many American newspapers have relatively consistent political orientations,' these carry over to news reporting only to a limited extent. At the same time, US news media are oriented towards the views of the white middle-class readers who are the preferred target of advertisers (2004, 208–210). However, Hallin and Mancini also admit that there are 'signs of change,' particularly when considering the actions of Rupert Murdoch, who has insisted on 'control of the political content of his media and using them to intervene in politics' (2004, 219). In addition, the twenty-four-hour news cycle has made it increasingly difficult and expensive to fill twenty-four hours will well-researched news that provides multiple perspectives. Hence, as Graber and Holyk argue, 'all news enterprises, including legacy media, have increased interpretive stories delivered by "pundits" who often are exceptionally outspoken, partisan, provocative, and sometimes even outrageous.' The overall consequence is an increasingly confrontational political climate, less willingness to compromise, and greater disrespect for opposing views (Graber and Holyk 2011). It goes without saying that these developments are harmful to a healthy public debate on society-wide issues.

3. Methodology

3. 1. Research design

This report employs qualitative textual analysis of newspaper articles published between 1 January 2010 and 31 April 2013 focusing on discourses and patterns of communication related to risk and security. To focus our research, we selected the following security-related topics: the introduction of 3D body scanners at American airports, the Stuxnet attacks, and the use of CCTV cameras. The analysis explored the ways in which media frame the implications of security and security technologies, namely the perceived trade-offs between security and privacy and the identity of the proponents and opponents of security and/or freedom/privacy considerations. At the same time, we were interested in investigating whether new technologies are portrayed as providing answers to security issues

or if, instead, they represent new risks. Lastly, we strove to examine how the media viewed and discussed various security threats and whether the media coverage of terrorism risks rendered the public more sensitive to the issue of security.

Acknowledging the limitations of qualitative research, we employed qualitative textual analysis research. This allowed us to examine in detail the discourses relating to different security risks and the perceived trade-offs between security and freedom/privacy and the trends therein over time. By using qualitative methods of data gathering and analysis, we were also able to overcome the limitations of secondary data employed for comparative quantitative analysis used in previous stages of the project, such as data unavailability for a selected time point and/or country. The selected articles were coded using *Atlas.ti*. As our unit of analysis, we chose individual statements, i.e. a sentence, a part of a sentence, or several sentences, comprising of an actor making an argument about one of the selected topics. We coded the statements by nine different categories: actor, topic, argumentation type, direction of argument, justification, interaction among actors, political orientation of newspaper, and origin of newspaper. We employed a specific coding scheme for each topic developed by a team of coders in Prague based on pre-tests. The master coding schemes were a product of participant inter-coder reliability tests during the training sessions at the Graduate School and detailed discussions about the aims of the research, about identifying coding sequences and categories of codes, and deconstructing the language of the media.

3. 2. Data gathering

3. 2. 1. Newspaper selection

The data set analysed in this report includes newspaper articles published in two US newspapers between 1 January 2010 and 31 April 2013. The objective of the study was to explore and understand the whole variety of discourses found in the press relating to our cases in order to better understand the role of the media in the public's risk perceptions. Hence we strove to select two English-language quality dailies with a national scope, which were among the top ten newspapers by circulation between 2009 and 2012. Research has demonstrated that the political orientation of the media influences how public issues and events are portrayed. Attempting to explore whether national newspapers with different political orientations portray the security risks and trade-offs differently, we selected newspapers with opposing political leanings. Taking the specifics of the US newspaper market into consideration, we selected *The New York Times* (NYT) and *The Wall Street Journal* (WSJ) for analysis.

The US newspaper market is predominantly local with newspapers whose readership cuts across class divisions. Hallin and Mancini write that 'only the New York City market … is really comparable to the British newspaper market,' characterised as 'a national newspaper market, which can support multiple newspapers directed toward distinct market segments (2004, 206)'. The expansion of newspapers based in the City of New York into the broader national market is a fairly recent development, enabled by technological advances. According to Hallin and Mancini, the US is 'so large that national daily newspapers were not technologically feasible until advances in telecommunication made it possible to send large amounts of data cheaply around the country. ' Hence, *USA Today* was only founded in 1982, with *The New York Times* also introducing its national edition in the 1980s (2004, 206). New York based papers have also long dominated the US newspaper market in terms of circulation (Table 1) with the financial daily *Wall Street Journal* topping the list. It is followed by the 'general-interest newspaper' *USA Today*, which is sometimes 'considered gimmicky and insubstantial,'[18] and by the reputable daily, *The New York Times.*

Table 1: Top ten US dailies by circulation, 2009 – 2012

Newspaper	Political leaning	Circulation rate			
		2009	2010	2011	2012
Wall Street Journal	Conservative	2,024,269	2,061,142	2,096,169	2,293,798
USA Today	Centre	1,900,116	1,830,594	1,784,242	1,713,833
New York Times	Liberal	927,851	876,638	1,150,589	1,613,865
Los Angeles Times	Liberal	657,467	600,449	572,998	641,369
Washington Post	Liberal	582,844	545,345	507,465	462,228
New York Daily News	Liberal	544,167	512,520	605,677	535,875
New York Post	Conservative	508,042	501,501	512,067	522,868
San Jose Mercury News	Liberal	224,937	477,595	527,568	529,999
Denver Post	Liberal	340,949	309,863	353,115	412,669
Chicago Sun-Times	Liberal	275,641	250,747	389,352	432,455

Source: Alliance for Audited Media, formerly Audit Bureau of Circulations: http://www.auditedmedia.com/
Note: Newspapers marked in yellow were coded.

As is apparent from the previous section, the left-right political division of political parties and the press is not as straightforward in the US as it is in the European context. Nevertheless, Eisinger, Veenstra and Koehn argue that 'the presence of systematic ideological bias' prevails in American media and 'would contradict claims of neutrality' (Eisinger et al. 2007, 19; cited in Ha 2012). A widening ideological divergence in US media in terms of the coverage of public issues and figures, particularly on the editorial and opinion pages, has

[18]Encyclopaedia Britannica. 2013. "USA Today." Accessed 9 September 2013. http://www.britannica.com/EBchecked/topic/683077/USA-Today.

been explored in various studies (Groeling; Iyengar and Hahn 2009). *The New York Times* and MSNBC maintain a Democratic, liberal editorial stance (Hallin and Mancini 2004, 208) and stand on the opposite side of the ideological divide from the Fox News Network and *The Wall Street Journal*, which target conservative, Republican readers. According to Jamieson and Cappella (2008), Fox News and *The Journal* (both owned by Rupert Murdoch), together with Rush Limbaugh's talk radio show, represent an 'echo chamber' that promotes conservative beliefs and defends the Republican Party (see also Iyengar and Hahn 2009). Analysing the news coverage of President Obama's health care reform proposals, Ha (2012) also found a 'clash of partisan framing between conservative and liberal media', with *The Wall Street Journal* and Fox News representing the former and *The New York Times* and MSNBC representing the latter.

3. 2. 1. 1. The New York Times

The New York Times is an English-language quality daily newspaper published in New York City. It has long been the newspaper of record in the United States.[19] The Ochs-Sulzberger family, one of the US newspaper dynasties, has owned the *Times* since 1896, when the paper was bought by Adolph Ochs. He formed the New York Times Company, which still owns the daily. Though well regarded, the newspaper has never been the largest of US newspapers in terms of circulation. Between 2009 and 2012, the *Times* sales ranged between 876,638 and 1,613,865, placing it third in terms of circulation (Table 2). The *Times* appeals to a cultured, intellectual readership, rather than to a mass audience. From the beginning, the strength of the paper has been 'its editorial excellence.'[20] By placing great emphasis on reporting the news of the day, maintaining and emphasizing good coverage of international news, and generally avoiding sensationalism, Ochs built the *Times* into 'an internationally respected daily.'[21] Indeed, by 2012 the *Times* had won 108 Pulitzers, awarded for excellence in journalism in a range of categories,[22] and the paper increased that number to 112 in 2013.[23] In fact, the *Times* has received more Pulitzers than any other news organisation

[19]Encyclopaedia Britannica 2013. "The New York Times." Accessed 28 August. https://www.britannica.com/EBchecked/topic/412546/The-New-York-Times.
[20]Ibid.
[21]Ibid.
[22]Rainey, James and Jessica Garrison. 2012. "Pulitzer winners span old, new media." Los Angeles Times, 17 April 2012. Web. Accessed 9 September 2013. http://articles.latimes.com/2012/apr/17/nation/la-na-pulitzers-20120417.
[23]The New York Times Company. 2013. "Pulitzer Prizes." Accessed 9 September 2013. http://www.nytco.com/company/awards/pulitzer_prizes.html.

worldwide.[24]

3. 2. 1. 2. The Wall Street Journal

The Wall Street Journal is an English-language daily business and financial newspaper edited in New York City and sold throughout the US. Other daily editions of the paper include *The Wall Street Journal Europe*, edited in Brussels, and *The Asian Wall Street Journal*, edited in Hong Kong.[25] The *Journal* has the widest circulation among all US newspapers. In the period of 2009 to 2012, between 2,024,269 and 2,293,798 copies were sold annually. Charles H. Dow of Dow Jones & Company established *The Wall Street Journal* in 1889. In 2007, Rupert Murdoch's News Corporation acquired Dow Jones and Company, the publisher of the newspaper. Despite assurances that 'the same standards of accuracy, fairness and authority will apply' to the daily regardless of ownership,[26] several of its former and current reporters have been said to claim that the takeover has had a significant impact on the publication. In their opinion, the *Journal* has become 'more newsier' and 'less analytical,' rendering it a 'much more ordinary paper' than before. Further, the paper has been thought to have adopted 'a more conservative tone,' and to have edited and headlined articles to 'reflect a chronic scepticism (sic)' of the Democratic administration.[27] While a 2005 study of media bias found *The Wall Street Journal* to be more liberal than *The New York Times* (Groseclose and Milyo 2005), in the past few years, academic sources have started to characterise the *Journal* as a conservative outlet.

3. 2. 2. Articles selected for analysis

Articles for analysis were gathered through searches of the web portals of *The New York Times* – www.nytimes.com – and of *The Wall Street Journal Europe* – http://uk.wsj.com/. We searched for articles published between 1 January 2010 and 31 April 2013 under the following search terms: 'body scanner' and 'body scan AND airport' for 3D body scanners; 'stuxnet' for the topic of Stuxnet; and 'cctv AND/OR camera AND surveillance' for CCTV camera systems. Only articles relevant for this study, that is articles providing arguments about security risks

[24]Encyclopaedia Britannica 2013. "The New York Times." Accessed 28 August. https://www.britannica.com/EBchecked/topic/412546/The-New-York-Times.

[25]Encyclopaedia Britannica. 2013. "The Wall Street Journal." Accessed 28 August. https://www.britannica.com/EBchecked/topic/634727/The-Wall-Street-Journal.

[26]Crovitz, L. Gordon. 2007. "A Report to Our Readers." *The Wall Street Journal*, 1 August 2007. Web. Accessed 10 September 2013. http://online.wsj.com/article/SB118592510130784008.html.

[27]Carr, David. 2009. "Under Murdoch, Tilting Rightward at The Journal." The New York Times, 13 December 2009. Web. Accessed 10 September 2013. http://www.nytimes.com/2009/12/14/business/media/14carr.html.

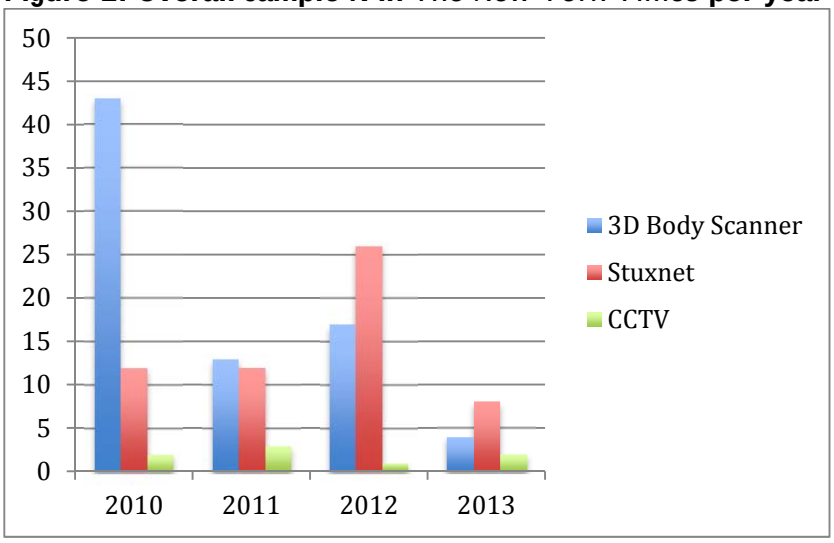
related to our three topics, were included in the overall sample N. Altogether, we found 224 articles. Of these, 122 or 54.5% were about 3D body scanners, 87 or 38.8% were about Stuxnet, and 15 or 6.7% of articles were about CCTV (Table 2). For each topic, we found more articles in *The New York Times* than in *The Wall Street Journal*. This is not so surprising, given that the *Journal* is largely a financial paper and our topics are not directly related to the economy or the world of business.

Table 2: The overall sample N – *NYT* and *WSJ* articles per topic and year

Newspaper	Topic	Number of articles per year				Total	%
		2010	2011	2012	2013		
The New York Times (left-leaning)	3D Body Scanner	43	13	17	4	**77**	34.38
	Stuxnet	12	12	26	8	**58**	25.89
	CCTV	2	3	1	2	**8**	3.57
The Wall Street Journal (right-leaning)	3D Body Scanner	29	5	9	2	**45**	20.09
	Stuxnet	6	10	12	1	**29**	12.95
	CCTV	0	4	2	1	**7**	3.13
Total		**92**	**47**	**67**	**18**	**224**	100
%		41.07	20.98	29.91	8.04		100

3D body scanners were thus the topic that attracted the largest media attention in the United States. In both papers, the topic was discussed most intensively in 2010 (Figures 1 and 2), with 43 articles in the NYT and 29 in the WSJ. The salience of the issue waned in the following year, only to increase again in 2012. In the first third of 2013, the interest in 3D body scanners decreased once more.

Figure 1: Overall sample N in *The New York Times* per year and topic

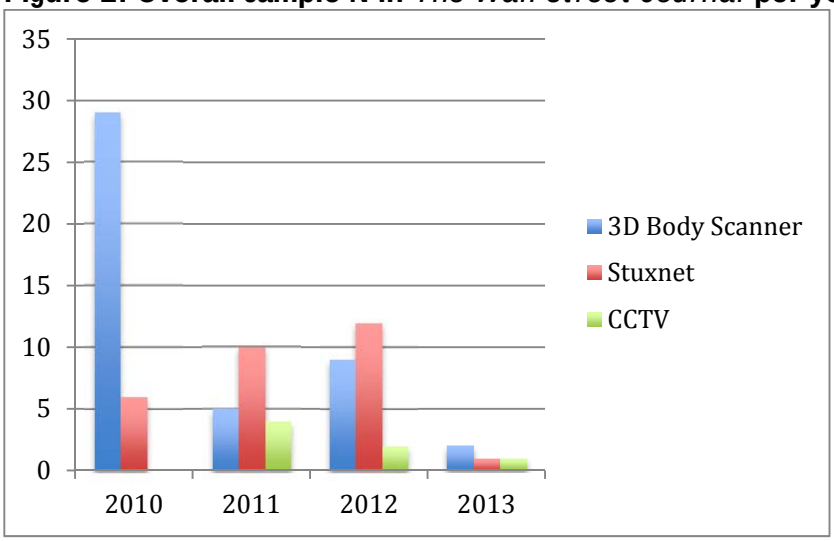


The Stuxnet phenomenon was the second most salient one in the US press. With 12 articles in 2010 and 2011, the interest in the topic in the NYT remained constant in the first

half of the studied period, peaking in 2012 with 26 articles. With 8 articles, the salience of Stuxnet in the NYT in the first four months of 2013 was comparable to that of the previous year. The coverage of Stuxnet in the WSJ doubled between 2010 (6 articles) and 2012 (12 articles), reaching its lowest point in the first four months of 2013 (1 article).

The issue of the use of CCTV camera systems was the least discussed in both the NYT and the WSJ. The salience of the topic in the *Times* remained almost constant throughout the studied period. In contrast, the interest in the issue in the *Journal* peaked in 2011 with 4 articles, while the previous year CCTV cameras attracted no attention from the paper. The salience of the topic decreased again in 2012, with a slight increase in proportionate terms in the first third of 2013.

Figure 2: Overall sample N in *The Wall Street Journal* per year and topic



We selected 43 articles for coding (Table 5) – 21 about 3D body scanners (thirteen from *The New York Times* and eight from *The Wall Street Journal*), 15 about Stuxnet (nine from the *Times* and 6 from the *Journal*), and seven about CCTV (four from the *Times* and three from the *Journal*). Appendix 1 includes the list of all coded articles. In our data set we attempted to achieve proportionality in relation to the numbers of coded articles by topic and publication year. Given the nature and objectives of our analysis, this was not always possible. If we wanted to retain proportionality in selection, we could only select three articles about CCTV. Coding of merely three articles would not allow for a thorough qualitative analysis of the whole spectrum of arguments put forward in the media. It would thus hardly produce an in-depth understanding of how the media frame the security vs. freedom dilemma and influence citizens' perceptions of security risks and acceptance of the use of CCTV cameras.

Table 3: Articles selected for analysis per topic and year

Newspaper	Topic	Number of articles per year				Total	%
		2010	2011	2012	2013		
The New York Times (left-leaning)	3D Body Scanner	7	2	3	1	**13**	30.23
	Stuxnet	2	1	5	1	**9**	20.93
	CCTV	2	0	1	1	**4**	9.30
The Wall Street Journal (right-leaning)	3D Body Scanner	5	1	1	1	**8**	18.60
	Stuxnet	1	2	2	1	**6**	13.95
	CCTV	0	1	1	1	**3**	6.98
Total		**17**	**7**	**13**	**6**	**43**	-
%		39.53	16.28	30.23	13.95	-	100

The main selection criteria were the quality of arguments and relevance to the objectives of our study. We thus only selected articles that discussed the dilemma between security and freedom related to our three topics. In the case of CCTV cameras, priority was given to articles in relation to their use in public transport before selecting articles about CCTV use in general or in other settings.

4. Security situation in the US, January 2010 – April 2013

According to the US National Defense Industrial Association, 2012 intelligence forecasts by the Obama administration drew attention to five major challenges threatening US and global security in the coming decades – biological and nuclear weapons, cyber-attacks, climate change, and transnational crime.[28] In the studied period of 2010 and 2013, the security situation in the US was explicitly influenced by incidents related to several of those security threats, which are directly related to the analysis presented below.

Since 11 September 2001, when the United States experienced its worst attack in sixty years, leaving 3,000 fatalities, the country has conducted a so-called 'war on terror.' Since 9/11, the threat of terrorism and transnational crime has been most vividly demonstrated by the failed airplane bomb plot of Christmas Day 2009. That day a Nigerian national with links to al-Qaeda, Umar Farouk Abdulmutallab, attempted to blow off a Northwest Airlines flight from Amsterdam to Detroit. Abdulmutallab had concealed plastic explosives in his underwear, but he failed to detonate them properly and was tackled and restrained by a fellow passenger. Had he succeeded, the deaths of the 290 passengers on board of the airplane would have been the deadliest aviation disaster on US soil. There were reports indicating that the US had

[28] Erwin, Sandra I., Stew Magnuson, Dan Parsons and Yasmin Tadjdeh. 2012. " Top Five Threats to National Security in the Coming Decade." National Defense, November 2012. Web. Accessed 10 September 2013. http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx.

received intelligence concerning a planned attack by a Yemen-based Nigerian man, but that the security agencies failed to act. After the incident, President Obama admitted that 'the system designed to protect Americans in the wake of the 9/11 attacks had failed', calling the breakdown 'totally unacceptable.' Obama claimed: 'When our government has information on a known extremist, and that information is not shared and acted upon as it should have been, so that this extremist boards a plane with dangerous explosives that could cost nearly 300 lives, a systemic failure has occurred and I consider that totally unacceptable.' The President acknowledged that 'there was a mix of human and systemic failures that contributed to this potentially catastrophic breach of security.' He thus argued that the US needed to 'learn from this episode and act quickly to fix the flaws' in its system because the national security was and lives were at stake.[29] The failed Christmas Day plot triggered a fierce discussion among lawmakers, authorities, experts and advocacy groups about air travel security measures. The discussions led to the so-called multi-layered approach to security deployed by the Department of Homeland Security and the Transportation Security Administration (TSA), including 'increased sharing of intelligence and boarding pass information, the widespread use of body scanners, officers monitoring human behavior [sic] in airports and closer relationships with airport officials around the world.'[30] Following the Christmas Day plot, the US became the world leader in introducing 3D body scanners at airports for routine security checks. Some US airports had previously deployed the millimetre wave, full-body scanners that produced less powerful, non-ionizing radiation, and less clear images. To prevent another terrorist attack using explosives hidden on an individual's body, US authorities moved towards large-scale introduction of the more controversial 'backscatter' body scanners that produced revealing images of passengers and exposed individuals to potentially harmful doses of ionizing radiation. In early January 2010 the US Congress announced that it appropriated funds for 450 backscatter scanners. In contrast, other countries with large international hub airports like the UK, France, Italy, and the Netherlands chose a more conservative approach to civil aviation security. They either merely agreed to test the backscatters or opted for the less contentious millimetre wave technology.[31] Following intense criticism of the use backscatters by privacy groups, various politicians,

---

[29]Allen, Nick. 2009. "Barack Obama Admits 'Unacceptable Systemic Failure' in Detroit Plane Attack." *Telegraph,* 29 December 2009. Web. Accessed 10 September 2013. http://www.telegraph.co.uk/news/worldnews/barackobama/6908709/Barack-Obama-admits-unacceptable-systemic-failure-in-Detroit-plane-attack.html.

[30]Schmidt. Michael S. and Nixon, Ron. 2012. "Airplane Security Debated Anew After Latest Bombing Plot." *New York Times,* 5 May 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/05/11/world/americas/airplane-security-debated-after-latest-bombing-plot.html.

[31]Wald, Matthew L. 2010. "Cancer Risks Debated for Type of X-Ray Scan." *New York Times*, 9 January 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/01/09/health/09scanner.html.

airline industry representatives and passengers, Congress passed a federal law requiring all body scanners to use privacy-protecting software by June 2013. Having failed to install such software to the backscatter scanners, the TSA was forced to remove all 250 units from US airports. While passengers were still required to go through full-body scans relying on the millimetre wave technology, such procedures raised fewer privacy and almost no health concerns.[32]

The 9/11 attacks on New York and the Pentagon triggered a boom in the video surveillance market. It has been estimated that the number of CCTV cameras deployed in the USA had increased by approximately 30 million in the decade since 2001.[33] In 2013, the CTTV and video surveillance market was valued at $3.2 billion, up from $3 billion in 2012,[34] and in 2007 it represented around one-third of the overall US security market.[35] Unlike the United Kingdom, the US had never fully adopted state-sponsored use of surveillance cameras. Instead, surveillance is done by a combination of private and public CCTV cameras.[36] Undoubtedly, the use of cameras predated 9/11. However, in the fearful months following the attacks, the need for improved security coincided with technological advancements. The resulting cost reduction of video surveillance equipment prompted a rush to introduce advanced security measures. Installing surveillance cameras became much cheaper, allowing even small businesses and private homes to install such equipment.[37] With the help of federal counter-terrorism funding from the Department of Homeland Security, American cities have also deployed numerous surveillance cameras.[38]

It is hard to establish the extent of CCTV surveillance use in US cities, since the information is generally not made public.[39] In San Francisco, for instance, cameras are installed in high-crime areas and reviewed for evidence after a crime has been committed. In

---

[32]Ahlers, Mike M. 2013. "TSA removes body scanners criticized as too revealing." *CNN.com*, 30 May 2013. Web. Accessed 20 October 2013. http://edition.cnn.com/2013/05/29/travel/tsa-backscatter

[33]Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. Web. Accessed 5 October 2013. http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[34]Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html.

[35]Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. Web. Accessed 5 October 2013. http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[36]Dailey, Kate. 2013. "The rise of CCTV surveillance in the US." *BBC.co.uk*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bbc.co.uk/news/magazine-22274770.

[37]Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. Web. Accessed 5 October 2013. http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[38]Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html.

[39]Ibid.

2011, Chicago authorities reportedly had access to around 10,000 private and public surveillance cameras.[40] In 2007, Boston-area authorities had, according to different reports, between 55[41] and 150 CCTV cameras[42] at their disposal, but they have expanded their surveillance system since then. In 2010, New York, a city that has faced more terrorist attacks than any other US city, reportedly had a network of over 4,000 CCTV cameras in its subway system alone.[43] The drive to install more CCTV cameras slowed down after 2006, partly due to the fact that no major terrorist incident had occurred for five years. Nonetheless, while it has never reached the levels in the UK, the penetration of surveillance cameras in public places in US cities in the studied period was considerably high.[44]

While there has been little evidence of CCTV cameras deterring would-be terrorists from perpetrating attacks,[45] surveillance equipment has been used to investigate and track-down terrorist suspects in at least two cases. The City of New York faced a failed terrorist attack on 1 May, 2010, when a US citizen of Pakistani origin, Faisal Shahzad, attempted to bomb Times Square by blowing up a parked vehicle with crude explosives hidden in its trunk. Although the bomb failed to explode properly, the sound it made attracted the attention of a street vendor, who alerted police.[46] The discovery of the bomb triggered an evacuation of Times Square, causing enormous disruption but no casualties. The police reviewed hours of video footage from 82 city surveillance cameras operating around Times Square, as well as cameras from business and tourist agencies. They released a video of a 'person of interest,' who, it was later revealed, was not linked to the attack.[47] But with the help of video footage,

---

[40]Ibid.

[41]Kelly, Heather. 2013. "After Boston: The Pros and Cons of Surveillance Cameras." *CNN.com*, 26 April 2013. Web. Accessed 20 October 2013. http://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/.

[42]Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html.

[43]Rivera, Ray and Michael M. Grynbaum. 2010. "Lack of Video Slows Hunt for a Killer in the Subway." New York Times, 29 March 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/03/30/nyregion/30subway.html.

[44]Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. Web. Accessed 5 October 2013. http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[45]Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html and Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. Web. Accessed 5 October 2013. http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[46]"Times Square Bomb Attempt Man Jailed for Life." 2010. *Guardian*, 5 October 2010. Web. Accessed 10 September 2013. http://www.theguardian.com/world/2010/oct/05/times-square-bomb-attempt-man-jailed.

[47]Warrick, Joby, Peter Finn and Ellen Nakashima. 2010. "Times Square Bombing Attempt Reveals Limits of Video Surveillance." *Washington Post*, 4 May 2010. Web. Accessed 20 October 2013. http://www.washingtonpost.com/wp-dyn/content/article/2010/05/03/AR2010050304522.html and Grynbaum, Michael M., William K. Rashbaum and Al Baker. 2010. "Police Seek Man Taped Near Times Sq. Bomb Scene."

Shahzad's movements were tracked down. He was arrested a couple of days after the attack at the JFK airport as he sought to flee the country. Shahzad was faced ten separate charges, including terrorism, to which he pleaded guilty, arguing he was 'part of the answer to the US terrorising the Muslim nations and the Muslim people.'[48] The attack sparked calls from elected officials to install hundreds of additional cameras in the city as a means of preventing terrorism and reducing crime. However, the attacks also demonstrated the limits of video surveillance. Not only did cameras fail to prevent Shahzad's bomb plot, the footage also did not lead the authorities immediately to the perpetrator. Instead, the recording initially released by the police implicated an innocent man.[49]

On 15 April 2013, an improvised pressure-cooker bomb exploded near the finish line of the Boston Marathon. The attack killed three people, while at least thirteen people lost their limbs and more than 260 were injured. Mass shootings apart, the number of casualties renders the attack 'the most deadly act of terror in America since September 11th 2001'.[50] Afterwards, the FBI reviewed hours of video footage and numerous smartphone images provided by law enforcement and private security cameras, broadcasters and bystanders.[51] Three days after the attacks, the FBI released pictures of the suspects captured by a department store camera.[52] Following a frantic manhunt, the suspects were tracked down only a day after the pictures were released. One of the suspected bombers, Tamerlan Tsarnaev, died after a confrontation with police. The other suspect, Tamerlan's younger brother, Dzokhar, was injured and later charged with using and conspiring to use a weapon of mass destruction. The surviving suspect was reported to have said that he and his brother also wanted to target New York City's Times Square.[53] The bombing sparked new fears of extremist attacks and triggered discussions about US surveillance and immigration policies. Most importantly, the crucial role that CCTV footage played in identifying and tracking the

---

New York Times, 2 May 2010. Web. Accessed 20 October 2013. http://web.archive.org/web/20100505083749/http://www.nytimes.com/2010/05/03/nyregion/03timessquare.html?hp

[48]Gabbatt, Adam. 2010. "Faisal Shahzad Pleads Guilty to Attempting to Bomb Times Square." *Guardian*, 22 June 2010. Web. Accessed 10 September 2013. http://www.theguardian.com/world/2010/jun/22/faisal-shahzad-pleads-guilty-new-york-times-square-bomb.

[49]Warrick, Joby, Peter Finn and Ellen Nakashima. 2010. "Times Square Bombing Attempt Reveals Limits of Video Surveillance." *Washington Post*, 4 May 2010. Web. Accessed 20 October 2013. http://www.washingtonpost.com/wp-dyn/content/article/2010/05/03/AR2010050304522.html.

[50]"The Boston Bombings. The Manhunt is Over." 2013. *The Economist (Online)*, 19 April 2013. *Factiva*. Accessed 10 October 2013.

[51]Dailey, Kate. 2013. "The Rise of CCTV Surveillance in the US." *BBC.co.uk*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bbc.co.uk/news/magazine-22274770 and "The Boston Bombings. The Manhunt is Over." 2013. *The Economist (Online)*, 19 April 2013. *Factiva*. Accessed 10 October 2013.

[52]Kelly, Heather. 2013. "After Boston: The Pros and Cons of Surveillance Cameras." *CNN.com*, 26 April 2013. Web. Accessed 20 October 2013. http://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/.

[53]Gabbatt, Adam and Dan Roberts. 2013. "Boston Suspects Planned Attack on New York City, Mayor Bloomberg Says." *Guardian*, 25 April 2013. Web. Accessed 10 September 2013. http://www.theguardian.com/world/2013/apr/25/boston-bomb-suspects-new-york-city-attack.

suspects' movements before and after the bombing had triggered a public debate about the importance of CCTV cameras and other surveillance tools in public spaces for national security and law enforcement.[54]

After 9/11, terrorist attacks occurred relatively rarely and claimed fewer lives than road accidents, for instance.[55] Rather than for preventing and catching (would-be) terrorists, CCTV cameras have thus been used for more mundane purposes, like tracking down common criminals or catching individuals misbehaving in the streets – if they have been used at all.[56] Some commentators and politicians have praised the widespread use of CCTV cameras, citing it as one of the factors that has contributed to the drop in crime rates the US has experienced since about 1991.[57] Between 1990 and 2013, the rate of crime against people and property has dropped the most in large US cities. There, violent crime has decreased 64%, though it was only down 32% across the United States as a whole. Whilst violent crime increased slightly during the global economic crisis, a new crime wave was deemed unlikely by commentators.[58] The fall in crime rates across the US had been attributed to the fact that fewer individuals were becoming criminals. Technological advancements, including surveillance equipment, such as CCTV cameras, were thought by some to have contributed to the downward trend in crime statistics. They improved the effectiveness of detective work and created fewer opportunities for criminals to commit crimes, since after shops and banks had invested in security, the risk of being caught rose substantially.[59] However, other experts and commentators considered the link between falling crime rates and use of surveillance cameras far from self-evident. They argued that cameras did not prevent terrorist and criminal attacks.[60] They also drew attention to the fact that the drop in crime rates in general, and in transport systems in particular, occurred in all cities regardless of the level of

---

[54]Dailey, Kate. 2013. "The Rise of CCTV Surveillance in the US." *BBC.co.uk*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bbc.co.uk/news/magazine-22274770 and Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html.

[55]"Why We Spy. The War on Terror is Obama's Vietnam." 2013. *The Economist (Online),* 10 June 2013. Web. Accessed 20 October 2013. http://www.economist.com/blogs/democracyinamerica/2013/06/why-we-spy.

[56]Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. Web. Accessed 5 October 2013. http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[57]For crime rates in the US between 1991 and 2010 see Federal Bureau of Investigation. "Crime Rate in the United States." Web. Accessed 24 October 2013. http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl01.xls.

[58] "Where Have All the Burglars Gone? Falling Crime." 2013. *The Economist,* 20 July 2013. *ProQuest.* Accessed 24 October 2013. http://search.proquest.com/docview/1411815450?accountid=9630.

[59]Ibid.

[60]Kelly, Heather. 2013. "After Boston: The Pros and Cons of Surveillance Cameras." *CNN.com*, 26 April 2013. Web. Accessed 20 October 2013. http://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/ and "How much surveillance do you need?" 2010. *The Economist (Online*), 3 April 2010. Web. Accessed 10 October 2013. http://www.economist.com/blogs/gulliver/2010/04/security_cameras.

investment in CCTV camera systems.[61]

Nonetheless, between 2010 and 2013, cities, law-enforcement authorities, and politicians periodically called for the introduction of more advanced surveillance technologies, including face recognition software. According to expert opinion, more surveillance is supposed to be introduced in the US in the near future.[62] One of the various law-enforcement initiatives strives to link real-time video with artificial intelligence software able to act before a crime or a terrorist bombing occurs. Such systems would alert police to warning signs, such as a recognized face or an abandoned piece of luggage, in time to prevent a potential terrorist or criminal incident. In 2013, New York was reportedly advancing to that capability with its so-called Domain Awareness System, which uses real-time feeds from around 3,000 CCTV cameras and other sensors located in lower and midtown Manhattan.[63] The FBI is also working on a biometric information system, the so-called Next Generation Identification (NGI) programme that is to include iris scans, and voice and facial recognition software. The NGI programme, which is planned to be fully operational in 2014, is supposed to consist of a database of 12 million images. Mugshots uploaded to the database by law enforcement authorities are to be searched and matched against pictures from crime scenes.[64] Drones outfitted with technology to intercept mobile phone signals and identify people on the ground are reportedly used by the federal government to patrol the border. It was reported that local law enforcement agencies in cities with population as small as 33,000 were also evaluating their use.[65] Such security initiatives triggered opposition from advocacy groups, who were concerned about the potential for misusing data gained from hi-tech surveillance software, if it were to be used for routine surveillance.[66] The issues of privacy

---

[61]Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html and "How much surveillance do you need?" 2010. *The Economist (Online*), 3 April 2010. Web. Accessed 10 October 2013. http://www.economist.com/blogs/gulliver/2010/04/security_cameras.

[62]Dailey, Kate. 2013. "The Rise of CCTV Surveillance in the US." *BBC.co.uk*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bbc.co.uk/news/magazine-22274770.

[63]Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html.

[64]Bennett, Drake. 2013. "Using Facial-Recognition Technology to Track Down the Boston Bombers (and Why Humans Are Still Better at It)." Businessweek.com, 19 April 2013. Web. Accessed 20 October 2013. http://www.businessweek.com/articles/2013-04-19/did-the-fbi-use-facial-recognition-software-to-find-the-boston-bombers.

[65]Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html.

[66]See Dailey, Kate. 2013. "The Rise of CCTV Surveillance in the US." *BBC.co.uk*, 29 April 2013. Web. Accessed 20 October 2013. http://www.bbc.co.uk/news/magazine-22274770 and Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. Web. Accessed 5 October 2013.

that have arisen from the more extensive use of cameras and advanced face recognition and other surveillance software are particularly complicated. Since legal precedent has rejected the 'reasonable expectation of privacy' in public space, the US has placed minimal restrictions on the deployment of face recognition software.[67]

Whilst security cameras and surveillance equipment were omnipresent in the US, security companies and the government were increasingly concerned with the less obvious threat of cyber-attacks.[68] In 2012, network intrusions were reportedly widely considered 'one of the most serious potential national security, public safety and economic challenges'. Army Gen. Keith Alexander, commander of new US Cyber Command argued that 'other than intercontinental ballistic missiles and acts of terrorism, an adversary seeking to reach out and harm the United States' had 'only one other option: destructive cyber-attacks'. He asserted that while the past decade had largely seen the theft of intellectual property and money, 'distributed denial of service attacks' overwhelming networks and disrupting operations of businesses or other organizations would follow. This, in his opinion, 'could result in loss of life and damage to the economy on par with what occurred after 9/11.'[69] Commentators estimated that American businesses lost between $100 billion to $1 trillion a year from online theft of research findings, proprietary information trade secrets, marketing plans, personal information, credit-card number, bank account details, etc.[70] While many attacks went unreported, during 2011 alone 200 attacks on core critical infrastructures in the communication, transportation, and energy industries were reported to the Department of Homeland Security.[71]

In many cases, evidence implicated hackers in Russia, China, Iran and elsewhere. The high security echelons, including General Alexander, were concerned about the fact that the foreign cyber-attacks on the US were increasing aimed at the country's critical infrastructure.

---

http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[67]"I Spy, With My Big Eye. Video Surveillance." 2012. *The Economist,* 28 April 2012. *ProQuest.* Accessed 24 October 2013. http://search.proquest.com/docview/1010371320?accountid=9630.

[68]Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com,* 23 August 2011. Web. Accessed 5 October 2013. http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL.

[69]Erwin, Sandra I., Stew Magnuson, Dan Parsons and Yasmin Tadjdeh. 2012. " Top Five Threats to National Security in the Coming Decade." National Defense, November 2012. Web. Accessed 10 September 2013. http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx.

[70]"Cyber-security. Difference Engine: Swamped with data." 2012. *The Economist (Online),* 11 May 2012. Web. Accessed 20 October 2013.
http://www.economist.com/blogs/babbage/2012/05/cyber-security.

[71]Erwin, Sandra I., Stew Magnuson, Dan Parsons and Yasmin Tadjdeh. 2012. " Top Five Threats to National Security in the Coming Decade." National Defense, November 2012. Web. Accessed 10 September 2013. http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx.

They also feared that the US was not ready to 'ward off a major attack.' [72] American intelligence officials believed that 'Iranian specialists in cyber sabotage' were behind the cyberattacks that 'thousands of Saudi files had temporarily prevented some American banking customers from gaining access to their accounts.' In an October 2012 speech, the US Defence Secretary Leon E. Panetta cited those attacks while warning 'of America's vulnerability to a coordinated computer warfare attack,' describing such a possibility as a 'cyber-Pearl Harbor'. [73] The security authorities urged the passage of the so-called Cyber Intelligence Sharing and Protection Act (CISPA) that, as General Alexander put it, would give the government new powers 'to defend private computer networks in the United States.'[74] The bill was criticised by various Internet privacy and civil liberties groups[75] and was rejected by the Senate.[76] The increased rate of cyber-attacks on US targets was discussed in connection with the top-secret US security operation 'Olympic Games'. As part of the operation, the US and Israel allegedly developed a virus called Stuxnet that targeted Iran's nuclear plants in order to delay the development of an atomic bomb by the Iranian regime, which was viewed as a threat to US security.[77] The latest cyber advancements were thus seen as a double-edged sword. By improving the US's cyber-warfare capabilities, they contributed to national security. On the other hand, they posed a risk, as America's adversaries could use those same techniques to target the US's critical infrastructure. As the White House asserted, 'the very technologies that empower us to lead and create also empower individual criminal hackers, organized criminal groups, terrorist networks and other advanced nations to disrupt the critical infrastructure that is vital to our economy, commerce, public safety, and military.'[78]

---

[72]Sanger, David E. and Eric P. Schmitt. 2012. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." *New York Times*, 26 July 2012. Web. Accessed 19 August 2013.

[73]Gladstone, Rick. 2012. "Iran Suggests Attacks on Computer Systems Came From the U.S. and Israel." *New York Times*, 25 December 2012. Web. Accessed. http://www.nytimes.com/2012/12/26/world/middleeast/iran-says-hackers-targeted-power-plant-and-culture-ministry.html.

[74]Sanger, David E. and Eric P. Schmitt. 2012. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." *New York Times*, 26 July 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html.

[75]"Cyber-security. Difference Engine: Swamped with data." 2012. *The Economist (Online)*, 11 May 2012. Web. Accessed 20 October 2013.
http://www.economist.com/blogs/babbage/2012/05/cyber-security.

[76]Selyukh, Alina and Deborah Charles. 2013. "CISPA Cybersecurity Bill Backers Hope Second Time's a Charm." *NBCNews.com*, 16 May 2013. Web. Accessed 20 October 2013. http://www.nbcnews.com/technology/cispa-cybersecurity-bill-backers-hope-second-times-charm-1C9948195.

[77]Sanger, David E. and Eric P. Schmitt. 2012. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." *New York Times*, 26 July 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html and Sanger, David E. 2012. "Obama Order Sped Up Wave of Cyberattacks Against Iran." New York Times, 1 June 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&pagewanted=print.

[78]Erwin, Sandra I., Stew Magnuson, Dan Parsons and Yasmin Tadjdeh. 2012. " Top Five Threats to National Security in the Coming Decade." National Defense, November 2012. Web. Accessed 10 September 2013.

5. Analysis

The following sections outline the findings of the qualitative textual analysis of the coverage of the controversies around 3D body scanners, Stuxnet, and the use of CCTV cameras in *The New York Times* and *The Wall Street Journal* between 1 January, 2010 and 31 April, 2013. The actors, their discussions, opinions and justifications, the manner in which the newspapers framed them and the trends therein are explored. The quality and content of coverage of individual topics in the two papers is also compared and contrasted. The analysis is first divided into sub-chapters by topic. The following section discusses the influence of domestic and international factors on the coverage, with the concluding section summarising and synthesising the findings of the press coverage of all three topics.

5. 1. 3D body scanner

5. 1. 1. Quality of articles and topics discussed

In relation to the 3D body scanner controversy, we coded twenty-one articles (13 from *The New York Times* and 8 from *The Wall Street Journal*). The articles varied in quality, length and style. However, we did not notice any apparent differences between the two newspapers. The articles ranged in length from around 450 to 1350 words. Some were more informative, providing factual and practical information about full body scanners and their introduction at American airports, setting the controversy in context and presenting statements from various actors. Other articles were more analytical, putting forward well-evidenced arguments about the use of body scanners. We coded articles found in the US news, travel, business, and health sections. We also analysed one article published in the World/Europe section, as well as five articles from the opinion columns. This suggests that the controversy was framed as a domestic issue. We did not observe considerable differences between the topics related to 3D body scanners covered by the two dailies. Only in a single instance did the WSJ discuss a distinct topic not mentioned in the NYT. A commentator discussed the divergent experience of his wife and himself when using commercial 3D body scanner in order to buy better fitting clothing. The coverage also developed in similar ways over time in both papers.

---

http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx.

5. 1. 2. Content analysis: Actors and themes

The 3D body scanners topic had largest media salience with the highest number of coded statements. Of all actors whose origin was possible to ascertain, 89% came from the USA, 6% were mentioned in general terms without specifying their origin, and 2% came from the European Union (EU). Hence, it can be safely claimed that the press considered the issue as an almost purely domestic issue. The Transport Security Administration (TSA), which was responsible for introducing the full body scanners at American airports, was the single most frequently coded actor, found 18.4% of the time. Journalists were found in 17.9% of statements. However, given that almost 24% of the coded articles were opinion pieces, we could claim that journalists did abide by the rules of journalistic objectivity. Various state institutions (9%), experts (8.7%), passengers (8.5%), airlines, airports and their associations (7%, coded as 'transportation company') politicians (5.7%) and private companies (4.7%) also had their say in the discussions about the use of 3D body scanners. Under 'private companies' we most frequently coded the suppliers and manufacturers of body scanners. The code, however, also included US fashion stores that have installed full body scanners to take measurements for make-to-measure clothes for their customers. Further, in 4.7% cases, the US newspapers presented the opinions of pilots and critics of the scanners, mentioned in general terms (both coded under 'others'). Advocacy groups and civil society representatives were given voice in 4.2% of statements, with various institutions, including the United States Court of Appeals for the District of Columbia, EU institutions, and the United Nations International Civil Aviation Organisation, heard in 4% of discussions. We found no interaction among actors.

Table 4: Actors coded in relation to 3D body scanners and their origin

Actor	#	%	Actor's origin							Total
			USA	Other	UK	Italy	International	EU	Mentioned generally	
Transport Security Agency	74	18.4%	74							74
Journalist	72	17.9%	72							72
State institutions	36	9.0%	35						1	36
Experts	35	8.7%	33						2	35
Passengers	34	8.5%	28				1		5	34
Transportation Company	28	7.0%	24						4	28
Politicians	23	5.7%	23							23
Private company	19	4.7%	16						3	19
Others	19	4.7%	11						8	19
Advocacy Group/civil society	17	4.2%	15						2	17
Institutions	16	4.0%	10				2	4		16
Scanners	11	2.7%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
States	10	2.5%	2	2	1	1		4		10
Individuals	3	0.7%	3							3
Terrorists	3	0.7%		2			1			3
President	2	0.5%	2							2
Total	**402**	**100%**	**348**	**4**	**1**	**1**	**4**	**8**	**25**	**391**

The themes of security-related rules and regulations (42.7%), the use and characteristics of body scanners (35.2%), and the increase in use and installation of body scanners (10.1%) dominated the coverage. It is important to note that the code 'security related rules and regulations' denoted the rules accompanying the use of 3D body scanners at airports. Such rules include the possibility for passengers to refuse scanning and instead submit to a pat-down, or the fact that 3D body scanners were supposed to produce blurred images of the human body. At the same time, we also assigned the code to discussions about other, alternative and/or complementary security measures used at American airports, including tiered screening, metal detectors, thermal cameras, and dogs. Under 'body scanner' we coded the use of full body scanners, as well as their characteristics and functions, such as how much radiation they emit. Other notable topics discussed in connection to 3D body scanners were health issues (5.2%), terrorism and a government led anti-terrorist campaign (3.5%), and privacy (2.3%). Body scanners and security-related rules and regulations were the two topics most frequently coded together, followed by body scanners and health issues. The topic of body scanners was also coded together with privacy and terrorism. The increase of body scanners and terrorism were also discussed together.

Table 5: Topics coded in relation to 3D body scanners

Topic	#	%
Security-related rules and regulations	182	42.7%
Body scanner	150	35.2%
Increased number of body scanners	43	10.1%
Health issues	22	5.2%
Terrorism	14	3.3%
Privacy	10	2.3%
Political partisanship	2	0.5%
Security general	2	0.5%
Government-led antiterrorism campaign	1	0.2%
Total	**426**	**100.0%**

5. 1. 3. Content analysis: Discussions about 3D body scanners

We found almost as many statements using a definitive argumentative strategy (45.4%) as those employing an evaluative one (44.1%). The coverage thus offered almost an equal amount of factual information about the increase, characteristics, functioning, and rules surrounding the use of 3D body scanners or their alternatives as it provided the readers with evaluative statements of different actors. In addition, we coded 10.5% statements advocating for or against the use of 3D body scanners and/or other security measures. Negative evaluative arguments about 3D body scanners and related issues (60%) outweighed the positive ones (40%). It is important to note that many of the positive comments concerned alternative security measures either proposed by the scanners' critics or later introduced by the TSA.

Table 6: Argumentative strategies and direction of arguments about 3D body scanners

Argumentative strategy	#	%	Direction of argument					
			positive		negative		neutral	
			#	%	#	%	#	%
Definitive	**174**	**45.4%**	0	0%	4	2.3%	170	97.7%
Evaluative	**169**	**44.1%**	44	26.0%	115	68.0%	10	5.9%
Advocative	**40**	**10.5%**	36	90.0%	4	10.0%	0	0%
Total	**383**	**100%**	**80**		**123**		**180**	

61.4% of statements included a more or less explicit justification. Proponents as well as opponents of 3D body scanners defended their views by citing the perceived efficiency or inefficiency of the machines in detecting various explosives (23.3%). Health (12.7%), security (12.1%), privacy (12.1%), quality of service (11.8%), costs (10.6%), legality (6.1%), and business (3%) were other repeatedly given justifications for actors' statements. Security and efficiency were coded together most frequently as explanations, followed by costs and

efficiency, then by privacy and health, then privacy and efficiency, then quality of service and efficiency, then health and efficiency, and finally quality of service and security.

Table 7: Justifications in relation to 3D body scanner

Justification	#	%
Efficiency	77	23.3%
Health	42	12.7%
Security	40	12.1%
Privacy	40	12.1%
Quality of service	39	11.8%
Costs	35	10.6%
Legality	20	6.1%
Dignity	17	5.2%
Business	10	3.0%
Other justification	9	2.7%
Freedom/Liberty	1	0.3%
Total	**330**	**100.0%**

The 3D body scanner controversy in the US newspapers revolved around the 'backscatter' type of scanners that the TSA wanted to introduce at US airports in increasing numbers after the failed terrorist bomb attack on Christmas Day 2009. As explained in a January 2010 NYT article, 'the scanning machines, called "backscatter scanners," deliver a dose of ionizing radiation equivalent to 1 per cent or less of the radiation in a dental X-ray. The amount is so small that the risk to an individual is negligible, according to radiation experts. But collectively, the radiation doses from the scanners incrementally increase the risk of fatal cancers among the thousands or millions of travellers [sic]who will be exposed, some radiation experts believe.'[79] Unlike metal detectors, the 'backscatter scanners' could detect objects made from other materials, such as plastic and ceramic.[80] Unlike the less controversial body scanners using the reportedly less harmful millimetre wave technology, the backscatters also produced much clearer images of the human body. In the wake of the failed attack and the following perception of an acute terrorist threat facing the USA, the TSA and other state authorities thus advocated the use of the backscatters in the name of security. President Obama called for 'greater use of "imaging technology" to spot weapons and explosives.'[81] A TSA spokesman said that the new security measures were introduced to 'keep the traveling public safe.'[82] Security officials were repeatedly heard saying that 'the new procedures were the only way to detect explosives hidden under clothing,' while the chief of the TSA reiterated that 'we cannot forget that less than one year ago a suicide

[79]Wald, Matthew L. 2010. "Cancer Risks Debated for Type of X-Ray Scan." *New York Times*, 9 January 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/01/09/health/09scanner.html.

[80]Stellin, Susan. 2010. "Are Scanners Worth the Risk?" *New York Times*, 7 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/12/travel/12prac.html.

[81]Wald, Matthew L. 2010. "Cancer Risks Debated for Type of X-Ray Scan." *New York Times*, 9 January 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/01/09/health/09scanner.html.

[82]Stellin, Susan. 2010. "Are Scanners Worth the Risk?" *New York Times*, 7 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/12/travel/12prac.html.

bomber with explosives in his underwear tried to bring down a plane over Detroit.'[83] President Obama claimed that the measures were 'the only ones right now that they [the TSA and his counterterrorism advisers] consider to be effective against the kind of threat that we saw in the Christmas Day bombing.'[84]

Other actors also recognised the need to introduce full body scanners for security reasons. In a 3-0 ruling, rejecting the claim that the full-body scans violated the Fourth Amendment's prohibition against unreasonable searches, the US Court of Appeals for the District of Columbia reasoned, 'The need to search airline passengers to ensure public safety can be particularly acute, and, crucially, an AIT [advanced imaging technology] scanner, unlike a magnetometer, is capable of detecting, and therefore of deterring, attempts to carry aboard airplanes explosives in liquid or powder form.'[85] Also citing security concerns, some passengers were reported to support the introduction of 3D body scanners. The WSJ wrote that 'many travellers say they have come to accept the electronic peek under their clothing.' The *Journal* further argued that 'public opinion polls show widespread acceptance in the U.S. of the technology, with many saying tighter security outweighs inconvenience.' The WSJ cited 'a small sampling at O'Hare' airport from early June 2010, which 'showed broad support for the scanners.' According to the poll, 'most people who came through the body-scanner had no problem with it.' A passenger was quoted saying about her experience: 'If it's for passenger protection, why not?'[86]

The biggest concerns of the scanner critics were potential health risks, privacy issues linked to the quality of service provided at airports, and even doubts about the ability of the scanners to efficiently prevent a terrorist attack. The NYT reported that the passenger feedback filed to the TSA about the scanners as a result of the above-discussed court ruling, addressed the issues of 'privacy, safety and efficacy' of body scanners, 'with a large majority of respondents objecting to the technology.'[87] Critics among passengers, privacy groups, and politicians were cited calling the machines the digital equivalent of a strip search' and saying

---

[83]Shane, Scott. 2010. "Administration to Seek Balance in Airport Screening." *New York Times*, 21 November 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/11/22/us/22tsa.html.

[84]Ibid.

[85]Kendall, Brent. 2011. "Court Rejects Challenge to Airport Body Scanners." *Wall Street Journal*, 15 January 2011. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424052702304203304576447953332822830.html.

[86]Mccartney, Scott. 2010. "Airport Screeners Reveal Travelers' Surly Side." *Wall Street Journal*, 9 June 2010. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424052748704749904575292542252755192.html.

[87]Stellin, Susan. 2013. "Trying Passenger Patience." *New York Times*, 15 April 2013. Web. Accessed 19 August 2013. http://www.nytimes.com/2013/04/16/business/public-pours-scorn-on-airport-body-scanners.html.
Wald, Matthew L. 2010. "Mixed Signals on Airport Scanners." *New York Times*, 13 January 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/01/13/us/13scanners.html?_r=0.

their ability to record images could be abused by operators.[88] A privacy group representative said: 'we're not denying that threats exist … The question is, are the solutions proposed effective and are they legal?'[89] Pilots and travellers were reportedly 'rebelling against scanners that douse them with X-rays and reveal their private parts.'[90] The alternative to going through the scanner was to submit to, what one article called, an 'enhanced pat down' conducted by a TSA employee, which some travellers had described as 'quite intimate'.[91] A female passenger, for instance, was quoted saying: 'I opt out of the scanners, and it's not a comfortable experience … There is no patting – they run their hands along every part of you.'[92]

Addressing those concerns, the government argued that passenger privacy would be maintained with the help of special software that would obscure the faces[93] or mask the particulars of passengers' bodies.[94] Republican Congressman Chaffetz, who filed 'an amendment blocking the use of full-body scanners as the main way of screening passengers who don't fit risk profiles,' indicated that he would be willing to drop it if the scanners used technology that ensured a passenger could not be identified during the scan.[95] However, based on emails received from readers, a report that travelers did 'not fully trust the security agency's assurances that the new machines are safe, that they can't be defeated by a terrorist and that personal privacy will be protected – at least, to the extent the agency has claimed'[96] Indeed, it was revealed that despite the TSA's promise 'not to store or transmit nude images of airline passengers made by whole-body scanners,' the Agency requested

---

[88]Ibid.

[89]Stellin, Susan. 2010. "Are Scanners Worth the Risk?" *New York Times*, 7 September 2010. Web. Accessed 19 August 2013.
http://www.nytimes.com/2010/09/12/travel/12prac.html.

[90]Shachtman, Noah. 2010. "Has Airport Security Gone Too Far?" *Wall Street Journal*, 17 November 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704658204575611031585381708.html.

[91]Stellin, Susan. 2010. "Are Scanners Worth the Risk?" *New York Times*, 7 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/12/travel/12prac.html.

[92]Stellin, Susan. 2013. "Trying Passenger Patience." *New York Times*, 15 April 2013. Web. Accessed 19 August 2013. http://www.nytimes.com/2013/04/16/business/public-pours-scorn-on-airport-body-scanners.html.

[93]Simpson, Cam and Daniel Michaels. 2010. "TSA Pressed on Full-Body Scans Despite Concerns." *Wall Street Journal*, 9 January 2010. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB126296286103421603.html.

[94]Mccartney, Scott. 2010. "Airport Screeners Reveal Travelers' Surly Side." *Wall Street Journal*, 9 June 2010. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424052748704749904575292542252755192.html.

[95]Simpson, Cam and Daniel Michaels. 2010. "TSA Pressed on Full-Body Scans Despite Concerns." *Wall Street Journal*, 9 January 2010. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB126296286103421603.html.

[96]Sharkey, Joe. 2010. "Radiation Questions Over a Body Scanner." *New York Times*, 26 July 2010. Web. Accessed 19 August 2013.
http://www.nytimes.com/2010/07/27/business/27road.html?gwh=C83901D128D32AABA74A69684B5F93CC.

scanner manufacturers to equip them with 'exactly those capabilities.'[97] The TSA thus failed to alleviate the fears of many of the scanners' opponents.

Passengers who had experienced the scanners were often dissatisfied with the quality of service. They described scenes of confusion, undignified situations with security staff behaving in a bullish way, making an impression that passengers could not refuse to go through a scan, or even suspicious selection criteria applied by airport screeners. One passenger 'was ordered to put his belt and other belongings through the baggage X-ray machine and step into a body-scanning machine.' When trying repeatedly to hold up his trousers, he was allegedly barked at by the screener 'to keep his hands over his head, prisoner-style. That way the machine could get clear pictures of the whole body.' The passenger thought that 'it was ridiculous' that he 'should be yelled at' because his 'pants were falling down' and subsequently filed a complaint with TSA.[98] Another passenger at a different airport noticed that 'screeners seemed to be directing young, good-looking people to the body-scanner, while children, older adults and overweight people were sent to the walk-through metal detector.' When she refused to be scanned because she was 'upset about the possible selection criteria and concerned about radiation exposure,' she was told by the TSA screener administering the pat-down that 'she was being "unpatriotic."' Frustrated, she said: 'We take our shoes off, our jackets off, don't carry liquids anymore and now I have to be completely patted down or peeped at to get on a plane.'[99] Travelers also complained that it was not always clear at airports that they had an option to refuse to be scanned and submit to a metal detector screening and a pat-down instead. 'It definitely didn't feel optional at all,' claimed one passenger. In response, the TSA claimed that it had learned some lessons in training' and was 'trying to better educate travelers about what to expect from body-scanning with signs at checkpoints.'[100]

Worried about the negative impact on their profits, airlines were also worried about the potential influence of introducing full-body scanners on the quality and speed of service. The International Transport Association was cited to be 'concerned about how the machines could slow the passenger screening process, and how they will fit logistically with current airport design.' The major goal of the airline industry was to make 'the screening process more efficient' as they were worried that as the economy improved and passenger traffic increased,

---

[97]Wald, Matthew L. 2010. "Mixed Signals on Airport Scanners." *New York Times*, 13 January 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/01/13/us/13scanners.html?_r=0.

[98]Mccartney, Scott. 2010. "Airport Screeners Reveal Travelers' Surly Side." *Wall Street Journal*, 9 June 2010. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424052748704749904575292542252755192.html.

[99]Ibid.

[100]Mccartney, Scott. 2010. "Airport Screeners Reveal Travelers' Surly Side." *Wall Street Journal*, 9 June 2010. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424052748704749904575292542252755192.html.

security lines would slow down, deterring people from traveling.[101] Passenger, or customer experience, thus seemed to be an important aspect influencing the satisfaction and acceptance of the airport security measures by different actors.

Despite the TSA's assurances that full-body scanners are completely safe and that they had been thoroughly tested, experts and the public expressed doubts about the health risks the scanners posed. The main concerns related to the amount of radiation emitted by scanners, to the possibility of malfunction and consequent increased levels of radiation, and the health effects this may have for travelers. The TSA argued that 'the machines have been approved by the Federal Drug Administration [FDA] and other agencies as safe for human use, even for pregnant women,' and that radiation emission from the scanners 'is the equivalent to the exposure each person receives in about two minutes of airplane flight at altitude.'[102] In the words of an FDA spokesman, 'If there is any risk, it's very, very small,' as 'an individual could receive up to 1,000 screenings a year before reaching recommended annual limits for this type of radiation exposure.'[103] For those concerned about their health, the TSA said that it anticipated 'making the machines permanently optional, letting travelers choose between a body scan or pat-down by hand.[104]

However, some articles pointed to the fact that the scanners had actually not been 'thoroughly tested.' According to the NYT, the only aspect of the scanners that had been tested was 'whether the amount of radiation emitted meets guidelines established by the American National Standards Institute.' Those guidelines for X-ray scanners, however, were reported to have been developed by a committee comprised of 'representatives from the companies that make the machines and the Department of Homeland Security.' In the words of the NYT journalist, 'the machines passed a test developed, in part, by the companies that manufacture them and the government agency that wants to use them.'[105] Thus an expert argued: 'The scary thing to me is not what happens in normal operations, but what happens if the machine fails… Mechanical things break down, frequently.'[106] Another commentator was worried about the possible malfunctioning of the machines when not operated by experts.

---

[101]Stellin, Susan. 2011. "Support Grows for Tiered Risk System at Airports." *New York Times*, 7 February 2011. Web. Accessed 19 August 2013. http://www.nytimes.com/2011/02/08/business/08security.html.

[102]Mccartney, Scott. 2010. "Airport Screeners Reveal Travelers' Surly Side." *Wall Street Journal*, 9 June 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704749904575292542252755192.html.

[103]Stellin, Susan. 2010. "Are Scanners Worth the Risk?" *New York Times*, 7 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/12/travel/12prac.html.

[104]Mccartney, Scott. 2010. "Airport Screeners Reveal Travelers' Surly Side." *Wall Street Journal*, 9 June 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704749904575292542252755192.html.

[105]Stellin, Susan. 2010. "Are Scanners Worth the Risk?" *New York Times*, 7 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/12/travel/12prac.html.

[106]Ibid.

> 'Recent research has demonstrated that the cancer risks of radiation have been grossly underestimated, even for medical equipment operated by qualified radiologists and their trained technicians. It is therefore no good showing that in the manufacturer's tests the level of radiation is only moderately harmful, because once distributed at airports, those machines will not necessarily be perfectly calibrated, nor will they be operated correctly by experts.'[107]

The risks of radiation exposure were not just debated among experts, but were portrayed as real concerns for passengers, too. A WSJ reporter argued, 'radiation is a hot issue, so to speak. Reader reaction to the backscatters has ranged from a few claiming "there is no safe level of radiation exposure" to the many others expressing concern that the T.S.A. has rushed into buying these devices without adequately assessing the health question of repeated exposure to radiation.'[108] A passenger said that when she asked an airport screener about the amount of radiation she would be exposed to, she was given 'a cryptic answer saying it was the same as just a few minutes of sunshine.' Even when she asked for more details regarding the units of radiation, the screener could not answer. The passenger claimed: 'I don't appreciate being touched all over but I prefer that to adding to my cancer risk.' She added: 'I think the public is basically uninformed and unless this is clarified, why do it?'[109]

Given the above concerns and the high costs of installing numerous new full-body scanners at US airports, some actors questioned the efficiency and need for the machines. A security expert writing for the WSJ considered the machines not only extremely expensive, inconvenient for passengers, and potentially dangerous. He also found them futile in the TSA's security effort because they could not reveal explosives hidden inside human cavities. In the expert's opinion, machines that would be able to do so would, on the other hand, be unacceptably intrusive of travelers' privacy:

> 'The scanners … would perpetuate futility at even greater cost. True, it is perfectly feasible to design very high definition scanners that could detect objects inside body cavities, and at least one manufacturer already claims that capability. But to use those scanners would throw out any pretense of preserving privacy. It also would mean

---

[107]Luttwak, Edward N. 2010. "The Body Scanner Scam." *Wall Street Journal*, 18 January 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704541004575010962154452900.html.

[108]Sharkey, Joe. 2010. "Radiation Questions Over a Body Scanner." *New York Times*, 26 July 2010. Web. Accessed 19 August 2013.
http://www.nytimes.com/2010/07/27/business/27road.html?gwh=C83901D128D32AABA74A69684B5F93CC.

[109]Mccartney, Scott. 2010. "Airport Screeners Reveal Travelers' Surly Side." *Wall Street Journal*, 9 June 2010. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424052748704749904575292542252755192.html.

subjecting every passenger to whatever level of radiation those machines will emit.'[110]

Others also questioned the 'TSA's tech-centric approach to security'. A *Wall Street Journal* commentator claimed that, '[e]ven the most modest of us would probably agree to a brief flash of quasi-nudity if it would really ensure a safe flight.' However, he thought that body scanners merely provided 'incremental, uncertain security improvements against particular kinds of concealed weapons.' He compared this kind of trade-off to that provided when the TSA ordered passengers to take off their shoes and prohibited liquids on board of airplanes in order to prevent shoe bombs and liquid explosives, respectively. A security guru cited by the commentator called this approach 'magical thinking… Descend on what the terrorists happened to do last time, and we'll all be safe. As if they won't think of something else. [sic]' However, pointing to the fact that terrorists were 'starting to smuggle weapons in body cavities, going where even the most droit [sic] body scanners do not tread,' he dismissed the need to introduce the backscatters. 'No wonder that the Israelis, known for the world's most stringent airport security, have so far passed on the scanners', he added.[111]

Due to the alleged inefficiency of scanners, some experts called for alternative measures, which they thought would be able to alleviate passengers' concerns and ensure their safety. Writing for the WSJ opinion section, one expert claimed that screening passengers 'as persons instead of their bodies and belongings' was the logical alternative to scanners, 'which costs much less, inflicts much less inconvenience and would have a much higher probability of intercepting terrorists before the fact'. In his opinion, the 'overwhelming advantage' of such an approach was that it could 'detect a would-be terrorist even if the specific technique he tries to employ is not previously known.' Within the bounds of this procedure, 'many individuals could also be included in the document examination plus random check category: frequent travelers who have multiyear travel records with airline alliances, whose travel history could instantly be determined by the TSA', for instance. 'The aim would be to identify innocent travelers as quickly as possible to send them on their way, while being ready to persist with further questions that might even end with the denial of boarding and a referral to police authorities.' The expert concluded that 'with such a system that would discriminate only positively – only in favor of groups and categories of passengers, and never against them – we could have real security at a drastically lower cost in money and inconvenience.'[112]

---

[110]Luttwak, Edward N. 2010. "The Body Scanner Scam." *Wall Street Journal*, 18 January 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704541004575010962154452900.html.

[111]Shachtman, Noah. 2010. "Has Airport Security Gone Too Far?" *Wall Street Journal*, 17 November 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704658204575611031585381708.html.

[112]Luttwak, Edward N. 2010. "The Body Scanner Scam." *Wall Street Journal*, 18 January 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704541004575010962154452900.html.

In contrast, responding to prominent Republican politicians' criticism of the scanning procedures and suggestions to start profiling passengers instead, the *New York Times* was not absolutely convinced by the merits of such an approach. One Republican politician, for example, was quoted calling the scanners and pat-downs a 'humiliating and degrading, totally unconstitutional intrusion.' 'If the president thinks such searches are appropriate," the politician continued, "he should subject his wife, two daughters, and mother-in-law to them.' The NYT, however, argued that 'the Obama administration should weather this storm by realizing these attacks are purely partisan and ideological. Americans know the difference between a big scanner and big government.'[113] The editorial acknowledged that 'some individual pat-downs have gone too far,' and that the TSA 'was ham-handed in answering those concerns.' Nonetheless, it viewed the proposals of some Republicans as both violating civil liberties and ineffective:

> 'It is bad enough that many of these politicians seem happy to trade away a long and proud history of civil liberties over a few moments of inconvenience in the airport. But even beyond the violation of such a basic principle, it has long been clear that the substitution of profiling for searches simply doesn't work. The T.S.A. already pulls aside travelers for extra searching and questioning based on their nationality and travel patterns. But terrorists, tragically, aren't fools, and constantly adapt to the screening regimes. Before the T.S.A. started searching for bombs in shoes, underwear or printer cartridges, that's where they were hidden. If terrorists learn that elderly white women from Iowa are exempt from screening, that's exactly whom they will recruit.'[114]

In another article, a NYT commentator also discussed the partisan political tendencies that became apparent in the body scanner controversy:

> 'But Barack Obama is our president instead, so the body-scanner debate played out rather differently… It was the populist right that raged against body scans, and the Republican Party that moved briskly to exploit the furor. It was a Democratic administration that labored to justify the intrusive procedures, and the liberal commentariat that leaped to their defense.'

According to the commentator, the power of partisanship in the scanner controversy was evident as 'millions of liberals' could 'live with indefinite detention for accused terrorists and intimate body scans for everyone else,' as long as a Democrat was 'overseeing them.' At the

[113]"Politicizing Airport Security." 2010. *New York Times*, 23 November 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/11/24/opinion/24wed2.html.
[114]Ibid.

same time, 'millions of conservatives' found 'wartime security measures vastly more frightening when they're pushed by Janet "Big Sis" Napolitano'. Arguing that there was nothing good to be said about the partisan mindset on an individual level, he found 'a modest virtue' in it for the whole country. Partisanship guaranteed that 'even when there's an elite consensus behind whatever the ruling party wants to do…, there will always be a reasonably passionate opposition as well'. The commenter thought that 'even a hypocritical and inconsistent opposition' was 'better than no opposition at all' because it guaranteed that there would 'always be someone around, when Americans are standing spread-eagled and exposed in the glare of Rapiscan [the manufacturer of scanners], to speak up and say "enough!"'[115]

Under mounting pressure from different corners, the TSA and lawmakers gradually abandoned their fervent advocacy of the need for body scanners. Lawmakers 'dissatisfied with the performance of the Transportation Security Administration' were in January 2012 pushing to revive a proposal that would allow airports to use screeners hired by private contractors.' This step was welcomed by many in the air travel industry who thought they could do it cheaper and more effectively, while ensuring more security for passengers.[116] The support for various types of tiered screening procedures also grew over time. In an attempt to improve its relationship with travellers, in 2012, the TSA introduced two different types of expedited screening programmes at large airports – the 'Pre-check' and 'Global Entry' programmes. 'When the agency was set up, it was focused almost exclusively on the security mission and not as much on the passenger experience,' the TSA chief said. 'It became an adversarial relationship, so what we're trying to do through all these initiatives is change that paradigm and make this a partnership.'[117] Passengers welcomed the change of approach in relation to screening procedures. A frequent flier, for instance, claimed, 'It's a completely different experience than what you're used to.' In addition to going through security screening quickly and easily, he also noticed that TSA agents at the 'Pre-check' lane would usually be smiling. 'It's really a jarring contrast. It reminds you just how much of a hassle the security procedures in place really are,' he argued.[118]

Following complaints from passengers and a Congressional mandate, TSA announced a withdrawal of the controversial backscatters by June 2013. They were to be replaced with

---

[115]Douthat, Ross. 2010. "The Partisan Mind." *New York Times*, 28 November 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/11/29/opinion/29douthat.html.

[116]Stellin, Susan. 2012. "Gatekeepers Under Scrutiny." *New York Times*, 30 January 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/01/31/business/lawmakers-push-for-more-private-screeners-at-airports.html.

[117]Stellin, Susan. 2012. "A Quest for Speedier and Smarter Airport Security." *New York Times*, 17 December 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/12/18/business/a-quest-for-speedier-and-smarter-airport-security.html.

[118]Ibid.

the less harmful millimetre-wave scanners. In June 2012, Congress passed a bill, which banned detailed body images in airport security screenings, granting the TSA a one-year extension. Since the scanners' producer was unable to change the technology to comply with the law, the 'backscatter' controversy concluded with a victory for privacy advocates. 'This solves our most significant concern' said a representative of a privacy group. 'Not having TSA agents sitting in darkened rooms looking at naked pictures of people getting on a plane is a good outcome.'[119]

5. 2. Stuxnet

5. 2. 1. Quality of articles and topics discussed

The length, quality and style of articles coded about Stuxnet varied. We coded six articles from *The Wall Street Journal* and nine from *The New York Times*. While the majority of articles were around 800 words in length, the seminal article by David Sanger, [120] cited by media all over the world, was considerably longer, providing detailed information about the development and deployment of Stuxnet. We coded three opinion pieces (two from the WSJ and one from the NYT), with other articles found in the technology, World/Middle East, and US sections of the dailies. Over time, the topic was thus framed in a number of different ways – as technology news, world news, as well as domestic news, depending on the specific aspect emphasised by the individual author. We found several topics that were covered by one newspaper, while not covered at all in the other. The WSJ, for instance wrote about the attacks of a virus named Duqu, which the WSJ called 'Stuxnet's son.'[121] The *Journal* also published an expert interview discussing the options the US had to react to Chinese cyber-attacks on American targets.[122] The NYT, on the other hand, discussed the increasing cyber-attacks targeting US infrastructure as a response to America's cyber operations.[123] The *Times*

[119]Nicas, Jack. 2013. "TSA to Halt Revealing Body Scans at Airports." *Wall Street Journal*, 18 January 2013. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424127887323783704578250152613273568.html.
[120]Sanger, David E. 2012. "Obama Order Sped Up Wave of
Cyberattacks Against Iran." New York Times, 1 June 2012. Web. Accessed 19 August 2013.
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&pagewanted=print.
[121]Rooney, Ben. 2011. "'Son of Stuxnet' Virus Targets Specific Organizations, Assets." *Wall Street Journal*, 24 October 2011. Web. Accessed 19. August 2013.
http://online.wsj.com/article/SB10001424052970204485304576642654085725710.html.
[122]Feith, David. 2013. "Timothy Thomas: Why China Is Reading Your Email." *Wall Street Journal*, 29 March 2013. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424127887323419104578376042379430724.html.
[123]Sanger, David E. and Eric P. Schmitt. 2012. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." *New York Times*, 26 July 2012. Web. Accessed 19 August 2013.
http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html.

also drew attention to the gap in Internet security certificates revealed after a counter-attack by an Iranian hacking activist, and reported on the first official attempts to publicly discuss America's cyber warfare efforts,[124] urging the US to push for international rules on the use of cyber warfare.[125]

5. 2. 2. Content analysis: Actors and themes

The coverage of the Stuxnet attacks attracted the second largest number of coded statements. While the single most frequently coded actor were experts with 18.6%, the discussions about the Stuxnet phenomenon were dominated by the actions and opinions of various states and state institutions, or their representatives (coded under 'state institutions', 'state(s)', presidents), which were presented in 36.6% of statements. The next most frequently coded actors were journalists (18.3%). As in the case of the 3D body scanner coverage, the newspapers seemingly observed the professional principles of objectivity, given that 20% of all coded articles were found in the opinion sections. Stuxnet featured as an actor in 5.2% of cases, followed by the US National Security Agency (4.8%), officials involved with Operation Olympic Games (4.5%, coded as 'others'), private companies active in the Internet security industry, as well as those that came under attack by Stuxnet (4.1%), and UN nuclear inspectors (2.1%). In contrast to 3D body scanners, the Stuxnet issue was not framed solely in domestic terms. Whilst 66% of all living actors came from the US, 10% were of Iranian origin, 8.9% were mentioned generally, and 5.8% were of Israeli origin.

We coded seven cases of cooperation. These involved either the cooperation between USA and Israel, or their respective security agencies on operation Olympic Games and/or developing and deploying Stuxnet. *The Wall Street Journal* reported, for instance, that 'a key element of Olympic Games which hasn't been previously disclosed was a partnership between the CIA's Information Operations Center and the Idaho National Laboratory.'[126] Sanger wrote about the US-Israeli cooperation: 'Then the N.S.A. and a secret Israeli unit respected by American intelligence officials for its cyber skills set to work developing the enormously complex computer worm that would become the attacker from within.'[127] Other cases of

[124]Shane, Scott. 2012. "Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials." *New York Times*, 26 September 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all.

[125]Glenny, Misha. 2012. "A Weapon We Can't Control." *New York Times*, 24 June 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html.

[126]Gorman, Siobhan. 2012. "U.S. Team and Israel Developed Iran Worm." *Wall Street Journal*, 1 June 2012. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052702304821304577440703810436564.html.

[127]Sanger, David E. 2012. "Obama Order Sped Up Wave of

cooperation among actors were related to the reported collaboration between Presidents Bush and Obama on operation Olympic Games. Sanger described in the following terms: 'Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice (sic).'[128]

Table 8: Actors coded in relation to Stuxnet and their origin

Actor	#	%	Actor's origin										Total
			USA	National	Iran	Other	Israel	China	Russia	International	Supranational	Mentioned generally	
Experts	54	18.6%	32	0	0	7	0	0	0	0	0	15	54
Journalist	53	18.3%	53	0	0	0	0	0	0	0	0	0	53
State institutions	53	18.3%	39	0	6	2	3	2	0	1	0	0	53
State(s)	37	12.8%	12	1	14	0	8	1	1	0	0	0	37
President	16	5.5%	15	0	1	0	0	0	0	0	0	0	16
Stuxnet	15	5.2%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
National Security Agency	14	4.8%	14	0	0	0	0	0	0	0	0	0	14
Others	13	4.5%	6	0	0	0	0	0	0	0	1	6	13
Private company	12	4.1%	8	0	0	3	0	0	1	0	0	0	12
Institutions	6	2.1%	0	0	1	0	0	0	0	5	0	0	6
Activists	4	1.4%	0	0	3	0	0	0	0	0	0	1	4
Media	4	1.4%	1	0	2	0	0	0	0	0	0	1	4
Israel secret service	3	1.0%	0	0	0	0	3	0	0	0	0	0	3
Flame	3	1.0%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virus/Malware/Worm	2	0.7%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Non-state institutions	1	0.3%	0	0	0	0	0	0	0	0	0	1	1
Total	**290**	**100%**	**180**	**1**	**27**	**12**	**14**	**3**	**2**	**6**	**1**	**24**	**270**

The coverage of Stuxnet revolved around the themes of the deployment or attack using Stuxnet (18.4%) and Iran's nuclear programme (17.1%). These two themes were also most commonly cited together in statements about Stuxnet. The discussions addressed a myriad of other topics, including the development of Stuxnet by a state (6.8%), the operation Olympic

Cyberattacks Against Iran." New York Times, 1 June 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&pagewanted=print.

[128]Ibid.

Games (5.3%), the characteristics of Stuxnet itself (5.3%), cyber wars led by states (5%), different cyber-attacks on Iran (5.%), cyber-attacks on private companies (5%), and the lack of rules and regulations governing the deployment of cyber weapons (4.5%). The coverage also touched on several cyber-attacks on other states (4%), counterattacks as a result of the deployment of Stuxnet (3.8%), and the willingness of US authorities to publicly discuss the development of cyber weapons (3.5%, coded as 'communication'). Operation Olympic Games was often mentioned together with the Iranian nuclear programme, as were cyber war and communication, and also security-related rules and regulations and legality.

Table 9: Topics coded in relation to Stuxnet

Topic	#	%
Deployment/attack using Stuxnet	73	18.4%
Iranian uranium enrichment programme	68	17.1%
Development of Stuxnet by a state	27	6.8%
Olympic Games	21	5.3%
Stuxnet	21	5.3%
Cyber war	20	5.0%
Attack on Iran	20	5.0%
Attack on a company	20	5.0%
Security-related rules and regulations	18	4.5%
Attack on other state	16	4.0%
Counter-Attack	15	3.8%
Attack	15	3.8%
Communication	14	3.5%
USA accused of attack	12	3.0%
State accused of attack	9	2.3%
Israel accused of attack	9	2.3%
Development of Stuxnet	6	1.5%
Legality	5	1.3%
Flame	5	1.3%
Security General	2	0.5%
Privacy	1	0.3%
Total	**397**	**100.0%**

5. 2. 3. Content analysis: Discussions about Stuxnet

In contrast to the controversy around the use of 3D body scanners, which attracted a lot of value-laden discourse in the press, the discussions about Stuxnet were much more factual. We ascribed a definitive argumentative strategy to 72% of coded statements, while we found 22.5% of arguments about Stuxnet to be evaluative and 5.5% advocative. The coverage was thus largely focused on reporting the Stuxnet attacks over time, outlining the characteristics of the virus, its development, and the reasons behind it, as well as the increasing cyber

warfare among states, its effects, and the lack of rules governing it. Of the evaluative and advocative statements, the majority (60%) were negative. The evaluative and advocative views conveyed by the coverage, however, were rather more negative than is apparent from these figures. The coded statements did not merely evaluate the Stuxnet virus. The positive ones also spoke of the need for establishing international cyber warfare rules, for instance.

Table 10: Argumentative strategies and direction of arguments about Stuxnet

Argumentative strategy	**#**	**%**	**Direction of argument**					
			positive		negative		neutral	
			#	%	**#**	%	**#**	%
Definitive	198	72.0%	0	0%	15	7.6%	183	92.4%
Evaluative	62	22.5%	15	24.2%	42	67.7%	5	8.1%
Advocative	15	5.5%	13	86.7%	2	3.2%	0	0%
Total	**275**	**100%**	**28**		**59**		**188**	

Almost a third of all statements (31.6%) comprised a justification. The actors most frequently justified their statements by referring to security needs (35.7%) and efficiency or sophistication of Stuxnet or other malware and cyber-attacks (35.7%). These two justifications were also most often cited together. In addition, defence was offered as reasoning for statements in 8.2% of cases, often in combination with efficiency. Actors also based their views of Stuxnet on the perceived need for a pre-emptive strike (6.1%) and expert opinion (5.1%). Costs (2%), legality (2%), political credibility (1%), liberty (1%), and privacy (1%), on the other hand, were used as justification only marginally.

Table 11: Justifications in relation to Stuxnet

Justification	**#**	**%**
Security	35	35.7%
Efficiency	35	35.7%
Defence	8	8.2%
Pre-emptive strike	6	6.1%
Expert opinion	5	5.1%
Costs	2	2.0%
Experimentation	2	2.0%
Legality	2	2.0%
Political credibility	1	1.0%
Freedom/Liberty	1	1.0%
Privacy	1	1.0%
Total	**98**	**100.0%**

Presidents Bush and Obama, and other US officials were among the supporters of Stuxnet. They viewed the virus as crucial in their effort to delay or hinder the Iranian uranium enrichment programme, which they considered a direct security threat to the US

and the West. According to David Sanger, the impetus for operation Olympic Games, which included the development and deployment of Stuxnet, came in 2006, 'when President George W. Bush saw few good options in dealing with Iran'. Then security officials presented him with 'a radical new idea' involving 'a far more sophisticated cyber weapon than the United States had designed before.' While no one expected the initial tests to be as successful as they were, they proved that Stuxnet was ready to be deployed in Iran.[129] Praising the effectiveness of Stuxnet, the former Chief of the CIA argued that 'somebody crossed the Rubicon' with the virus. While previous cyber-attacks had had limited effects, the Stuxnet attack was the first major attack in which a cyber-attack was deployed to achieve physical destruction, rather than merely slow another computer, or hack into it to steal data. Officials involved with the development and deployment of the virus also admired the ingenuity and destructiveness of Stuxnet. An official thought that the fact that Stuxnet could operate inside the Iranian nuclear plant, destroying centrifuges for weeks without being noticed, leaving the Iranians confused about what was going on, 'may have been the most brilliant part of the code.' Another participant in the attacks claimed that the attack was successful in making the Iranians 'feel they were stupid' when Stuxnet made centrifuges fail without any apparent reason.[130]

Given the virus's role in damaging Iranian centrifuges, President Obama reportedly decided to continue and even intensify operation Olympic Games even after Stuxnet 'escaped' from the Iranian nuclear plant in Natanz. However, President Obama was allegedly troubled about 'pushing the United States into new territory' with every new attack. He was concerned that 'any American acknowledgment that it was using cyber weapons – even under the most careful and limited circumstances – could enable other countries, terrorists or hackers to justify their own attacks.' Nonetheless, Obama reportedly concluded that the Stuxnet attacks were the only way to stop Iran's uranium enrichment programme. Cyber-attacks targeting Iran were a pre-emptive strategy to avoid an Israeli military attack, which could destabilise the Middle East. If Olympic Games failed, Obama was cited to have said to his advisors, 'there would be no time for sanctions and diplomacy with Iran to work' because 'Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.'[131] Viewing cyber-attacks positively, some US officials even questioned why they had not been used more aggressively against North Korea, or to disrupt

[129]Sanger, David E. 2012. "Obama Order Sped Up Wave of Cyberattacks Against Iran." New York Times, 1 June 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&pagewanted=print.

[130]Ibid.

[131]Ibid.

Chinese military plans, suppress the conflict in Syria, or used world-wide in operations against Al Qaeda.[132]

However, many commentators and experts, as well as American businesses that became victims of attacks in retaliation to the Stuxnet virus, were not convinced about the US and Israel's achievements with the virus. Some argued that even if Stuxnet managed to delay Iran's nuclear programme, the security threat posed by Iran was not eradicated because Iran was still able to produce an atomic bomb. Comparing the Stuxnet attack to a so-called 'Farewell' spy dossier employed to confuse the Soviets during the Cold War, a WSJ commentator argued that Stuxnet's apparent success 'cannot be a cause for complacency,' since 'wars are never won by covert means alone.' He noted that even though Stuxnet temporarily stopped 'further expansion of Iran's enrichment activities,' the Iranian nuclear programme continued after the 2009 attack. He argued that regardless of the Stuxnet attack, with further enrichment, Iran already possessed enough fissile material for two or three atomic bombs. Moreover, the commentator claimed that Iran could quite easily obtain enriched uranium from North Korea or China. Since 'Pyongyang has already demonstrated its willingness to build a secret reactor for Syria,' he asked why it would not 'export enriched uranium to Iran, a country with which it already does a thriving trade in WMD-related technologies and to which it is deeply in debt?' Finally, he warned that Iran was 'not likely to be fooled again' with a cyber-attack, meaning future attacks would be much less targeted and not as bloodless.[133]

Vindicating the above viewpoint, in January 2013, Iran announced its plans to upgrade its main nuclear plant at Natanz, which could accelerate uranium enrichment by a factor of two or three. However, in this regards another expert argued that 'Iran has a long history of overstating its capabilities, and both the number of machines that Iran can deploy and their effectiveness is not yet known.' Be that as it may, it has also been reported that a few years after the Stuxnet sabotage, 'a newer uranium enrichment plant, known as Fordo, has raised Western concerns because it is buried deep underground, making it more impervious to scrutiny or attack.'[134]

Others were unimpressed by Stuxnet and its developers because of the damage it caused to computer systems worldwide after it had 'escaped' from the Natanz nuclear site. A NYT reporter wrote: 'the most striking aspect of the fast-spreading malicious computer program… may not have been how sophisticated it was, but rather how sloppy its creators

---

[132]Ibid.

[133]Stephens, Bret. 2011. "The Limits of Stuxnet." *Wall Street Journal*, 18 January 2011. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html.

[134]Cowell, Alan. 2013. "Iran Said to Be Set to Hasten Uranium Enrichment." *New York Times*, 31 January 2013. Web. Accessed 19 August 2013. http://www.nytimes.com/2013/02/01/world/middleeast/iran-is-said-to-be-set-to-accelerate-uranium-enrichment.html.

were in letting a specifically aimed attack scatter randomly around the globe.'[135] The representative the US oil giant Chevron, whose networks Stuxnet attacked in 2010, was convinced that the downside of the government-led cyber-attacks was 'going to be far worse than what they actually accomplished.' He saw the efforts of the authorities to tackle Iran's nuclear programmes in a rather negative light because his and other companies had to deal with the Stuxnet attacks damaging their systems.[136]

Numerous experts feared the risk of proliferation of cyber-attacks. Already in 2010, the NYT reported, 'Stuxnet has laid bare significant vulnerabilities in industrial control systems. The program is being examined for clues not only by the world's computer security companies, but also by intelligence agencies and countless hackers.'[137] A group of industrial control specialists warned that 'the widespread distribution of the Stuxnet code could lead to disaster' because equipment produced by Siemens and its competitors is used worldwide to manage transportation, power distribution, and communications systems.[138] A former US national cyber security coordinator argued that 'the widespread availability of the attack techniques revealed by the software has set off alarms among industrial control specialists,' who were 'scared to death.'[139] Another cyber security expert explained that the real worry was 'that instead of just stealing information, [hackers are] gaining control of target systems so that they can cause physical damage.'[140] Yet another expert was concerned that computer security organizations were not adequately communicating the potential for serious industrial sabotage that Stuxnet presents. He said: 'I just want the lights to stay on and water flowing, and people not dying.'[141]

It would appear from the coverage in the US press that some of the experts' fears have materialised. In the opinion of one expert, Stuxnet 'opened Pandora's box,' since 'whatever restraint might have been holding damaging attacks back' was gone and while targeting

---

[135]Markoff, John. 2010. "A Silent Attack, but Not a Subtle One." *New York Times*, 26 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/27/technology/27virus.html.

[136]King, Rachael. 2012. "Virus Aimed at Iran Infected Chevron Network." *Wall Street Journal*, 9 November 2012. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424127887324894104578107223667421796.html.

[137]Markoff, John. 2010. "A Silent Attack, but Not a Subtle One." *New York Times*, 26 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/27/technology/27virus.html.

[138]Markoff, John. 2010. "Worm Can Deal Double Blow to Nuclear Program." *New York Times*, 19 November 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html.

[139]Markoff, John. 2010. "A Silent Attack, but Not a Subtle One." *New York Times*, 26 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/27/technology/27virus.html.

[140]King, Rachael. 2012. "Virus Aimed at Iran Infected Chevron Network." *Wall Street Journal*, 9 November 2012. Web. Accessed 19 August 2013.
http://online.wsj.com/article/SB10001424127887324894104578107223667421796.html.
Markoff, John. 2010. "A Silent Attack, but Not a Subtle One." *New York Times*, 26 September 2010.

[141]Markoff, John. 2010. "Worm Can Deal Double Blow to Nuclear Program." *New York Times*, 19 November 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html.

American companies in particular, hackers 'went from stealing information to using cyberattacks to cause destruction.' [142] In March 2011, a young Iranian activist working alone attacked the US Internet security company Comodo to avenge the Stuxnet attacks. He claimed that he intended 'to snoop on opponents of the Iranian regime'. He warned, 'As I live, you don't have privacy [on the] Internet, you don't have security in [the] digital world.'[143] In July 2012, General Alexander stated that between 2009 and 2011 American infrastructure had seen a 17-fold increase in computer attacks by criminal gangs, hackers, and other nations. General Alexander argued that those attacks were not related to the deployment of Stuxnet. Nonetheless, the NYT saw his speech as 'the government's first official acknowledgment of the pace at which America's electricity grids, water supplies, computer and cellphone networks, and other infrastructure are coming under attack', implying a direct connection to Stuxnet.[144] Arguing cyber-attacks have escalated in speed and scale during the past few months, the WSJ reported about attacks on Saudi Arabian Oil Co. and a Qatari natural-gas company, which were thought to be of Iranian origin.[145] Moreover, several experts claimed that parts of the Stuxnet code had already been used to facilitate financial cybercrimes such as stealing bank-account information and credit card data. To what proportions the risks connected to the deployment of Stuxnet could grow becomes clear from the words of yet another cyber security expert, 'Employees who have a deep understanding of cyber security and their company's systems are the only defense [sic] against viruses like Stuxnet… There are probably only 18 to 20 people in the [U.S.] who have those fundamental skills.'[146]

Other experts and commentators saw the development and deployment of Stuxnet by the US and Israel as dangerous because it could lead to a militarisation of or even an uncontrolled arms race in cyberspace. According to an expert, 'Stuxnet has effectively fired the starting gun in a new arms race that is very likely to lead to the spread of similar and still more powerful offensive cyber weaponry across the Internet.' The greatest threat of such developments was that in contrast to nuclear or chemical weapons, states were acquiring cyber weapons outside any regulatory framework. The expert thought that one of the 'frightening dangers of an uncontrolled arms race in cyberspace' was that 'once released,

---

[142]King, Rachael. 2012. "Virus Aimed at Iran Infected Chevron Network." *Wall Street Journal*, 9 November 2012. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424127887324894104578107223667421796.html.

[143]Richmond, Riva. 2011. "An Attack Sheds Light on Internet Security Holes." *New York Times*, 7 April 2011. Web. Accessed 19 August 2013. http://www.nytimes.com/2011/04/07/technology/07hack.html.

[144]Sanger, David E. and Eric P. Schmitt. 2012. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." *New York Times*, 26 July 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html.

[145]King, Rachael. 2012. "Virus Aimed at Iran Infected Chevron Network." *Wall Street Journal*, 9 November 2012. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424127887324894104578107223667421796.html.

[146]Ibid.

virus developers generally lose control of their inventions, which will inevitably seek out and attack the networks of innocent parties.' In addition, he believed that all states in possession of cyber weapons would be tempted to deploy them as a result of the Stuxnet attacks. He thus urged the US to initiate talks on an international treaty on the use of cyber weapons before to 'the monster it [the US] has unleashed comes home to roost.'[147]

While some actors were concerned that greater openness about US cyber capabilities could trigger a global arms race, more experts were quoted advocating for open discussions of the US actions concerning cyber warfare. An Arms Control Association representative, argued, for instance that 'more talk about the United States' cyber warfare capabilities might prompt other countries to step up their own programs at a time when the world is "on the cusp of a cyber-arms race."'[148] The proponents of open discussion, on the other hand, thought that it 'would allow the United States to stake out legal and ethical rules in the uncharted territory of computer combat.'[149] A former Defense Department official argued that 'speaking openly about cyber warfare policy was important because it allowed the United States to make clear its intentions on a novel and fast-emerging form of conflict.' Since both the Bush and Obama administrations were reluctant to speak publicly about the USA's use of armed drones, in his opinion, 'they ceded a lot of ground to critics to shape the narrative and portray U.S. practices as lawless.' As a consequence, the US was 'trying to play catch-up, giving speech after speech, saying "We abide by the law."' He argued that because the US still occupied 'a position of advantage on offensive cyber capabilities, it should seize the opportunity to lay out a set of rules for itself and others.'[150] Yet another expert claimed that the United States must begin discussions with the world's major powers about the rules governing the Internet as a military domain because its technical superiority was 'not written in stone'. Moreover, he argued that the US was more 'dependent on networked computer systems than any other country in the world.' The expert thus urged Washington to 'halt the spiral toward an arms race,' which he thought in the long term it was 'not guaranteed to win'.[151]

In a stark contrast, 'one of America's foremost experts' on Chines warfare argued in an interview for the Wall Street Journal that since 'Beijing's cyber-attacks are rooted in military strategy,' the best way to combat them was for the U.S. to go on the cyber offensive too.'

---

[147]Glenny, Misha. 2012. "A Weapon We Can't Control." *New York Times*, 24 June 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html.

[148]Shane, Scott. 2012. "Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials." *New York Times*, 26 September 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all.

[149]Ibid.

[150]Ibid.

[151]Glenny, Misha. 2012. "A Weapon We Can't Control." *New York Times*, 24 June 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html.

Implying that 'the best defense is a good offense,' the expert dismissed talks about establishing international standards for cyber space. Instead, he advocated 'building deterrence through offensive capabilities, such as the 13 new teams at the U.S. Cyber Command'. The expert asserted that 'there might be some comfort in knowing that the U.S. is doing unto China what China is doing unto the U.S.,' but he thought that 'we [sic] don't seem as intrusive as the other side.'[152]

5. 3. CCTV cameras

5. 3. 1. Quality of articles and topics discussed

We coded seven articles about CCTV cameras, of which four were found in *The New York Times* and three in *The Wall Street Journal*. The articles varied in length as well as quality and quantity of arguments. The NYT articles were between 900 and 1100 words long, while the WSJ reports ranged from 260 to 1450 words in length. We found informative statements as well sound arguments about the benefits and risks of using CCTV cameras in articles from both papers. Two of the articles (both from the NYT) were found in the opinion/commentary section of the paper, providing evaluative statements from their authors. We coded three articles from the New York and US sections of the newspapers (two from the NYT and one from the WSJ) and two from the technology section. One of these was a short blog post about CCTV use rules and regulation in the United Kingdom, without any direct link to the situation in the US.[153] Besides the latter article, all other articles covered the CCTV topic as a domestic issue. This applied particularly to the most recent articles in both the NYT and the WSJ, which were written in response to the Boston Marathon bombings of 15 April, 2013.[154] In one article, the NYT also covered the use of CCTV cameras in the public transport system in relation to solving crimes and increasing passengers' safety.[155] The paper

[152]Feith, David. 2013. "Timothy Thomas: Why China Is Reading Your Email." *Wall Street Journal,* 29 March 2013. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424127887323419104578376042379430724.html.

[153]Clayton, Nick. 2012. "CCTV Technology has 'Overtaken Ability to Regulate it'." *Wall Street Journal*, 4 October 2012. Web. Accessed 19 August 2013. http://blogs.wsj.com/tech-europe/2012/10/04/cctv-technology-has-overtaken-ability-to-regulate-it/.

[154]Valentino-DeVries, Jennifer and Geoffrey A. Fowler. 2013. "Call for More Video Cameras Spotlights Debate on Use." *Wall Street Journal*, 19 April 2013. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424127887324763404578433143080413704.html, and
Landler, Mark and Dalia Sussman. 2013. "Poll Finds Strong Acceptance for Public Surveillance." *New York Times*, 30 April 2013. Web. Accessed 19 August 2013. http://www.nytimes.com/2013/05/01/us/poll-finds-strong-acceptance-for-public-surveillance.html?pagewanted=all.

[155]Rivera, Ray and Michael M. Grynbaum. 2010. "Lack of Video Slows Hunt for a Killer in the Subway." New York Times, 29 March 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/03/30/nyregion/30subway.html.

further discussed the use of CCTV cameras to monitor public spaces by the police and private companies,[156] with one commentator comparing the use of CCTV cameras to combat terrorism with the previous overzealous fights against other "–isms" throughout the history of the mankind.[157] Both the technology section articles were found in the WSJ. While one discussed the rules governing the use of CCTV camera systems,[158] the other was an investigative report into the booming private market in surveillance gear and software used by different governments and state security agencies.[159]

5. 3. 2. Content analysis: Actors and themes

The coverage of the use of CCTV cameras returned the smallest number of coded statements. The most frequently coded actors were journalists (29.7%), followed by citizens and passengers (11.9%), private companies (8.9%), experts (7.9%), transport companies (7.9%), and state institutions (7.9%). The prevalence of journalistic voice in the discussions may seem surprising at first. However, given that about 28%, or two out of seven articles, were found in the opinion section, the relatively high frequency of journalistic actors in the CCTV data set was to be expected. CCTV cameras were coded as actors in 5.9% of statements, as were advocacy groups and civil society. Other actors, e.g. police, municipalities and politicians, were each coded in 3% of cases. Lastly, 2% of statements were attributed to a government security agency. Under private companies, we coded a vendor of CCTV cameras and different companies producing and selling surveillance gear and software. The transport companies in CCTV coverage were the New York Metropolitan Transportation Authority (MTA) and the Massachusetts Bay Transportation Authority. The actors were predominantly of US origin (82%), with the second largest group of actors coming from the UK (12%). This suggests that the topic was largely framed as a domestic issue. We coded one case of confrontation between actors involving a legal dispute between the MTA and a private company installing CCTV cameras in the New York City subway system. The vendor sued the authority, 'claiming it could not complete the project because of problems with

[156]Kaminer, Ariel. 2010. "Has the Big Apple Become the Big Eyeball?" *New York Times*, 7 May 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/05/09/nyregion/09critic.html?_r=0.

[157]Murphy, Cullen. 2012. "The Certainty of Doubt." *New York Times*, 11 February 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/02/12/opinion/sunday/the-certainty-of-doubt.html?pagewanted=all.

[158]Clayton, Nick. 2012. "CCTV Technology has 'Overtaken Ability to Regulate it'." *Wall Street Journal*, 4 October 2012. Web. Accessed 19 August 2013. http://blogs.wsj.com/tech-europe/2012/10/04/cctv-technology-has-overtaken-ability-to-regulate-it/.

[159]Valentino-DeVries, Jennifer, Julia Angwin and Steve Stecklow. 2011. "Document Trove Exposes Surveillance Methods." *Wall Street Journal*, 19 November 2011. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html.

access and delays caused by transit officials.' The MTA counter-sued, arguing that the vendor 'had provided faulty technology.'[160]

Table 12: Actors coded in relation to CCTV and their origin

Actor	#	%	Actor's origin						Total
			USA	UK	Mentioned generally	France	Italy	National	
Journalist	30	29.7%	30						30
Citizen/Passenger	12	11.9%	12						12
Private company	9	8.9%	5	1	1	1	1		9
Experts	8	7.9%	8						8
Transport Company	8	7.9%	8						8
State institutions	8	7.9%	1	7					8
CCTV Cameras	6	5.9%	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Advocacy Group/Civil society	6	5.9%	4	1	1				6
Others	3	3.0%	1	1	1				3
Police	3	3.0%	3						3
Municipality	3	3.0%	2	1					3
Politicians	3	3.0%	3						3
Government security agency	2	2.0%	1					1	2
Total	**101**	**100.0%**	**78**	**11**	**3**	**1**	**1**	**1**	**95**

While public domain monitoring was the single most frequently coded theme of the discussions about CCTV cameras (21.4%), surveillance and it's increasing prevalence attracted the attention of the dailies in over a quarter of all statements. It is important to note that the code did not refer solely to CCTV cameras, but also to other surveillance systems. The purchase or installation of CCTV cameras featured as topic in almost 10% of the coverage, as did the issue of terrorism and government-led anti-terrorist campaigns. Private domain monitoring was discussed 8.4% of the time, and the features and characteristics of CCTV equipment in 6.1% of statements. While crime prevention, solution, or detection was discussed in 7.6% of cases, privacy was mentioned in relation to CCTV only in 3.1% of the coverage. Finally, the dailies also marginally touched on the issue of costs of CCTV camera systems. The most debated topics together were surveillance and private domain monitoring. These themes featured very prominently, particularly in an article that reported on the growing market for different surveillance tools, including software for intercepting mobile phone or Skype conversations. Other topics discussed together included surveillance and public domain monitoring, security-related rules and regulations with private domain monitoring, and the purchase or installation of CCTV cameras with public domain monitoring.

[160]Rivera, Ray and Michael M. Grynbaum. 2010. "Lack of Video Slows Hunt for a Killer in the Subway." New York Times, 29 March 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/03/30/nyregion/30subway.html.

Table 13: Topics coded in relation to CCTV

Topic	Frequency	%
Public domain monitoring	28	21.4%
Surveillance	20	15.3%
Surveillance Increase	15	11.5%
Purchase/Installation of CCTV cameras	13	9.9%
Private domain monitoring	11	8.4%
Cameras CCTV	8	6.1%
Security related rules and regulations	8	6.1%
Terrorism	7	5.3%
Crime solution	6	4.6%
Government-led antiterrorism campaign	6	4.6%
Privacy	4	3.1%
Crime Prevention	2	1.5%
Crime detection	2	1.5%
Costs	1	0.8%
Total	**131**	**100.0%**

5. 3. 3. Content analysis: Discussions about CCTV cameras

The majority of statements coded comprised of definitive argumentative strategies. More than a half of the coverage on CCTV thus provided value-free, factual information. We found over 38% of statements to be of an evaluative nature, with 10% of the coverage involving advocative declarations. The value-making statements were slightly more positive (57%) than negative (43%). It cannot be conclusively argued that the coverage in one paper was more negative than in the other. Both the opinion pieces were rather negative in their assessment of CCTV cameras. Both were published in the *Times*. The other two NYT articles provided both arguments for and against surveillance cameras, whereby the positive prevailed over the negative ones. One *Journal* article presented an equal number of positive statements about CCTV cameras; one was more negative, and a third one more positive in its coverage of surveillance cameras.

Table 14: Argumentative strategies direction of arguments about CCTV cameras

Argumentative strategy	#	%	Direction of argument					
			positive		negative		neutral	
			#	%	#	%	#	%
Definitive	**51**	**51.5%**	1	2.0%	1	2.0%	49	96.0%
Evaluative	**38**	**38.4%**	17	44.7%	15	39.5%	6	15.8%
Advocative	**10**	**10.1%**	7	70.0%	3	30.0%	0	0.0%
Total	**99**	**100.0%**	**25**		**19**		**55**	

Just over 45% of all statements in relation to CCTV cameras contained a justification. Efficiency was cited most often as a justification, both by the opponents and proponents of CCTV cameras (34.3%). The second most popular justification in discussions about CCTV camera systems, used predominantly by the advocates of surveillance cameras, was their ability to solve crime (20.9%), followed by national security (10.4%), safety (6%), security in general (3%), and crime prevention (3%). In contrast, critics of surveillance systems gave the right to privacy (10.4%) and freedom and liberty (3%) as justification for their opinions.

Table 15: Justifications in relation to CCTV

Justification	Frequency	%
Efficiency	23	34.3%
Crime solution	14	20.9%
National Security	7	10.4%
Right to Privacy	7	10.4%
Safety	4	6.0%
Transparency	3	4.5%
Legal issues/Litigation	2	3.0%
Security	2	3.0%
Freedom/Liberty	2	3.0%
Costs	2	3.0%
Crime Prevention	1	1.5%
Total	**67**	**100.0%**

Discussions about the benefits and risks of using CCTV camera systems in the US were reinvigorated particularly after the Boston Marathon bombings of April 2013. As reported by *The Wall Street Journal* a few days after the attacks, 'Video cameras played a critical role in helping authorities track suspects in this week's Boston bombings… now calls for increased camera surveillance in the U.S. are putting a spotlight on the technology and the debate about its use.'[161] The proponents of surveillance camera systems most frequently cited their efficiency and ability to solve crimes, often in connection to terrorism, as justifications for the need to install such systems. The WSJ cited US lawmakers arguing that 'use of a better-connected system of cameras controlled or monitored by law enforcement might have helped speed the suspects' identification.' New York Mayor Michael Bloomberg asserted that the Boston attack was 'a terrible reminder of why we've made these investments [sic] – including camera technology that could help us deter an attack, or investigate and apprehend those involved.' He added that the New York network could 'alert police to abnormalities it detects

[161]Valentino-DeVries, Jennifer and Geoffrey A. Fowler. 2013. "Call for More Video Cameras Spotlights Debate on Use." *Wall Street Journal*, 19 April 2013. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424127887324763404578433143080413704.html.

on the street, such as an abandoned package that is left on a corner.'[162]

Similar arguments advocating the increase in the number of CCTV cameras in the public transport system were voiced already in early 2010 shortly after the Moscow Domodedovo airport bombing and an incident in the New York subway that left a man dead. NYT reporters argued that CCTV cameras were an effective crime solution measure, 'The value of surveillance cameras in apprehending suspects was demonstrated… when the police quickly captured a man accused of savagely beating a woman in a Midtown bar, after putting out video of him from surveillance cameras outside the bar and in a nearby store.'[163] The New York police commissioner had also 'made no secret of his desire to see cameras in as many public places as possible, whether in the subways or on the streets.' The Chairman of the MTA's safety and security committee advocated further installation of CCTV cameras on public transport, arguing that they could have assisted in solving the recent killings and would help to increase the safety of passengers. 'This definitely should have been recorded on surveillance camera… Post-9/11, the terrorist bombings that just occurred in Moscow, the two murders that just occurred, plus other incidents that continue to occur in the subway system, we cannot wait any longer to ensure the safety of the public.' He was further reported saying that 'the lack of installed and operable cameras made the work of the police that much harder, especially as the authority greatly reduced station agent jobs to save money.'[164] Writing shortly after the failed bomb attack on Times Square of 1 May, 2010, an NYT commentator asserted that 'the bomb scare was a stark reminder of the risks New Yorkers take every day and of the crucial role that cameras can play in the first few hours after a crime.'[165]

As a result of the perceived omnipresent threat of terrorism, American citizens polled after the Boston attacks were also in favour of using CCTV cameras in the public space. Since they considered cameras to be an effective measure for efficiently solving crimes and/or increasing national security and their personal safety, they were willing to surrender some of their privacy. A *New York Times*/CBS News opinion poll conducted a week after the Boston Marathon attack found that 78% of the public thought that 'surveillance cameras were a good idea.'[166] 90% of the poll respondents thought that Americans would always have to live with

---

[162]Ibid.

[163]Rivera, Ray and Michael M. Grynbaum. 2010. "Lack of Video Slows Hunt for a Killer in the Subway." New York Times, 29 March 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/03/30/nyregion/30subway.html.

[164]Ibid.

[165]Kaminer, Ariel. 2010. "Has the Big Apple Become the Big Eyeball?" *New York Times*, 7 May 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/05/09/nyregion/09critic.html?_r=0.

[166]Landler, Mark and Dalia Sussman. 2013. "Poll Finds Strong Acceptance for Public Surveillance." *New York Times*, 30 April 2013. Web. Accessed 19 August 2013. http://www.nytimes.com/2013/05/01/us/poll-finds-strong-acceptance-for-public-surveillance.html?pagewanted=all.

the risk of terrorism. The public considered surveillance cameras as an effective measure to ensure safety in the face of the ever-present terrorist threat. 'I know some people are paranoid about the government intruding on their privacy,' a retired teacher said, 'but with all the horrible things that have been happening, I think you have to trust this as a way to protect our well-being.' Another citizen considered CCTV an effective means of solving crimes and finding terrorists, saying, 'Our families would be safer and surveillance cameras would provide evidence to help agencies pursue people, like they just did in Boston.'[167] The poll suggested that US citizens were willing to 'tolerate further tough measures to foil future attacks,' while merely 20% of respondents believed 'the government had gone too far in restricting civil liberties in the fight against terrorism.' Meanwhile, 26% thought it 'had not gone far enough' and 49% judged that 'the balance was about right.' In contrast, in 2011, the percentage of those worried about losing civil liberties (25%) was reported to be higher than that favouring more intrusive government approach (17%).[168]

However, the ability of CCTV cameras to solve crimes – the most frequently used justification by the advocates of surveillance cameras – did not remain unquestioned. Discussing the New York City subway system, NYT reporters stated that, 'More than eight years after the Sept. 11, 2001 attacks, the subway's video surveillance system, one of the key tools the city has in deterring and investigating attacks of any and all kinds in the subways, remains a patchwork of lifeless cameras, unequipped stations and problem-plagued wiring.' In 2010, almost half of the cameras that had been installed in the NYC subway network were not operable. More than 50% of them were held up by a lawsuit between the vendor and the MTA, while the rest were not equipped to function in the underground environment. Moreover, according to officials, crime in the New York transport system had been at a record low in 2010. With 5.3 crimes a day on average, as opposed to 47.8 in 1990, an MTA spokesman claimed that the subway system was safer that it had ever been.[169]

Those opposed to the introduction of further surveillance measures in the name of counter-terrorism, among them citizens and privacy advocates, were concerned about the government's encroachment on civil liberties. A citizen, for instance, claimed that 'in a country dealing with the threat of terrorism since the September 2001 attacks, the fight against it should not be a pretext for more pervasive forms of surveillance.' Saying that she did not 'have a problem with cameras as long as they are public,' she, however, considered 'wiretapping without a warrant' as going too far, particularly when 'the immediate 9/11 crisis

[167]Ibid.

[168]Ibid.

[169]Rivera, Ray and Michael M. Grynbaum. 2010. "Lack of Video Slows Hunt for a Killer in the Subway." *New York Times*, 29 March 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/03/30/nyregion/30subway.html.

was over.[170] Comparing the efforts to ensure national security to the Inquisition conducted by the Roman Catholic Church, a *New York Times* commentator warned against the moral certainty of the fight against terrorism, which could have horrific consequences for civil liberties of Americans. He argued that in the past decade, 'the inventory of measures advanced in the name of homeland security' such as 'the surveillance of citizens and non-citizens alike' had become 'increasingly pervasive.' Justified with reference to a greater good, arguments had even been made that torture could 'play a legitimate role in interrogation.' As a counterbalance to necessity and moral certainty, the author thus called for more doubt when assessing measures advocated in the name of national security, stating, 'A long philosophical tradition in the Roman Catholic Church itself … has long balanced the comfort of certainty against the corrective of doubt. Human beings are fallen creatures. Certitude can be a snare. Doubt can be a helping hand.'[171]

Pointing to the Boston attacks, some privacy advocates argued that 'the ability of investigators to track the suspects within a matter of days' demonstrated that 'more invasive surveillance' was not needed.[172] They were primarily concerned about the hi-tech, potentially invasive, surveillance technology, which had increasingly been employed by the US government. A privacy advocate claimed: 'it's one thing to have private closed-circuit cameras and look at feeds after the fact,' as was done by investigators of the Boston bombings. 'It's very different if you're talking about systems of cameras identifying and tracking people over time, all the time. Especially if you couple that with facial recognition and license-plate readers and databases. [sic]'[173] In this respect, the WSJ reported a considerable expansion of the use of surveillance technology by the government in the past decade.[174] According to an expert, through all the recent efforts, the US had overtaken London's reputation as 'the world's surveillance capital.' The expert found it problematic that, in contrast to the UK, American law did not 'provide clear limits on the use of such technology,' since most of it was used in areas that were considered public.[175] The WSJ reported a similar discussion about the need for rules governing the use of hi-tech surveillance technology that took place in the UK in 2012. The first surveillance commissioner

---

[170]Landler, Mark and Dalia Sussman. 2013. "Poll Finds Strong Acceptance for Public Surveillance." *New York Times*, 30 April 2013. Web. Accessed 19 August 2013. http://www.nytimes.com/2013/05/01/us/poll-finds-strong-acceptance-for-public-surveillance.html?pagewanted=all.

[171]Murphy, Cullen. 2012. "The Certainty of Doubt." *New York Times*, 11 February 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/02/12/opinion/sunday/the-certainty-of-doubt.html?pagewanted=all.

[172]Valentino-DeVries, Jennifer and Geoffrey A. Fowler. 2013. "Call for More Video Cameras Spotlights Debate on Use." *Wall Street Journal*, 19 April 2013. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424127887324763404578433143080413704.html.

[173]Ibid.

[174]Ibid.

[175]Ibid.

appointed by the UK government was quoted warning that such sophisticated camera systems were being introduced in the country, which could 'be in breach of human rights laws,' particularly of 'privacy due to face recognition functions.' A further concern of the commissioner was that cameras were often installed 'without consultation and without the public being aware of their capabilities.'[176]

Even in light of the failed 2010 Times Square attack, a NYT commentator found it hard to adjust to the loss of privacy as a result of public area monitoring in big cities. 'Cities – New York in particular, and Times Square most of all – used to be places to lose yourself in the thrilling anonymity of a crowd, to find yourself reflected in the eyes of strangers.' She found it 'hard to adjust to the idea that cities … are now places where unseen watchers can monitor your every move.'[177] The commentator acknowledged that these places were probably more intensely monitored by tourists taking pictures on their mobile phones. However, she admitted to being less concerned about this kind of surveillance, since she perceived it as being aimed at celebrities, as opposed to ordinary citizens. She said, 'That's surveillance far more intensive, and more granular, than anything Walgreens or Bank of America will ever manage. So why doesn't it feel as creepy? Maybe because its primary target is the Naked Cowboy.'[178] She found privacy intrusion an unacceptable trade-off for the possibility that CCTV cameras may help when investigating crimes, especially when they are costly and are ineffective as crime prevention measures. She states further, 'The city's new plan for increased video surveillance will cost millions, and however helpful it may be in solving crimes, there is no guarantee that it will prevent even one.'[179] According to a former secret service agent, neither the Orwellian fears of CCTV cameras' opponents omnipresent surveillance, nor the arguments of cameras' advocates about their usefulness by preventing crimes, were completely justified. The expert claimed that while some CCTV cameras were actively monitored, many were 'set up just to record, for review as needed.' Moreover, the cameras are often monitored by 'people who have been staring at the screen so long they have lost focus.' The concerns about the government centrally collecting footage from various cameras were also not accurate according to the agent. He argued that 'for the government to tap into multiple proprietary databases — it's not actually possible without a subpoena… even if you took away all the liability concerns and all the privacy concerns, the

[176]Clayton, Nick. 2012. "CCTV Technology has 'Overtaken Ability to Regulate it'." *Wall Street Journal*, 4 October 2012. Web. Accessed 19 August 2013. http://blogs.wsj.com/tech-europe/2012/10/04/cctv-technology-has-overtaken-ability-to-regulate-it/.

[177]Kaminer, Ariel. 2010. "Has the Big Apple Become the Big Eyeball?" *New York Times*, 7 May 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/05/09/nyregion/09critic.html?_r=0.

[178]Ibid.

[179]Ibid.

video's not in the same format.'[180]

However, that it may not be such an unthinkable scenario was revealed by an investigative report into 'a new global market for the off-the-shelf surveillance technology,' including hacking tools that allow governments to break into citizens' computers and mobile phones, and eavesdropping gear, able to collect all Internet communication in a country. In the decade since the 9/11 attacks, the market had grown from 'nearly zero' to about $5 billion a year according to the WSJ.[181] Critics argued that the market represented 'a new sort of arms trade supplying Western governments and repressive nations alike,' and advocated for more transparency about the activities of surveillance technologies' manufacturers. The producers and sellers, on the other hand, were divided in their views on the potential of abuse of the technology. Some stated that they would not sell to 'countries subject to international embargoes,' and that their products 'must be used for national-security purposes only and in accordance with ethical practices and applicable laws.' Others admitted that they 'were aware their products could be abused by authoritarian regimes,' but said they could not 'control their use after a sale.' One manufacturer said, 'This is the dilemma… It's like a knife. You can always cut vegetables but you can also kill your neighbour [sic].'[182]

5. 4. Influence of domestic and international factors

Domestic and international factors influenced the security risks discourse in relation to each topic. The influence was apparent in terms of the volume of articles dedicated to each individual issue, in the themes discussed, and their development over time. Since the US was a world leader in the number of body-scanners introduced, the 3D body scanner controversy touched the lives of ordinary American citizens to a large degree. By September 2010, nearly 200 'backscatter' scanners were operating at around 50 US airports, with 800 more to be installed, there was a real possibility that Americans would come into contact with the security-privacy dilemma posed by the machines. In the words of *The New York Times*, passengers were 'facing real-life decisions about what to do' at airports.[183] The high probability that an average American would come into contact with the machines could explain the high volume of coverage the controversy attracted. The trends in media coverage

[180]Ibid.

[181]Valentino-DeVries, Jennifer, Julia Angwin and Steve Stecklow. 2011. "Document Trove Exposes Surveillance Methods." *Wall Street Journal*, 19 November 2011. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html.

[182]Ibid.

[183]Stellin, Susan. 2010. "Are Scanners Worth the Risk?" *New York Times*, 7 September 2010. Web. Accessed 19 August 2013. http://www.nytimes.com/2010/09/12/travel/12prac.html.

can also be accounted for by domestic events. The peak in the articles about full-body scanners published in the NYT and WSJ was observed in 2010, the year after the failed bomb attack on the American jet flying from Amsterdam to Detroit. As a result of the failed plot, US airport security saw the 'most significant changes… since the terrorist attack of Sept. 11, 2001.'[184] The press coverage thus followed the plans and discussions about the proposed measures. Another peak in the number of articles about 3D body scanners was seen in 2012. This can also be explained by the domestic context. In 2012, the TSA started to introduce the 'Pre-check' and 'Global Traveler' programmes of tiered security screenings, the Congress also passed a law ordering the TSA to adjust the screening technology so that passengers' privacy is not compromised. At that time legislators also passed a law allowing airports to employ private screeners. The press followed these developments, providing readers with information and background about these changes.

The coverage of Stuxnet was also shaped by international and domestic developments. In 2010, both newspapers discussed the attacks on Iran and the potential damage it could have caused to the Iranian nuclear programme. They presented the opinions of experts about the efficiency of Stuxnet in relation to the damage it caused and speculated about the identity of its developers. In 2011, the papers gave space to other experts expressing their views about the new cyber weapon. They also discussed the counter-attack on the US security firm Comodo and the security problems it revealed, and reported on new malware detected by cyber security firms that shared some characteristics with Stuxnet. The coverage of Stuxnet was most intensive in 2012 in both the NYT and WSJ. This was a result of several interconnected developments. In June 2012, David Sanger published his seminal article describing operation Olympic Games and the development and deployment of Stuxnet by the NSA and the Israeli intelligence service. Based on Sanger's work, the WSJ published an article discussing those topics on the same day. 2012 also saw an increase in the number of cyber-attacks on US infrastructure and energy companies, as well as in Saudi Arabia and Qatar, which attracted the attention of both the papers. In the same year, Iran reported a second wave of attacks on its energy companies connected to Stuxnet. Finally, US authorities started more openly discussing the US involvement with cyber warfare. All these developments were mirrored in the press coverage of Stuxnet in 2012. The 2013 coverage also responded to the reports of Iran's renewed efforts to hasten its enrichment of uranium and to the talks about an international treaty to govern the use of cyber weapons.

The use of CCTV camera systems did not attract much attention from the US press. The fact that the US public transport system did not become a direct target of a successful,

[184]Schmidt. Michael S. and Nixon, Ron. 2012. "Airplane Security Debated Anew After Latest Bombing Plot." New York Times, 5 May 2012. Web. Accessed 19 August 2013. http://www.nytimes.com/2012/05/11/world/americas/airplane-security-debated-after-latest-bombing-plot.html.

destructive terrorist attack, such as those in Madrid in 2004 or London in 2005, can partially explain the low number of articles discussing the use of surveillance cameras. The few articles we found on this topic framed it largely as a domestic news item. Its coverage was thus mostly, albeit not exclusively, influenced by domestic events. Chronologically, the first article on CCTV cameras' use was published in response to an incident in the New York subway system and only a short while after the Moscow Domodedovo airport terrorist attacks. The following article was written just days after the failed Times Square bomb attack, which sparked calls from the New York Mayor for more CCTV cameras, as they were vital in tracking down the perpetrator. One of the articles reacted to moves to introduce official rules on the use of hi-tech surveillance technology in the UK. The last two reports responded to the Boston Marathon bombings of April 2013, where CCTV cameras played a crucial role in catching the alleged terrorists.

5. 5. Summary

The 3D body scanner controversy resonated with the US press the most of the three topics analysed in this report. Following the failed airplane attack in late 2009, the US authorities were intensely reconsidering airport security measures. The new air travel regulations included the screening by 'backscatter' full-body scanners, which could see through passengers' clothes, in an attempt to expose explosives. The machines became the subject of a controversy due to fears of possible health risks, as well as privacy and even efficiency concerns. The US introduced these scanners across the country, using them on a much larger scale than any other state. This directly influenced the lives of many US citizens, so the controversy was naturally of great interest to them and attracted much media coverage. The newspapers explained the rules governing the use of scanners and presented the views of the various parties to the controversy. The issue of body scanners was framed as a domestic news item and in a negative light. The message implied by the articles was that the security risks related to a potential terrorist threat in air travel do not justify the intrusion of passengers' privacy, the unpleasant experience of the screening, and/or a potential risk of developing cancer. At times, the coverage also questioned the ability of the scanners to detect a novel terrorist threat and proposed alternative security measures instead. In the end, US lawmakers and citizens valued passenger privacy and comfort over security and rejected backscatter scanners as excessive, forcing the TSA to withdraw them. As one commentator argued, 'sometimes, customer experience has to be integrated into a technology for it to succeed. Otherwise, the numbers just don't add up.'[185]

[185]Crease, Robert P. 2010. "Invasion of the Full-Body Scanners." *Wall Street Journal*, 21 May 2010. Web. Accessed 19 August 2013. http://online.wsj.com/article/SB10001424052748704608104575220542781522702.html.

The US media showed the second largest interest in the Stuxnet topic. This is understandable as the virus did not target private computers and thus did not directly affect ordinary Americans. On the other hand, given the virus's connection to the rising number of cyber-attacks on US infrastructure and the increasing intensity of state-led cyber warfare, the Stuxnet attack could have had enormous consequences for the public. For that reason, it was desirable for US citizens to be informed about the issue. The coverage varied between descriptive, factual accounts of Stuxnet's development, the attacks, counter-attacks, and assessments of the US and Israeli efforts. Two aspects of the coverage are worth noting for their potential impact on public perceptions. Firstly, Iran's nuclear programme was often mentioned in relation to the Stuxnet attacks – explicitly as a target, and implicitly as a threat that the virus was supposed to eliminate. Based on the coverage, the public might have perceived Iran's uranium enrichment as a real threat, and would thus have positively evaluated USA's cyber strategy. On the other hand, due to the potential risks linked to the virus's proliferation and counter-attacks triggered by its deployment, the coverage was rather negative towards the use of Stuxnet. Based on the discussions in US newspapers, we would expect the public to become apprehensive of the government's use of new, advanced technologies to combat the threat of Iran's nuclear programme or other possible targets, especially in an unregulated environment.

Interestingly, the use of CCTV camera systems in public transport and in general was a virtual non-issue for the US newspapers. We observed increased salience of the topic only after major successful and unsuccessful terrorist attacks. Despite the omnipresence of surveillance cameras on or inside shops, official buildings, in the public transport network and in public spaces in general, the newspapers paid very little attention to their use. Public discussions about the benefits of surveillance only really started after the tragic Boston Marathon bombing of April 2013, when CCTV footage proved crucial in tracking down the suspects. From the coverage, it would seem that the public was either oblivious or in favour of using surveillance cameras because they viewed cameras as vital in the efforts to solve crimes and increase security. On the other hand, the newspapers also presented views critical of the lawmakers' intentions to use more invasive surveillance systems and measures. Yet, given the lack of coverage of the issue and the overall positive tone, we would expect that the public remained largely unaware of and uninterested in the ever more pervasive use of CCTV cameras and other surveillance methods by the authorities.

6. Conclusion

This report has explored the role media plays in influencing citizens' perceptions of security risks and the related trade-offs. The core of the report focused on qualitative analysis of press coverage of three security-related topics – 3D body scanners, Stuxnet, and CCTV camera systems – in two internationally acclaimed US newspapers between January 2010 and 30 April 2013. The analysis revealed that the coverage was considerably influenced by various domestic and national developments. While we did not observe any clear-cut differences in the portrayal of the issues between topics or between newspapers, we uncovered some subtler, but no less interesting, trends in terms of the volume of coverage dedicated to topics and discourses employed by the newspapers.

The volume and framing of security-related issues in terms of argumentative strategies involved differed depending on the relevance of the topics to readers' everyday lives. In general, the extent of coverage dedicated to phenomena more likely to be experienced by readers when going about their day-to-day business exceeded the coverage of issues that touched people's lives in less apparent ways. The intriguing exception to this rule was the coverage of CCTV cameras, as discussed above. Whereas definitive argumentative strategies providing factual information about events and phenomena prevailed in the coverage, the topics with more relevance to readers attracted many more evaluative views than factual statements. In general, articles located in the domestic, business, and technology sections also put forward fewer evaluations, particularly from journalists, than commentaries and editorials. In this sense, it could be argued that the leading US newspapers adhered to the journalistic values of objectivity and neutrality. These values were also evident in the fact that the papers put forward the views of proponents as well as opponents of the various security measures discussed. Justifications for statements were present particularly in the more evaluative discussions of full-body scanners and CCTV cameras. While this is to be expected, as factual statements do not often need explicit justification, on the whole, the arguments in the leading US newspapers were comparatively well supported by evidence or expert opinion.

The analysis also revealed that even if the articles were not solely found in the domestic news sections, they predominantly provided the views of US actors. On the one hand, this trend is understandable for two reasons in particular. First, the key developments in our three security-related topics occurred in the United States. The failed Christmas Day bomb plot, which led to the introduction of backscatter full-body scanners, happened on board of an airplane heading for Detroit. The US was also allegedly behind the Stuxnet attacks, which were linked to the increased number of cyber-attacks on critical US infrastructure and businesses. At the same time *The New York Times* and *The Wall Street*

Journal were the first to reveal the US involvement in the operation Olympic Games, and the growth of the secret surveillance equipment market, respectively. The second reason concerns the falling revenues of the newspaper industry. As part of cost-cutting measures, many news organisations had to severely reduce or entirely close their foreign desks and increasingly rely on foreign news agencies. On the other hand, to form an informed opinion on security-related technologies and threats in broader context, US readers would have benefited from views and experiences of foreign countries and actors. This is not to say that actors coming from outside the US were not given voice in the coverage. The argument here is that the discussions of airport security measures, for instance, could have been enriched with the experiences and practices of other countries that operate international hub airports and how they deal with the security vs. privacy dilemma. Similarly, whereas some articles briefly alluded to London as the surveillance capital of the world, a broader discussion about the rules governing real-time public surveillance or the use of face-recognition software in different countries was missing. Doing so would have helped readers to better assess the different government security policies and their implications for their safety and civil liberties.

The newspapers generally highlighted the same information about individual topics and there was no straightforward difference in the way in which the papers evaluated certain security measures. In general, in both papers the coverage of all three topics involved considerable discussions about security threats – terrorist attacks in civil aviation, public transport, or in general, but also the threat of Iranian nuclear programme. Even the scarce coverage of CCTV cameras increased after each terrorist incident that occurred between 2010 and 2013. This can be explained by the commercial nature of the media. Naturally, in the wake of terrorist attacks, people are more concerned with security threats posed by terrorists and thus more interested in the related issues. By further whipping up anxiety over terrorist strikes, newspapers are likely to attract more readers.[186] However, the portrayal of security measures and technologies by the US press in a positive or negative light would seem to have been influenced by three main factors – the extent to which the various security measures encroached on civil liberties, the availability of alternative measures, and whether they posed a risk of counter-attack or misuse by US adversaries. Press coverage of the use of CCTV cameras in public places to help track perpetrators was mostly positive. This can be accounted for by the attitudes in the US, which, based on legal precedent and technological developments, considered surveillance in the public space as justified and acceptable. In the age of social media, when around 30 million surveillance cameras were installed in the public spaces across the US, people were no longer disturbed about having their picture taken in

186"Why We Spy. The War on Terror is Obama's Vietnam." 2013. *The Economist (Online),* 10 June 2013. Web. Accessed 20 October 2013. http://www.economist.com/blogs/democracyinamerica/2013/06/why-we-spy.

public. Yet, the use of surveillance equipment to intercept private Internet communication, for face-recognition, for real-time surveillance and the creation of searchable image databases, as well as for wiretapping without warrants and the like were considered as unjustifiable intrusions into the private sphere and constitutional rights. These measures were thus portrayed in a negative light. Likewise, the use of backscatter full-body scanners was portrayed as endangering passengers' privacy and health. Given that alternative security measures were readily available, the newspapers viewed the scanners as needlessly risky and intrusive. Lastly, the coverage of Stuxnet, which highlighted the fact that security measures could trigger counterattacks or be acquired by the country's enemies to launch a counterattack, tended to be portrayed negatively by the US press.

We found some interesting differences in interpretations and space dedicated to some aspects of the issues related to the political-leaning of the dailies. Commentators and experts whose opinion was presented in *The Wall Street Journal* were for various reasons against backscatter body scanners and instead advocated alternative security measures, such as tiered security checks and the profiling of travelers. *The New York Times* also portrayed the scanners as an unnecessary infringement of civil rights, which posed health risks and inconvenienced passengers. In contrast to the *Journal*, however, it also mentions one aspect important for the citizens to form their own opinion on the issues, namely the partisan divide in public discussions of scanning at airports. The NYT drew readers' attention to the fact that Republican politicians and supporters who typically favoured tougher security measures over civil liberties were at the forefront of the opposition to body scanners, waving the flag of civil liberties. In contrast, Democrats, generally seen valuing civil liberties over national security, were fervently justifying the use of scanners. The *Times* editorial also condemned the calls of Republican politicians advocating profiling at airports as ineffective and purely ideological.

Although Stuxnet coverage was dominated by informative statements and we cannot clearly say that one newspaper valued its deployment more positively than the other, the political leaning of the papers was perhaps even more visible in the discussions of this topic. The *Times* commentators and reporters warned against the negative consequences of the deployment of Stuxnet for American critical infrastructure and private businesses. They were concerned about the counter-attacks and proliferation of the virus. They also advocated more openness about America's cyber-warfare initiatives and an international treaty on the deployment of cyber-weapons. The *Journal* framed the risk-benefits analysis of Stuxnet and cyber-weapons in a rather different light. The negative view of Stuxnet presented in the *Journal* was based on the evaluations of Stuxnet's limits in stopping Iran's nuclear efforts. The author was of the opinion that wars were never worn merely by covert means, such as Stuxnet. In stark contrast to the *Times*, the *Journal* published an interview with a military

expert on China who dismissed the calls for an international treaty on the use of cyber-weapons, and instead advocated further and more ruthless cyber-attacks on China.

In conclusion, we could argue that by presenting the differing views on the security versus privacy dilemma related to 3D body scanners, Stuxnet, and CCTV cameras the US newspapers fulfilled their democratic role to inform citizens about issues of public interest. Despite the various shortcomings of the coverage discussed above, the readers of these publications were in a relatively good position to form their own opinion on where to draw the line between security and civil liberties in relation to the three studied issues.

7. References

Academic literature:

Brown, Katherine Ann, and Todd Gitlin. 2011. "Partisans, Watchdogs, and Entertainers: The Press for Democracy and Its Limits." In *The Oxford Handbook of American Public Opinion and the Media*, edited by George C. Edwards, Lawrence R. Jacobs, and Robert Y. Shapiro. Oxford: Oxford University Press. Available from: http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199545636.001.0001/oxfordhb-9780199545636.

Graber, Doris A., and Gregory G. Holyk. 2011. "The News Industry." In *The Oxford Handbook of American Public Opinion and the Media*, edited by George C. Edwards, Lawrence R. Jacobs, and Robert Y. Shapiro. Oxford: Oxford University Press. Available from: http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199545636.001.0001/oxfordhb-9780199545636.

Groeling, Tim. "Who's the Fairest of Them All? An Empirical Test for Partisan Bias on ABC, CBS, NBC, and Fox News." *Presidential Studies Quarterly* 38 (4): 631–657.

Groseclose, Tim, and Jeffrey Milyo. 2005. "A Measure of Media Bias." *The Quarterly Journal of Economics* CXX (4): 1191–1237.

Ha, Jeasik. 2012. "'Health Care Reform' Vs. 'ObamaCare': Partisan Framing of FOX, MSNBC, NYT, and WSJ." *Gnovis* XIII (I). [online]. Available from: http://gnovisjournal.org/2012/11/30/health-care-reform-vs-obamacare-partisan-framing-of-fox-msnbc-nyt-and-wsj/. Accessed 5 September 2013.

Hallin, Daniel C., and Paolo Mancini. 2004. *Comparing Media Systems: Three Models of Media and Politics*. Cambridge: Cambridge University Press.

Iyengar, Shanto, and Kyu S Hahn. 2009. "Red Media, Blue Media: Evidence of Ideological Selectivity in Media Use." *Journal of Communication* 59 (1): 19–39. doi:10.1111/j.1460-2466.2008.01402.x.

Jamieson, Kathleen Hall, and Joseph N. Cappella. 2008. *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*. Oxford University Press.

Patterson, Thomas A. 2000. "The United States: News in a Free-Market Society." In *Democracy and the Media: A Comparative Perspective*, edited by Richard Gunther and Anthony Mughan, 241–265. Cambridge: Cambridge University Press.

Internet sources:

Ahlers, Mike M. 2013. "TSA removes body scanners criticized as too revealing." *CNN.com*, 30 May 2013. [online]. Available from: http://edition.cnn.com/2013/05/29/travel/tsa-backscatter. Accessed 20 October 2013.

Allen, Nick. 2009. "Barack Obama admits 'unacceptable systemic failure' in Detroit plane attack." Telegraph, 29 December 2009. [online]. Available from: http://www.telegraph.co.uk/news/worldnews/barackobama/6908709/Barack-Obama-admits-unacceptable-systemic-failure-in-Detroit-plane-attack.html. Accessed 10 September 2013.

Atlas, Terry and Greg Stohr. 2013. "Surveillance Cameras Sought by Cities After Boston Bombs." *Bloomberg.com*, 29 April 2013. [online]. Available from:

http://www.bloomberg.com/news/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html. Accessed 20 October 2013.

Ball, James, Julian Borger and Glenn Greenwald. 2013. "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security." *Guardian,* 5 September 2013. [online]. Available from: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. Accessed 13 September 2013.

Bennett, Drake. 2013. "Using Facial-Recognition Technology to Track Down the Boston Bombers (and Why Humans Are Still Better at It)." Businessweek.com, 19 April 2013. [online]. Available from: http://www.businessweek.com/articles/2013-04-19/did-the-fbi-use-facial-recognition-software-to-find-the-boston-bombers. Accessed 20 October 2013.

"Bezos buys the Post: The newspaper industry." 2013. The Economist (Online), 6 August 2013. *Proqest*. [online]. Accessed 18 October 2013.

Crovitz, L. Gordon. 2007. "A Report to Our Readers." *The Wall Street Journal*, 1 August 2007. [online]. Available from: http://online.wsj.com/article/SB118592510130784008.html. Accessed 10 September 2013.

"Cyber-security. Difference Engine: Swamped with data." 2012. *The Economist (Online),* 11 May 2012. [online]. Available from: http://www.economist.com/blogs/babbage/2012/05/cyber-security. Accessed 20 October 2013.

Dailey, Kate. 2013. "The rise of CCTV surveillance in the US." *BBC.co.uk*, 29 April 2013. [online]. Available from: http://www.bbc.co.uk/news/magazine-22274770. Accessed 20 October 2013.

Encyclopaedia Britannica. 2013. "USA Today." [online]. Available from: http://www.britannica.com/EBchecked/topic/683077/USA-Today. Accessed 9 September 2013.

Encyclopaedia Britannica 2013. "The New York Times." [online]. Available from: https://www.britannica.com/EBchecked/topic/412546/The-New-York-Times. Accessed 28 August.

Encyclopaedia Britannica. 2013. "The Wall Street Journal." [online]. Available from: https://www.britannica.com/EBchecked/topic/634727/The-Wall-Street-Journal. Accessed 28 August.

Erwin, Sandra I., Stew Magnuson, Dan Parsons and Yasmin Tadjdeh. 2012. " Top Five Threats to National Security in the Coming Decade." National Defense, November 2012. [online]. Available from: http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx. Accessed 10 September 2013.

Federal Bureau of Investigation. "Crime Rate in the United States." [online]. Available from: http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl01.xls. Accessed 24 October 2013.

Freedom House. 2013. "Freedom of the Press 2013 – United States." [online]. Available from: http://www.freedomhouse.org/report/freedom-press/2013/united-states. Accessed 20 August 2013.

Freedom House. 2010. "Freedom of the Press 2010 – United States." [online]. Available from: http://www.freedomhouse.org/report/freedom-press/2010/united-states. Accessed 20 August 2013.

Gabbatt, Adam. 2010. "Faisal Shahzad pleads guilty to attempting to bomb Times Square." Guardian, 22 June 2010. [online]. Available from: http://www.theguardian.com/world/2010/jun/22/faisal-shahzad-pleads-guilty-new-york-times-square-bomb. Accessed 10 September 2013.

Gabbatt, Adam and Dan Roberts. 2013. "Boston suspects planned attack on New York City, Mayor Bloomberg says." Guardian, 25 April 2013. [online]. Available from: http://www.theguardian.com/world/2013/apr/25/boston-bomb-suspects-new-york-city-attack. Accessed 10 September 2013.

Gladstone, Rick. 2012. "Iran Suggests Attacks on Computer Systems Came From the U.S. and Israel." *New York Times*, 25 December 2012. [online]. Available from: http://www.nytimes.com/2012/12/26/world/middleeast/iran-says-hackers-targeted-power-plant-and-culture-ministry.html. Accessed 10 September 2013.

Grynbaum, Michael M., William K. Rashbaum and Al Baker. 2010. "Police Seek Man Taped Near Times Sq. Bomb Scene." *New York Times*, 2 May 2010. [online]. Available from: http://web.archive.org/web/20100505083749/http://www.nytimes.com/2010/05/03/nyregion/03timessquare.html?hp. Accessed 20 October 2013.

"How much surveillance do you need?" 2010. *The Economist (Online*), 3 April 2010. [online]. Available from: http://www.economist.com/blogs/gulliver/2010/04/security_cameras. Accessed 10 October 2013.

"I Spy, With My Big Eye. Video Surveillance." 2012. *The Economist,* 28 April 2012. *ProQuest.* [online]. Available from: http://search.proquest.com/docview/1010371320?accountid=9630. Accessed 24 October 2013.

Kelly, Heather. 2013. "After Boston: The Pros and Cons of Surveillance Cameras." *CNN.com*, 26 April 2013. [online]. Available from: http://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/. Accessed 20 October 2013.

Launder, William Christopher S. Stewart and Joann S. Lublin. 2013. "Bezos Buys Washington Post for $250 Million." Wall Street Journal, 5 August 2013. [online]. Available from: http://online.wsj.com/news/articles/SB10001424127887324653004578650390383666794. Accessed 10 October.

"Lexington: Keeping the mighty honest." 2013. *The Economist*, 10 August 2013. [online]. Available from: http://www.economist.com/news/united-states/21583274-new-wave-press-barons-should-not-allow-newspapers-become-niche-products-keeping?zid=293&ah=e50f636873b42369614615ba3c16df4a. Accessed 18 October 2013.

Linn, Allison. 2011. "Post 9/11, Surveillance Cameras Everywhere." *NBCNews.com*, 23 August 2011. [online]. Available from: http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere/#.Um5vCiRshQL. Accessed 5 October 2013.

Pew Research Centre for Excellence in Journalism. 2009. The State of the News Media 2009. [online]. Available from: http://www.stateofthemedia.org/files/2011/01/COMPLETE-EXEC-SUMMARY-PDF.pdf. Accessed 20 August 2013.

Rainey, James and Jessica Garrison. 2012. "Pulitzer winners span old, new media." Los Angeles Times, 17 April 2012. [online]. Available from: http://articles.latimes.com/2012/apr/17/nation/la-na-pulitzers-20120417. Accessed 9 September 2013.

Schmidt. Michael S. and Nixon, Ron. 2012. "Airplane Security Debated Anew After Latest Bombing Plot." New York Times, 5 May 2012. [online]. Available from: http://www.nytimes.com/2012/05/11/world/americas/airplane-security-debated-after-latest-bombing-plot.html. Accessed 19 August 2013.

Selyukh, Alina and Deborah Charles. 2013. "CISPA Cybersecurity Bill Backers Hope Second Time's a Charm." *NBCNews.com*, 16 May 2013. [online]. Available from: http://www.nbcnews.com/technology/cispa-cybersecurity-bill-backers-hope-second-times-charm-1C9948195. Accessed 20 October 2013.

The New York Times Company. 2013. "Pulitzer Prizes." [online]. Available from: http://www.nytco.com/company/awards/pulitzer_prizes.html. Accessed 9 September 2013.

"The Boston Bombings. The Manhunt is Over." 2013. *The Economist (Online),* 19 April 2013. *Factiva*. [online]. Available from: Accessed 10 October 2013.

"Times Square bomb attempt man jailed for life." 2010. Guardian, 5 October 2010. [online]. Available from: http://www.theguardian.com/world/2010/oct/05/times-square-bomb-attempt-man-jailed. Accessed 10 September 2013.

Warrick, Joby, Peter Finn and Ellen Nakashima. 2010. "Times Square Bombing Attempt Reveals Limits of Video Surveillance." *Washington Post*, 4 May 2010. [online]. Available from: http://www.washingtonpost.com/wp-dyn/content/article/2010/05/03/AR2010050304522.html. Accessed 20 October 2013.

"Where Have All the Burglars Gone? Falling Crime." 2013. *The Economist*, 20 July 2013. *ProQuest*. [online]. Available from: http://search.proquest.com/docview/1411815450?accountid=9630. Accessed 24 October 2013.

"Why We Spy. The War on Terror is Obama's Vietnam." 2013. *The Economist (Online),* 10 June 2013. [online]. Available from: http://www.economist.com/blogs/democracyinamerica/2013/06/why-we-spy. Accessed 20 October 2013.

8. Appendix: Analysed articles by topic

3D body scanner

Newspaper	Date	Title of article
New York Times	09/01/2010	Cancer Risks Debated for Type of X-Ray Scan
Wall Street Journal	09/01/2010	TSA Pressed on Full-Body Scans Despite Concerns
New York Times	13/01/2010	Mixed Signals on Airport Scanners
Wall Street Journal	18/01/2010	The Body Scanner Scam
Wall Street Journal	21/05/2010	Invasion of the Full-Body Scanners
Wall Street Journal	09/06/2010	Airport Screeners Reveal Travelers' Surly Side
New York Times	26/07/2010	Radiation Questions Over a Body Scanner
New York Times	07/09/2010	Are Scanners Worth the Risk?
Wall Street Journal	17/11/2010	Has Airport Security Gone Too Far?
New York Times	21/11/2010	Administration to Seek Balance in Airport Screening
New York Times	23/11/2010	Politicizing Airport Security
New York Times	28/11/2010	The Partisan Mind
Wall Street Journal	15/01/2011	Court Rejects Challenge to Airport Body Scanners
New York Times	07/02/2011	Support Grows for Tiered Risk System at Airports
New York Times	26/09/2011	Paying for Security
New York Times	30/01/2012	Gatekeepers Under Scrutiny
New York Times	15/03/2012	New Law Clears the Way for Airports to Drop T.S.A. Screeners
Wall Street Journal	19/03/2012	$100 to Fly Through the Airport
New York Times	17/12/2012	A Quest for Speedier and Smarter Airport Security
Wall Street Journal	18/01/2013	TSA to Halt Revealing Body Scans at Airports
New York Times	15/04/2013	Trying Passenger Patience

Stuxnet

Newspaper	Date	Title of article
New York Times	26/09/2010	A Silent Attack, but Not a Subtle One
New York Times	19/11/2010	Worm Can Deal Double Blow to Nuclear Program

Wall Street Journal	24/11/2010	Iran Nuclear Sites Temporarily Suspended
Wall Street Journal	18/01/2011	The Limits of Stuxnet
New York Times	07/04/2011	An Attack Sheds Light on Internet Security Holes
Wall Street Journal	24/10/2011	'Son of Stuxnet' Virus Targets Specific Organizations, Assets
New York Times	01/06/2012	Obama Order Sped Up Wave of Cyberattacks Against Iran
Wall Street Journal	01/06/2012	U.S. Team and Israel Developed Iran Worm
New York Times	24/06/2012	A Weapon We Can't Control
New York Times	26/07/2012	Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure
New York Times	26/09/2012	Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials
Wall Street Journal	09/11/2012	Virus Aimed at Iran Infected Chevron Network
New York Times	25/12/2012	Iran Suggests Attacks on Computer Systems Came From the U.S. and Israel
New York Times	31/01/2013	Iran Said to Be Set to Hasten Uranium Enrichment
Wall Street Journal	29/03/2013	Timothy Thomas: Why China Is Reading Your Email

CCTV

Newspaper	**Date**	**Title of article**
New York Times	29/03/2010	Lack of Video Slows Hunt for a Killer in the Subway
New York Times	07/05/2010	Has the Big Apple Become the Big Eyeball?
Wall Street Journal	19/11/2011	Document Trove Exposes Surveillance Methods
New York Times	11/02/2012	The Certainty of Doubt
Wall Street Journal	04/10/2012	CCTV Technology has 'Overtaken Ability to Regulate it'
Wall Street Journal	19/04/2013	Call for More Video Cameras Spotlights Debate on Use
New York Times	30/04/2013	Poll Finds Strong Acceptance for Public Surveillance