universität wien

MASTERARBEIT

Titel der Masterarbeit

Casual Biometrics:
Sociological Expectations and Changing Discourses

Verfasser

Jack Kerr

angestrebter akademischer Grad

Master of Arts (MA)

Wien, 2015

Studienkennzahl lt. Studienblatt: A 066 906

Studienrichtung lt. Studienblatt: Master Science-Technology-Society

Betreuer: Philippe Björn Sormani, PhD

Dedicated to:

Österreiech;

for touching my cultural ID, forever changing my social discourse, and enriching life's expectations

immer wieder...

Abstract

Keywords: *media, expectations, discourse, biometric(s), fingerprint, identification, verification, Touch ID, security, privacy*

In an era filled with constant technological innovation, and a world of hype and expectations, the media plays a strong role in framing how future technologies are depicted to the public. The invention of the modern smartphone alongside 'mobile internet' and big data revolutions has changed the way society functions, in terms of communications, connectedness, as well as providing a platform for many industries to blossom. Is biometrics one of them? Coming from a strong criminality discourse of forensics and government databases, this thesis questions whether the modern day smartphone can be a vector to transform the biometric discourse away from its sociohistorical past, to a more casual, day-to-day discourse. By analyzing the differences in identification and verification this thesis asks whether Apple's Touch ID has paved the path for biometrics to replace the password as an authentication system, and questions the privacy and security issues of whether both identification and verification discourses can co-exist. By looking closely at US and UK media articles based on the release of Apple's iPhone 5S's Touch ID and its subsequent 'hacking', this thesis shows how the media has framed the expectation of both the emergence and the quality of this verification system and its socio-technical issues. Through close empirical research and analysis of an array of articles and user comments, as well as video analysis of the actual hack 'in situ', this study will provide a better understanding of how sociological expectations are framed through the media. Ultimately, it proves that the changing discourses are crucial for the future of casual biometrics.

Zusammenfassung

Schlüsselwörter: *Medien, Erwartungen, Diskurs, biometrische(n), Fingerabdruck, Identifizierung, verifizierung, Touch ID, Sicherheit, Privatsphäre*

In einer Zeit konstanter technologischer Innovation, des Hypes, sowie großer Erwartungen spielen Medien in der Rahmung und Präsentation zukünftiger Technologien gegenüber der Öffentlichkeit eine Schlüsselrolle. Die Erfindung moderner Smartphones, des mobilen Internets und die „Big Data Revolution" hat das Zusammenspiel der Gesellschaft grundlegend verändert: Darin, wie wir kommunizieren und wie wir miteinander in Verbindung stehen, aber auch in Form eines neues Geschäftsfeld in dem zahlreiche neue Industrien florieren. Ist Biometrie einer dieser aufstrebenden Industriesektoren? Ausgehend von der Forensik (etwa auch im Zusammenhang von staatlichen Datenbanken), wird der Diskurs zu Biometrik stark kriminologisch geführt. Hier wird die Frage aufgeworfen, inwiefern das moderne Smartphone dem Biometrik-Diskurs eine neue Richtung geben könnte: Weg von seiner sozio-historischen Vergangenheit und hin einer weitaus größeren Alltäglichkeit und Zwanglosigkeit. Diese Thesis wirft mittels der Analyse von Unterschieden in der Methode der Verifikation und Identifikation die Frage auf, inwieweit Apples „Touch ID" der Biometrik den Weg geebnet hat, das Passwort als Authentifikationsmittel zu ersetzen. Darüber hinaus soll dem Spannungsfeld von Privatheit und Sicherheit nachgegangen und überprüft werden, ob Identifikations- und Verifikationsdiskurse beider technologischer Mittel koexistieren können. Es wird ein tiefgreifender, analytischer Blick auf die US und britische Medienberichterstattung geworfen: Jene, unmittelbar nach Veröffentlichung von Apples iPhone 5S, sowie jene nach dem „Hack" der Touch ID. Mittels einer solchen Analyse wird die vorliegende Arbeit aufzeigen, wie Medien die Erwartungshaltungen hinsichtlich Aufkommen und Qualität dieses Verifikationssystems zu prägen vermögen. Eine tiefgreifende empirische Analyse einer Vielzahl ausgewählter Artikel und User-Kommentare, sowie die Video-Analyse des eigentlich „Hacks" in situ erschließt ein besseres Verständnis sozio-technologischer Erwartungen und deren Rahmung durch Medien. Dabei wird aufgezeigt, dass sich verändernde Diskurse der Schlüssel zu einer zwangloseren Zukunft von Biometrie sind.

Table of Contents

Acknowledgements

In travel, I like to think the journey is the destination. For months you plan, the expectations are high as you save up for that magical getaway. Then, when it's over, a sense of emptiness seeps out, as you realize how quick it all went, and you long for that next adventure. For those that have had the pleasure of submitting a Master Thesis, I daresay many would agree, it is conversely, all about the destination. Days, hours, even mere paragraphs and words before that final full stop and ctrl P is entered, the gut aches as that unfulfilling feeling of incompleteness drags on. It is not until those words finally turn from flashing pixels on your screen to permanent, tangible, ink, that it all seems real. The destination becomes the culmination of a hard-earned, years-long effort from a rough idea, to a finished Master Thesis. In this, you are overcome by the knowledge, that you fulfilled what is to this point, most likely the most important thing you have ever written. It is at least the longest!

However, that is not to say that I did not enjoy the journey. There were many moments along the way of pure joy, be it finding the perfect article that opened my eyes to new possibilities of research, or simply sharing the moment with friends, family and colleagues, and receiving the joy that others found interest in my ideas. For a thesis may be an individual effort, in that my biometric fingertips alone slaved night and day, muscles tearing, to write all 44,975 words, but without the help and support of many, not only would this have not been possible, but it would not be worth doing. Why else would I write, if I didn't want somebody to read?

In that, I would first like to thank all of the strangers along the way that I have met on some of my travels whilst writing this thesis, who, upon listening to me explain the topic, insisted on reading it as soon as it was done, and provided one of many seeds of motivation that proved necessary to continue my lengthy journey. If I still have your contact details, I will gladly send you the finished copy.

I would also like to thank all of my friends and family in Australia for supporting me during my journey, not just in this thesis, but also in moving to Austria, a commitment which on many levels, particularly Austrian bureaucracy, was no easy task. Thank you for the support in helping me do something I would never have dreamed of in the past; completing my masters in a foreign country.

Special mention has to go to my family in Australia; especially my mum, dad and brother for being always supportive of my actions, especially allowing me to move to Austria. I know you always believed in me that I would finish this thesis, and I thank you for your love, support and motivation, especially our bi-weekly Skype sessions comprised of telling me the going-ons of life in Sydney, as

well as of course to ask me about my thesis; again, and again, and again. I say this not begrudgingly; this motivation was definitely necessary and I thank you for it!

I also have to thank my Austrian family who became my second family over here by taking me in and helping me adjust to life in Vienna. Without you, I would not have even been here to complete this Master's Degree, and gain experiences I never would have dreamed of. So to Simone, Angie and Thomas; *Vielen Dank!*

Of course this thesis would also not have been possible without the teaching staff at the STS department. To Ulrike, Max and my supervisor Phil, as well as the many other teachers I had throughout this Master's Degree, thank you for some very thought enriching classes, which has definitely changed my viewing of the world. I don't think I will ever be able to look at a door-hinge the same again.

I must also thank all my colleagues from the STS department that have gone through a similar journey with me, and helped in giving ideas and feedback to improve this thesis. Special mention has to go to my main thesis support group of Noel, Saransh and Leo for our weekly catch ups for beers and inevitable discussions of what we called the dreaded T-word. It was a pleasure studying with you guys. I thank you for your support and best of luck in finishing your thesis and future studies.

Lastly, having finished this thesis in the Tyrolean Alps, I have to give thanks to the St Anton weather, for being miserable at the time I needed you most, forcing me to stay inside and finish the last few pages of my thesis, instead of snowboarding in knee-deep powder. A quick mention also to *mamma* and the rest of the crew from Hotel Sonnbichl for taking me in, and giving me extra motivation to finish this thesis through providing gourmet meals, and daily reminders such as, "schreiben fertig? Warum Nicht? Wann fertig?" Thanks guys! You were the last step of motivation needed in a long, long, long journey.

Jack Kerr,
Wien, 2015.

Acronyms

STS: Science and Technology Studies

ANT: Actor Network Theory

SCOT: Social Construction of Technology

UK: The United Kingdom

US: The United States of America

EU: The European Union

WSJ: The Wall Street Journal

WP: The Washington Post

AT: ArsTechnica

TG: The Guardian

TDT: The Daily Telegraph

TR: The Register

CCC: Chaos Computer Club

PIN: Personal Identification Number

AI: Artificial Intelligence

AFIS: Automated Fingerprint Identification System

NSA: National Security Agency

1. Introduction

The problem with expectations is that ontologically, they are exactly that: something that is expected but will not necessarily become reality. Even if expectations do eventually lead to reality, the timeline of their implementation, as well as end result is a key problem and difficult to predict. In 1975, *Business week* famously hyped the future of the paperless office, and many industry experts agreed that computer electronics would replace paper by the early 1990's. The idea was that through being able to read documents from a computer screen and easily send and receive them, throughout an office and to other businesses, there would be no need to printout or use paper anymore. Yet almost 40 years since that claim, paper is still largely circulated throughout offices globally.

In fact, in Sellen and Harper's (2003) book, the 'Myth of the Paperless Office', they note how up until the turn of the millennium, rather than decreasing, paper production actually increased in many offices because of the ease at which an array of documents could be attained and copied through computer technology and the internet. They attributed this increase to the many more documents being printed because physical paper complemented the new digital technologies, and helped to add value to everyday work. However, since the introduction of e-readers and tablet computers in the late 2000's, as well as a change in thinking about environmental impacts of paper production, a shift has been occurring (Belz 2012). Libraries and book shops have decreased drastically, as newspapers, magazines and academic publications have moved online and people are becoming less inclined to print, especially for environmental reasons. This also seems to be because of the convenience and ease of reading from tablets and e-readers as opposed to laptops, leading to a revolutionary step towards a paperless world.

However, a decade after Sellen and Harper's (2003) book, paper still exists of course, and may well do indefinitely, perhaps as digital paper[1] in the future, though it still remains to be seen if one day the myth will become reality or not. Nevertheless, the story of the paperless office details the many problems with hype, prediction, timing and how technology is used, developed and adopted in society. The world of biometric technology has a similar story, in that as the tablet computer has increased expectations of destroying paper; a 'past' technology, perhaps the modern day

[1] At present digital or e-paper is in prototype stages, but the technology is essentially tablet computers as thin and as flexible as paper

smartphone has provided the seeds for biometrics, a previously hyped technology, to finally flourish. That is the investigation of this thesis.

Using science and technology studies, a field which has blossomed in recent decades to try and better understand the impact and roles of science and technologies *on* and *in* society, this thesis aims to map the debates around biometric technology and the expectations of its future implementation into society. Through a socio-political and socio-technical perspective, this thesis will compare media debates from differing geopolitical boundaries to show how media expectations have discussed the security and privacy issues surrounding the technology and their predictions on its implementation in a mass market perspective. Mass market in this context refers to a day-to-day use of the technology in an array of settings, outside of the current use mainly by police and government. Ultimately, this infers the expectations that biometrics could be used in such a 'casual' way of paying for a load of bread. How 'casual' this really is will be the subject of later debate.

To better understand this concept of casual, day-to-day use, imagine the following expectation of a possible future in which biometrics are a daily part of life;

> *You wake up in the morning to the gentle sounds of the ocean, echoing from your smartphone. You place your thumb carefully on the home button, stopping the alarm and accessing the home page. You rise from bed and head towards the television. Your smart TV analyses your irises and immediately switches to your pre-programmed channel. After getting ready, you leave your house; the door automatically locking behind you, before you proceed to unlock your car using your thumbprint at the driver's side door. On the journey to work in your self-driving car, you browse your phone, checking social media and your bank account. Each login requires a gentle press of your thumb for access, as well as the scanning of your iris for more secure actions such as a bank transfer. You arrive at work and use your finger to access both the door of the building, as well as simultaneously signing in to work for the day. Upon sitting at your desk, your computer scans your iris and turns itself on, back to the point you left it last. For lunch you head out to the cafe across the road and order an ice coffee and a bagel. To pay you simple press your thumbprint on a sensor connected to the cash register. Had the purchase been over $100, your iris would have been simultaneously scanned for double authenticity.*

This imagined future or 'sociotechnical imaginary' (see Felt 2013) utilizes a combination of biometric technology, interwoven seamlessly with 'the internet of things'[2]. It uses technologies that presently exists and are either already used in society or exist for now only as a prototype and are seldom used. Presently, for example, one can already access ATM's or make payments using just their fingerprint in certain places throughout the world, such as the supermarket chain *Auchan* in Villeneuve-d'Ascq, France (Winch 2013). Although these instances are increasing, they still remain rare to find and much of the uses are still being tested. Nevertheless their increasing implementation in society is evident. Just as signatures for bill recepts and/or PIN codes for financial cards became synonymous with payments and strongly embedded in society now for decades, perhaps the same might happen to biometrics. But before arguing on the expectations of biometrics as the 'password killer', one must understand the paradox of the password, and how despite its many flaws, its use has remained strong for decades. But what has changed? Why is the password being questioned more and more in recent times? Matt Honan brings forth an opinion.

Mat Honan's (November 2012) article in Wired titled, "Kill the Password: Why a String of Characters Can't Protect Us Anymore" caused remarkable buzz throughout the tech community questioning the future of the password and online verification, with the story boasting over 33,000 shares across multiple social media platforms. The front page story of Wired's November issue detailed how journalist Mat Honan's many online accounts, including his Apple account, email and twitter had all been hacked into over the summer. He details the exact way the hackers managed to do this, citing problems with 'password recovery services' and easily guessable 'secret questions' which allowed perpetrators to easily get around the many walls which users believed stood in the way of hackers.

First of all, Honan strongly noted how difficult many services make it to create a password, especially when having to remember passwords for so many different websites, and other services. Apple for instance for its online Apple ID states that "your password must be at least eight characters long. It must contain at least one number and two letters, one upper case and one lower case. It cannot include more than two consecutive and identical characters. It cannot be the same as your Apple ID or be any password you have used in the past year" (Apple T&C 2015). Even with this over-complicated requirement, what Honan notably describes is that regardless of the sheer length of his personal passwords, number of symbols used and randomly spelt words, it nevertheless proved no match for the hackers who found other ways for access. The crux of his argument is that he suggests increasing multiple problems with 'the password' and online identity verification in the 21st century.

[2] The internet of things is said to be the connection of an array of physical devices to one another through the internet and wireless technology.

Not only is the convenience factor very low through the difficulties of setting up a complicated yet memorable password, but in the end, security was a problem too.

The biggest problem he mentions is the daisy-chain effect whereby, in a bid for convenience, people use the same password for multiple sites and therefore if a hacker has access to one account, they have access to others. This story of Honan's is not new and over the past few years multiple hackings of online accounts have occurred (Oates 2011; Imperva 2012) and user details from big companies such as LinkedIn, Yahoo, Gawker, and eHarmony have all been affected. In 2013 a hacking of the Associated Press' (AP) Twitter account (Kwek 2013) further rattled the industry with the hack directly causing the New York Stock Exchange to plunge billions because of its automated nature.

Furthermore, as Honan mentions, passwords are a huge industry for organized crime which in "2011 Russian-speaking hackers alone took in roughly $4.5 billion" (2012:para42). Especially in light of 'the cloud', and the increasing rise in social media, details about people's entire lives including all of their data are becoming increasingly embedded online. With hugely influential companies, like the AP, becoming a very trusted and important online actor, the outcome of unauthorized access and identity theft online can be very detrimental to society and individuals such as politicians and celebrities who in recent times have had many of their online photos from the cloud hacked.

In light of all of these recent events, the argument to increase privacy and security in an array of different services has been strongly developing. Although there are solutions for improving password security systems, which are used in more personal online verification already, the problem is that there is a distinct trio of factors: security, convenience, and privacy, in users' uptake of different password systems, which makes implementing all three quite difficult. Honan (2012) notes that the best improvement and the only real solution to the current password system, is known as two-factor authentication in which a person combines their password (something they know) with something they have such as an SMS from their phone or a small electronic token that emits an extra code to use for a short period of time. This already commonly exists in financial areas whereby people use a credit card (something they have), and a PIN number (something they know).

Up until recently, the use of two-factors has been less common in other internet and computer uses for user verification. In light of the AP Twitter hacking, Twitter subsequently shifted to a two-factor authentication system (if the user wishes) and joined the likes of other tech giants with similar systems; Google and Facebook. However media attention has maintained criticism of the two-factor system (Gonsalves 2013; DesMarais 2013), especially for big companies, because of both the convenience issue of shared accounts and the second-factor authorization only going to one mobile

phone, as well as the problem of a code sent to a phone being intercepted making the two-factor still prone to attacks.

In Honan's article he mentions biometrics as a possible way to bridge the trio of factors mentioned above and to help solve the problems with hackings and identity theft, though he does identify a couple of major flaws with the technology. The first he notes is a chicken and the egg conundrum whereby "fingerprint readers and iris scanners are expensive and buggy, no one uses them, and because no one uses them, they never become cheaper or better" (2012:para55). This has to an extent changed with the iPhone's 'Touch ID', but to what extent will be further assessed later.

The second problem he mentions is that realistically (aside from dramatic plastic surgery) biometrics can't be replaced once hacked. This seems to be one of the biggest issue biometrics deals with. A password can easily be changed once it is compromised, but as the Guardian (Campbell 2013) hypes, people struggle with the issue of having a finger chopped off if one wanted to use someone else's biometric makeup to access one of their devices, or the inability to change ones facial features or fingerprints once a person has access to it. The fingerprint being chopped off by attackers is quite absurd, as a later section will detail further, but the issue of an unchangeable 'password' that fits all, still remains poignant. Biometrics also poses problems of user privacy, such as becoming a mass-classification systems and questions who has access to the data. It also raises issues of security and whether or not it is more effective at stoping hackers than a password.

It is the goal then of this thesis, to assess the expectations of these issues, note how strongly the scepticism is by both media and public comments, and note the extent to which biometrics may in fact be the solution to the paradoxical password by providing a solution to having the utopian trio of convenience, security and privacy. To achieve this, this thesis is organized as follows. This first chapter has given a brief summary of the overall aim. It has provided an imagined future of biometrics, outlined some of its inherent issues, shown the problems with the password, and the narrative formed about needing a solution.

Chapter two will first of all clarify the difference in definitions of biometric 'identification' and 'verification'. Through these definitions it will show how a shift in discourse is occurring and discuss if this shift has assisted in the expectations of biometrics growing on a day-to-day scale. It will then delve more thoroughly into the history of biometrics on both a broader scale, starting from a theoretical sense of the technology, before focusing closely on fingerprint identification, which is the main case study for this thesis. In brief it will argue that since the development of fingerprint identification in the late 19th century, among other mechanical ways to measure distinct human

characteristics and traits such as facial recognition and iris scanning, the expectations to transfer the human identity into the non-human world has risen in differing fields. Using Cole (2002) and Lynch et al. (2008) as a basis, it will discuss the dominant uses of biometrics in crime scene investigations from the mid 20th century through DNA evidence, as well as it being used for passport control and border security in recent times. It will then show that up until the very recent present, biometrics has lagged behind in other hyped day-to-day uses outside the realms of police and government, whereby the mental password and physical items, like keys for locks have remained strong. Chapter two will then conclude by leading up to the impact of smartphones as a means to mass produce biometrics and bring it into the mainstream.

Chapter three will look historically about revolutions in technology, especially mobile, and question whether the internet and smartphone are the start of the developed world entering the Third Industrial Revolution, through the Internet of Things. It further details how these technological revolutions have made way for the smartphone to spark huge innovations in industries leading to the case study of this thesis on the iPhone 5S and its fingerprint reader Touch ID which was released in September 2013. It will discuss how the mainstream nature of the iPhone 5S has provided the possibility of a large expansion in the use of fingerprints for secure access of one's phone, allowing biometric technology to be utilized daily by millions of people around the world.

Furthermore, chapter three will highlight two timelines surrounding the release of Touch ID, which is the basis for analysis for this thesis. These timelines are from the announcement of the iPhone 5S on September 11th 2013, to the subsequent hacking of the device on September 22nd 2013. The chapter will talk in detail about the hacking case, and reference the video of the iPhone being 'hacked', which will be used for subsequent analysis in Chapter eight. The chapter will also discuss in brief the problems with the word 'hack' and the overall impact of the 'hacking culture' on how privacy is understood around the device. This will show how there can be such a thing as a good hack (see Feinberg 2014), and how it affects the expectation on the future of the device, and on the terminology media and users tend to use.

Chapter four will then be the state of the art of the thesis, which will be divided into different actors and different issues surrounding biometric technology. The five actors surrounding this topic will be academics, journalists, governmental bodies, industry bodies and marketers. From these five actors, the issues of privacy, security, and convenience will be compared and contrasted, and then the emphasis and influence which each actor has on each issue will be analysed. It is important to compare these actors to show what role each plays on the expectations of biometrics becoming a day-to-day, casual system, and how the actors affect one another.

Using the perspective from the computer science literature (see Jain et al. 2004; Jain & Kumar 2010), a strong argument for the insecure nature of biometrics, especially in regards to fingerprint analysis is then made. The literature debates the fail rates of fingerprint analysis and identification, and Cole (2002) furthers this with studies on DNA analysis in crime scenes. From a more privacy oriented perspective, van der Ploeg (2003, 2005) notes how biometrics represents a kind of Big Brother, whereby a person's identity becomes ordered and classified in society.

Furthermore, surveillance studies such as Introna & Wood's (2004) paper on facial recognition systems discusses a sort of paradox between being secure and insecure at the same time, which relates to the comparison of a mental password, and biometrics (the physical password). This is in regards to individuals being surveyed to help to spot terrorism, but simultaneously taking away ones privacy. The marketing and industry body actors tend to lean more towards the convenience aspect of biometrics, and unsurprisingly present it in much more of a positive light. Through surveys, and research, they show how biometrics, despite its flaws, are the future of identity verification.

Chapter five will introduce the main research question this thesis will answer and splits it up into sub-questions to complement the discussion. The questions will also include hypotheses' of possible results which were developed before the empirical research took place. The actual main question refers to how both the release and hacking of the iPhone 5S was reported about in both US and UK media articles. This represents the entirety of the empirical thesis as, in a nutshell, it is a discussion on the media debates, and the affect of media, as well as user comments on such media, and how it relates to expectations, specifically in biometric technology.

The sub-questions then detail the different discourses the main question presents. One question discusses how the differing geopolitical nature of the media articles affects how the expectations are represented. Another looks at how both the differing timelines, before and after the hacking, affect the discussion. The third then looks at the different discourses of the media genres and their affect, and the last looks at the role of video, and how it being embedded in the article, as well as its content, timing and production, played a role in the development of the expectations by both the media, and the user comments presented in the same context.

Chapter six details the preparation to answer the main question, including the different ideas originally thought of to try and answer said question, as well as the final decision on the materials and methods chosen. The materials chosen are a total of 18 media articles, 9 from the US and 9 from the UK, both from differing timelines i.e. one with articles just before and at the announcement of the iPhone 5S, and the other following the 'hacking'. Furthermore a video of German group, Chaos

Computing Club (CCC), which is embedded within one of the articles, is used to complement the articles and to show the effect of video on the hacking culture and the overall discourse of biometrics, and how it relates to future expectations of it.

The exact method used is a discourse analysis in qualitative detail of the articles, by noting key words used, and the relationship between weasel words and words of hype solidifying the expectations. The headlines of the articles are compared with the actual content, to see how much the headline is used as more of a 'click bate' style, and the affect of the headline and opening paragraph on the rest of the article. This is done similarly with user comments, with a qualitative analysis of some of the key debates being presented in the comments, as well as comparing them with their geopolitical contexts.

Further, a quantitative analysis is also used for both the content of the articles, as well as the content in the comments sections to look at what keywords are used the most. This analysis especially looks for the terms 'privacy' and 'security', which in comparison with the qualitative analysis, discusses what both the hype displayed by the media and users comments believe to be the most important aspect of the biometric technology.

Chapter seven then looks at the topic in a theoretical view through the theorizing and sensitizing concepts to be utilized for this thesis. It will explore the 'sociology of expectations' (see Borup et al. 2006) which is one of the main forms of analysis for this topic. This will be complemented by both Actor-Network-Theory (ANT) and the idea of co-production in the development and expectations of biometrics through the differing actors; the security features of the technology, the marketers, journalists and users, all complementing one another in the realization and social adoption of the technology. This will show examples of other technologies and how they have developed and become co-produced through a socio-technical relationship. Lastly, it will theorize on the case of biometrics through its changing discourses (see Foucault 1979) to see how a shift from biometric identification to verification could pave the way for more casual day-to-day biometrics as well as how it is used as a classification and ordering system (van der Ploeg 2003).

Chapter eight contains the main empirical work of this thesis, comprising both media article analysis and video analysis. It provides a brief analysis of all 18 articles by looking at their particular perspective, to see which issue seems the most important, as well as analysing whether a positive or negative tone was placed on each respective issue. It further displays this analysis in a table form and compliments it by grouping keywords, sources used, and user comments, to paint an overall picture of how biometrics are reported on in the articles. It further compliments this picture with a

video analysis of the hack which highlights the political nature of some of the objects in the video, and how the video reflects hacking culture and the issue with security and privacy in Touch ID.

Chapter nine includes a discussion of the results obtained from the empirical research and how they reflect the hypotheses outlined earlier. It also analyses the relationship between the two data sets, that is discourse and content analysis and video analysis, and shows how each complement one another in outlining the expectation of biometrics.

Chapter ten then suggests further possible research for this topic which results from the empirical research being interesting for future studies of biometrics in more casual settings. It also briefly discusses other forms of biometrics and looks at how future research might relate to them as well as fingerprint identification.

Chapter eleven concludes the thesis by summarizing all of the data presented, and speculates and hypothesises on the future of biometrics as a day-to-day, casual system. It argues that the future use and adoption of biometrics in other circumstances is still up for debate and questions whether biometrics can ever be truly casual.

The challenge is that from the imagined future displayed earlier in this chapter, one must ask if *this* future is in fact desired. If that is the case, then to develop biometric technology into this desired future, it must maintain a high level of security and privacy for members of society which cannot be just seamlessly interwoven into a large technical system for a convenient answer to losing a tangible key, or forgetting a password. As has been suggested, much, if not all the technology currently exists to recreate the above solution. But just because it is possible does not mean it will happen. Thus, the purpose of this thesis is not to prove that this imagined future is destined to happen, nor is it to argue against the possibilities or say whether it should happen or not. Rather it attempts to account for the relationship between technology and society through media expectations of biometrics.

Using media analysis, this thesis will prove a strong relationship between how media hypes and discusses expectations for the production of technology, and how - using the idea of Sheila Jasanoff's Co-production (2004) (which will be expanded on in chapter seven) – the media affects social adoption of these technologies and vice versa. By doing this, the thesis will produce an analytical discussion of such an imagined future at the helm of biometric technology, and the possibilities of its day-to-day casual adoption. It ultimately suggests though that it is the changing discourses of how the technology is exactly used, that is the crux of this 'imagined future'.

2. History of Biometrics

In order to understand the expectations and framing of biometrics in both a present and future setting, it is necessary to discuss its historical background, to understand in detail how the technology has developed, adapted, emerged and been utilized throughout the past. In order to do this, it is also important to provide a proper definition for biometrics. As will be clarified and discussed in the definitions section of this chapter, a crucial impact to the future expectations of biometric technology are the implications of how, and in what discourse the data is exactly used, depending on the context, and what a person is actually classified as when this data is used. This becomes a large part of the privacy debate surrounding biometrics and this idea of identity is discussed by Lianos & Douglas (2000) in which they note how ones identity is described and the language used for it shifts depending on the context, causing a difference between 'identification' and 'verification'. This shift, as will be discussed, has strong sociotechnical impacts to the expectations and future of biometrics.

After clarifying these definitions, this section will begin with an early history of fingerprint biometrics, and discuss its broader role in society, before in detail discussing the 'analogue' Bertillon system and later digital uses of the technology during the 20th centuries through the studies of Cole (1999 & 2002) and Lynch et al. (2008). The crux of the studies focuses on how ones physical signature becomes translated into the digital world, and how this translation poses implications to one's actual identity and privacy being part of a criminality discourse.

Furthermore, although Martin (2011) distinguishes between 'identity' and 'identification', as will be shortly revealed, 'identification' will be used more dominantly in the fingerprint section as the majority of past studies (and to an extent, in the current uses of biometrics) have been for the 'identification' of humans. It is only in recent times, as this thesis will argue, that the discourse of biometrics as a 'verification' use has become more prominent, as it becomes more understood that in many day-to-day, casual biometric interactions, someone's actual identity is not necessarily needed.

2.1 Biometric Definitions

To begin, it is important to understand that biometrics is not an easily defined technological classification. To a certain extent, the knowledge and use of biometrics at the most fundamental level has, and will, always exist in all living beings with cognitive thinking, capable of sensing unique

traits and differences in each other. In regards to humans, biometrics as known today, originated from processes used over thousands of years; "Since the beginning of civilization, humans have used faces to identify known (familiar) and unknown (unfamiliar) individuals" (Jain et al. 2012). This means that in the most basic understanding, biometrics can be about both physical and behavioural characteristics and is essentially about telling humans apart by these characteristics. The home office in the UK for example, puts emphasis on uniqueness by describing "a biometric is a unique identifying physical characteristic. Examples include facial recognition, iris patterns and fingerprints" (Home Office 2004:36). This definition can also fit into a type of anthropometry or what can be seen as 'soft biometrics'.

Soft biometrics is something constantly used by members of society to identify one another, such as by knowing peoples facial features, their height and weight, their ethnicity, their eye colour, how they dress and so on. When humans have prior knowledge of others, such as recognising close friends, family members, and even the ability to recognise differences in identical twins, this form of soft biometrics is still very natural and effective in identification. As Reid and Nixon (2011) note, "one of the main advantages of soft biometrics are their relationship with human description; humans naturally use soft biometric traits to identify and describe each other" (2011:1216).

The actual origin of the term 'biometrics' on its own, comes from 'bio' meaning life and 'metric' meaning to measure, and hence, biometrics, as it is currently understood, is more in the league of 'hard biometrics' because it is about being able to measure or quantify a biological being and use these measurements or characteristics, which are inherently unique, for identification. Through this ability to identify uniqueness in beings, this has become evolutionary in a range of things from identifying gender, family members, and different types of species, among other traits which may inform a being of a possible danger. The terms 'soft' and 'hard' do the same thing, although are at different levels, and in many cases, they can complement one another in biometric identification as Jain et al. (2004) shows. The crux then of biometrics is the differing characteristic and the uniqueness of different beings.

When looking specifically at 'soft biometrics' one must be careful, as many studies on problems with eye witnesses and facial recognition of strangers have shown (see Megreya & Burton 2008; Steblay et al. 2003). Soft biometrics on its own is not exactly fool-proof due to human error with similarities in people's appearance which is hard to determine without a better understanding of peoples 'soft' characteristics. Since the invention of the computer and digital technologies, computer scientists have been arduously studying how to use computers to move away from the human error of soft biometrics and instead use non-human computers to make classification and identification full-proof

and wide-spread through 'hard biometric' analysis. The struggle with this attempt at full-proof technologies and/or extremely low fail rates is further discussed in the security section (see Jain & Kumar 2010; Davies 1994b) in the state of the art.

So what biometrics is known as today would be classified more as digital or 'hard' biometrics, though 19th and early 20th century fingerprint identification is a slight exception and will be further expanded on later. Essentially though, a biometric system uses human characteristics such as a person's fingerprints, iris, face, voice and/or many other characteristics for verification in order to determine who a person is, which *can* eventually lead to identification.

2.11 Biometric Identification / Identity

The emphasis on 'identification' relates very strongly to ones 'identity'. Although Martin (2011) describes a difference between these terms by noting that identity is "deeply personal and relational" (2011:19) whereas identification is more technological, both still inherently refer to providing proof and uniqueness to a person, revealing *who they are*. Through biometric identification, ones fingerprints could be used, not just to give one access to something, but also to show exactly who they are, and depending on the context, many things about their lives which make up their identity. Two distinct examples of this can be shown in the contexts of border security, and criminal investigations through DNA fingerprinting. For example, let's take a man; call him John Smith. John wants to enter the Unites States. As John is not a US citizen, he must, upon entering border security, scan all 10 of his fingerprints at the immigration desk as well as have a camera capture a photo of his face. He also provides his passport so the immigration officer can cross reference the data. According to *ezbordercrossings* (2014)[3], a website with information on border crossing procedures between the US and Canada, the immigration officer's computer, after John showed his passport and scanned his fingerprints at the

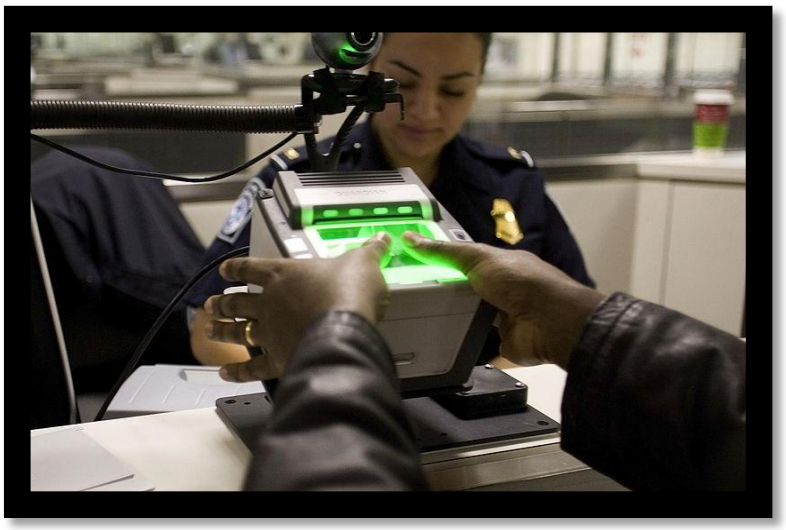


Figure 1: A man scanning his thumbprints at a border security checkpoint in the United States. The Camera above also captures his facial features. *Source: (BetaNews 2014).*

immigration desk, would detail John's "name, date of birth, citizenship, address, mode of travel, and purpose of travel" (2014:para3).

However let's say on this particular circumstance, John is flagged because he overstayed his visa last time he entered the US. He is then taken over to a secondary screening, where the border control officers have access to his criminal history, employment, family names, and his history of border crossings in other countries. What this example shows is that through identification, a person is not just gaining access to something, such as being able to enter a country through border security, but they are revealing who they are in the process - their identity.

Another example of biometric identification can be found in criminal investigations. Although this process may differ in different countries, in the US for example, when one is arrested for a crime they have their fingerprints taken, which are then placed on file along with the rest of a person's identity i.e. their personal details about place of birth, date of birth etc. If their fingerprints are then found at a crime scene, the prints are forensically examined, to determine if the prints are already on file, which then creates a 'match' and shows directly who that person is including their whole identity. Cole (1999 & 2002) disputes this exactness in identity, as will be explained later; however what this example shows is that using biometrics to verify a unique characteristic, such as a fingerprint, can lead to biometric identification of the whole of a person's identity.

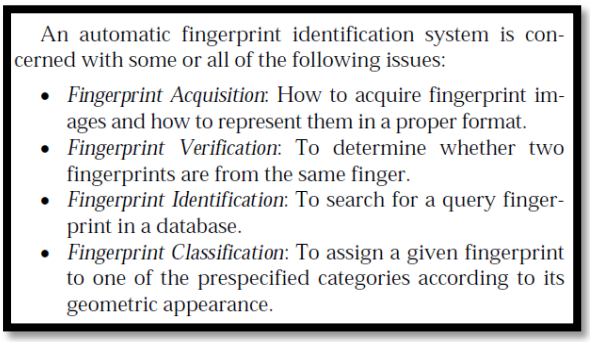
2.12 Biometric Verification

First of all, 'verification' and 'identification' are at times, especially in the past, used concurrently when talking about the process of using biometrics, and it is not always necessary to distinguish between the two. Secondly, although there are subtle differences between 'verification, 'authorization' and 'authentication', in the context of this thesis, they are all fairly similar to one another. Yet crucially, they are quite different to 'identification', due most dominantly to the absence of 'identity'. As explained before, identity is exactly who a person is, including both their physical and social characteristics which could range from their height and weight, to the name of their dog and their favourite movie.

Verification however, is a word that does not necessarily mean that a person's identity has to be revealed - depending on the context of course. All verification really shows, is that a match has been confirmed between two sources. Whatever task is taking place, or whatever needs to be authenticated, the process of verification creates a certified confirmation or a 'match' between two things, and access to a certain service is then given. What is crucial is the extent to how much one party knows about the other party. Again it is context dependent, but verification should mean only necessary information is transferred so that the only information, is that a person is authorized to do

what they are trying to do. See for example, figure 2 which clearly illustrates these differing definitions in fingerprint identification systems.

Furthermore, Lianos & Douglas (2000) give some useful examples when discussing the context of a situation and how this relates to whether one needs to be 'identified' or 'verified'. They argue that it has a lot to do with discourse, as well as word choice in certain circumstances. For example, they note, "to a telemetric service one is a 'caller', or more precisely a valid caller number. One is a ticket-holder in carparks, a 'press to cross'-button-pusher in pedestrian crossings, a 'too-fast-walker' in shopping malls..." (2000:265). That is to say, in each of these contexts, only certain verification and knowledge about a person is needed. When getting a ticket for a car park, you only need to verify that you are in a car, which in many automatic car parks is measured by simply the weight of a car. Thus to the nonhuman machine you become a 'ticket holder', not 'John Smith' and his whole identity.



An automatic fingerprint identification system is concerned with some or all of the following issues:

- *Fingerprint Acquisition*: How to acquire fingerprint images and how to represent them in a proper format.
- *Fingerprint Verification*: To determine whether two fingerprints are from the same finger.
- *Fingerprint Identification*: To search for a query fingerprint in a database.
- *Fingerprint Classification*: To assign a given fingerprint to one of the prespecified categories according to its geometric appearance.

Figure 2: How a fingerprint identification system distinguishes each step. *Source (Jain et al. 1997:302).*

This idea becomes clearer when looking at the impact of identity and the human versus the nonhuman. With automation, verification as opposed to identification becomes all that is needed for many services and identity can *theoretically* be protected such as in the example above. With human to human interaction, there is facial recognition between humans, seeing how one another dress, hearing perhaps each other's voices. All of this becomes a way to identify someone. Of course this is only part of a person's identity. Obviously this is not to say that identification is inherently a bad thing, and of course in many circumstances identification is the basis for social, friendly, human interaction. What it does though, is theorize that in certain situations humans want to protect their identity, and therefore a bridge needs to be built between identification and verification.

There are many more examples where people only need reveal a necessary part of their identity to be verified, without actually being identified. When one uses their credit card to purchase something for example, a card number and possibly a PIN verifies them. The card probably says their name, but that is the extent of the identification. One advantage is that with biometrics for example, there is a possibility of absence in financial transactions of a person's name, or their credit card number, which to an extent makes purchases more secure.

So when analyzing both identification and verification in the context of biometrics, the issue of privacy has two differing narratives depending on the context in which it is told. The whole issue with privacy comes down to how differing corporations, government or non-government, store biometric data, and to what extent having access to ones fingerprint, reveals ones actual identity. The privacy section in the state of the art, will further analyze this difference, but it is crucial to understand how being verified and identified are two distinct things in biometrics.

2.2 The Rise of Modern Biometrics through a Criminality Discourse

Over time, the human body has increasingly been seen as a unique identifier and because of this; many differing biometric techniques have been employed as a way of identifying differences in individuals throughout history such as the Bertillon system and fingerprint identification which became popular in the late 19th and early 20th century. As far back as Babylonian times, fingerprints for example, made in clay, were used for business transactions as a form of physical signature to confirm the identity of two parties. Although people perhaps attempted to contrast differences in the prints in order to identify individuals, fingerprints for much of history were simply used more as symbolic gestures in official documents and contracts be it in clay, ink or stone. It wasn't until the mid 19th century that the fingerprint, as well as the Bertillon system, started to become used as a tool in criminal investigations, largely to identify recidivists, previously arrested criminals. The modern era of biometrics was indeed born through a criminalist classification discourse as the following section explains.

2.21 Fingerprint identification

During the 1890's in Argentina, France and Britain, fingerprint identification bureaus were set up, and fingerprint analysis, started to become increasingly used as evidence for convictions. Over the next few decades many other countries followed suit and "...by the 1930's it was widely accepted that when a fingerprint expert declared a match between two prints, such testimony provided unambiguous evidence of identity. Courts were willing to accept that no two sets of fingerprints are exactly alike, and they reasoned from this assumption that latent print identification must be 'reliable'" (Lynch et al. 2008:11). The problem that Cole (2002) mentions is that, even considering broad underlying assumptions that no two fingerprints are alike, the system relies on trying to match two different prints, a latent print from a crime scene and an ink print from an archive. That is, two different settings where the former may only be a partial print. This creates issues about how so-called 'matches' are used as evidence in court as the different environments make it hard to be sure the two are the same print. It is then, "more about likeness than about unlikeness (Lynch et al. 2008:11).

Further, the actual 'science' behind the analysis is another strand of debate which has continually been questioned, with two schools of thought in latent fingerprint identification. As Cole (1999) explains, fingerprints are identified through two differing processes which he label's "counters" and "ridgeologists". The former is a cause for much scientific scrutiny because of the lack of scientific basis to it, where it is seen as a more technical process whereby the similarities between two fingerprints are merely counted. The latter then takes a more holistic approach whereby not only the 'points' are looked at "but also the size and orientation of the points themselves, the location of pores along ridges, and the characteristic of the ridges themselves" (1999:141). In a scientific sense, the ridgeologists are considered more pure and objective because they can reveal differences when counters reveal the same as 'identical'. However the counters argue that their technique has a proven track record for over a century and is widely used in court cases around the world.

Cole's (1999) paper then looks further into how certainty is practiced between both schools of thought. Where counters argue that their method is an "exact science", ridgeologists believe that fingerprint identification is based on a model of scientific expertise "which stresses credentials and knowledge rather than consistency and reliability" (Cole 1999:144). Ridgeologists also don't mind being uncertain if the science can't be proven, whereas the counters would rather be ignorant and prefer results over a strong scientific basis. In addition to this there is a lot of debate with the counters in terms of how many points are necessary to create a certain match between two sets of prints. It is suggested that without a certain number of identical points, two fingerprints could be perceived to be alike. Therefore what all of these debates demonstrate is that although both schools of thought have their accuracies, the problem is when *almost* perfect becomes perfect, when *probably* a match becomes a match, because just a few percent margin of error could potentially destroy a person's life through a false conviction.

Further, what is crucial in all of these debates is that there is a big distinction between testing techniques in the lab and proving them in a real case. One of the biggest issues in criminal investigations, as alluded to before, is that there is not necessarily always a clear fingerprint left at the scene and therefore a lot of forensic work involves analyzing partial prints which have a much larger margin for error. Crime TV show's like *CSI* seem to ignore this fact and hence any chance of a fingerprint is celebrated with conviction, as opposed to reality when a partial print is not always enough.

To return to the ridgeologists and counters debate, it is interesting to note how they seem to represent a science versus the law battle whereby the former, the ridgeologists argue for scientific expertise to explain individual cases, whereas the latter, the counters, argue for a more law style of

standardization in counting patterns to make cases easier to homogenize. As Cole concludes, this debate still continues, and a huge problem is that "the world's criminal justice systems have little incentive to cast any doubt, no matter how insignificant, on the 'scientific basis' of millions of criminal convictions" (1999:166). In other words, it is much easier for the law to continue with the status quo rather than questioning millions of decided cases, just as the "innocence project" is now doing since the introduction of DNA evidence. Either way, the counters are still favored in the courtroom at present.

Further, as alluded to before, forensic evidence is assumed to be true and objective, and the terminology of a "match" is prominent to suggest that one can be certain of who committed a crime. In reality, aside from perhaps video evidence and confessions, fingerprints are the most objectively accepted piece of evidence to be used in court cases as the science of fingerprint identification is rarely disputed in the courtroom. Yet there is still no such thing as a true match. Outside the courtroom in academia, the process of fingerprint identification is closely scrutinized as illustrated in Cole's (1999) paper. Fingerprints don't necessarily lie and while most arguments suggest no two fingerprints are 'exactly' alike, the process of identifying fingerprints is the cause of many issues. Even though in reality the term 'match' is not used in the courtroom, there is still a strong implication that there is a match, even though there are problems in how this 'match' has been interpreted.

It has only been in recent times that STS schools of thought have begin questioning these assumptions of how science is produced and represented, and in terms of the development of fingerprint identification – how much of a 'match' is a 'match. It is thus crucial to detail this history as it helps reveal the modern day uses of the 'fingerprint' and how it functions in terms of security issues of biometrics. If biometrics is to indeed replace the password, then its different forms need to approach this level of perfection in accuracy, that of which much computer science literature debates about false match rates (see Jain 2010) as will be further outlined in the state of the art section. However, what these scientific debates make clear is that through a criminality discourse, the idea to use the body as a readable, *codify-able* being to be classified has increased dramatically, not just with fingerprint identification, but with many other aspects of the human body too.

2.22 The Bertillon System

At the same time fingerprint identification started to become popular, so too were anthropometry techniques through the Bertillon system. As a crime 'epidemic' began seemingly sweeping across Paris during the mid 19th century, in the wake of recidivists being one of the key problems in keeping law and order, French police official Alphonse Bertillon realised that "In order to condemn a

recidivist to relegation, the first requirement is the recognition of his identity" (Cole 2002:33). Before the Bertillon system, police relied on identifying repeat offenders through poor quality photographs, personal recognition and bounty shared between police and former criminals who helped identify their cell-mates (Cole 2002). The Bertillon system changed this by attempting to bring a more 'scientific' approach to identifying individual traits and characteristics from an array of different language and measurement techniques.

Realizing, first of all, that there was a distinct lack of specific language to describe the human body, Bertillon created a diverse range of 'scientific' terms which he called a 'morphological vocabulary' to bring more accuracy to identifying individuals. This could include for example a description of different lips which are "'pouting', 'thick' or 'thin', 'upper' or 'lower prominent', with 'naso-labial height great' or 'little'..." (Cole 2002:39) and so on. To compliment this language, he introduced pin-point accurate measurement techniques for a range of body parts which he concluded could not change much through age and weight gain. From these processes, Bertillon created a way to translate the human body into a sequence of information which could be organized to identify recidivists when they reoffended. As Cole notes, "Bertillon reduced the body to language and then to code - turning the criminal body into pure information" (2004:49).

Although the Bertillon system is now seen as an archaic method of identification, especially in light of a 1903 court case where two identical twins were found to have almost the same measurements, it was nonetheless crucial in the early construction of how the criminality discourse is measured today. It not only questioned the accuracy of photography for identification, but it changed physical appearance to a system of words and numbers, which could eventually be computerized, as it was later in the 20th century, leading to how biometrics is used today.

2.23 The Move to Digital and Biometric *Verification*

The ordering and classification of both Bertillon-style and fingerprint biometric information has increased dramatically since the invention of computing in the mid to late 20th century. The shift marked an extension of discourse from using biometrics for criminals to everyday people. It also shifted trust in humans to trust in non-human machines, as computer software began to be used to 'match' between two prints. This software, known as an automated fingerprint identification system (AFIS), became necessary in many countries such as the US because of a large increase in the need for fingerprint identification. No longer was it just criminals being subject to fingerprint identification, but civil record checks became common in many aspects of life, such as background checks for employment, visas and citizenship (U.S. Department of Justice 2008).

A key aspect of the privacy and civil liberties debate has been in data retention and how these civilian acts such as background checks, could result in biometric data being stored indefinitely by a country to be perhaps later used against the civilian. As the US Department of Justice report notes, "Thirty-one of the 44 states that responded to a June 2001 SEARCH survey of state repositories reported using at least some of the fingerprints initially submitted for civil purposes for subsequent criminal justice purposes" (2008:10).

The same debates have been raging in the UK, culminating in the 2009 European Court of Human Rights case, *S and Marper v United Kingdom [2008],* which decided if individuals who are charged with a crime, but later acquitted have the right to have their fingerprint and DNA samples destroyed. The court ruled in favour of the applicants who received monetary compensation, and although the law surrounding the retention of DNA and fingerprint samples from individuals who are merely charged but not convicted of a recordable offence changed, it still wasn't to the right to privacy standard in other EU member states. Many records of innocents were not destroyed due to bureaucratic issues, and the laws only changed to provide that samples could still be kept for a number of years, even if the person was found innocent.

As computer processing power became more powerful, and technology became cheaper (as the next chapter details) biometrics began to emerge from a criminality discourse, to a semi-criminal, semi-civil discourse, to eventually a 'casual' day-to-day convenience. That is not to say that the original discourse is not still there. It is still the dominant discourse of biometrics and is used ever more so through government classification. Many countries implement border fingerprint checks for foreigners and immigrants now, and schemes such as the UK biometric card, although a failure which will be further discussed in the state of the art of this thesis (see Martin 2011), are being further developed for monitoring the everyday law abiding citizen.

But what this thesis is arguing and debating is how far aspects of the biometric discourse of identification to verification has emerged and how and if, it will continue to emerge, as well as whether a casual biometric system can ever truly become separated from its criminalistic background. At present for example, the use of biometric classification systems are widely used throughout many governmental institutions including the US, UK, Canada, Australia, Netherlands etc., with fingerprint or facial authorization required when applying for a visa, to physically enter the country, among other governmental institutions.

However, the use of biometrics on a personal scale, such as in personal smartphones and computing, has up until recently been seen as either too expensive to implement on a mass scale, or

not accurate enough to be used because it has not seen as being more secure than passwords. Early laptop computers and quasi-smartphones did for example begin to implement biometric devices as a means to provide access, as opposed to use for criminal background checks and forensic identification and through developments in accuracy and convenience, biometrics are increasingly being used in business areas to be used to monitor employment logins in companies, and now it has been introduced to a mainstream device through the Apple iPhone 5S and its TouchID.

Overall, there is no need to doubt that there has been a shift in the discourse of biometrics over time. From a symbolic gesture, to criminality specifics, to citizenship and casual transactions, how and why biometrics are implemented has indeed shifted. This does not mean however, that the former, criminal identification, doesn't still effect the latter, casual verification. Technologically it may be possible to reduce privacy issues, increase security, and find biometrics in a casual setting away from such criminalist discourses. But, as this thesis continually argues, technological advancements develop and emerge through a co-production of science, technology and society. The past shapes the future, and how society sees the past, affects how it sees the future. How biometrics will continue to flourish and whether it can truly rid itself of its previous discourses will be ultimately based on the impact of this co-production.

3. Internet & Mobile Revolutions and the Case of Touch ID

The term 'invention' is a dying concept as, although still heard frequently, it is often misconstrued with innovation. Inventions do of course exist, but in a globalized world with an abundance of differing technology, it is really 'innovation' which stands at the height of technological entrepreneurship. Although invention is the father of innovation, in the technological sense, it is inventions' offspring, that is innovation, which lays the foundation for revolution. This chapter explores this concept of innovation with regard to how the emerging *invention* of the internet, was eventually harnessed through innovation by the mobile capacity of the smartphone, and how this has led to a revolution in human interaction and communication. This invention will be detailed to lay the platform for how these changing discourses may lead biometrics to do the same by giving it a distribution network, making day-to-day uses of the technology more accessible. The chapter then further details the history of the smartphone before giving specifics on how Touch ID was implemented, its technical aspects, and debates how all of these factors affect the expectations of it becoming a future, widely used verification system. Lastly it discusses the hacking of Touch ID by CCC and the overall implications of the hack on the future of biometrics.

3.1 The Third Industrial Revolution?

The invention of the Internet and eventually the World Wide Web in the early 1990's marked an undeniable paradigm shift throughout the developed world (see Kuhn 1962) equivalent to the harnessing of electricity in the 1800's and automobiles and aircrafts in the 1900's. In these cases electricity changed human life by provided the possibility of extended working and leisure hours through artificial light as well as providing a source for increasing the life of food through refrigeration, thus fundamentally changing day-to-day life. The latter, automobiles and aircrafts, changed how cities function in both a local and global sense, the tyranny of distance became minimized as extended transportation networks vastly reduced the time of travel between places. The internet did the equivalent by fundamentally changing how we access information and how we communicate and connect with one another.

Whereas electricity became dominant through what has become known as the Second Industrial Revolution, the internet's implementation marked the first step of the apparent Third Industrial Revolution (Rifkin 2011) whereby the Internet of Things creates a hyper level of connectivity and efficiency between all things, objects and people as the majority of society merge into the so-called 'smart city'. In the developed world, the Third Industrial Revolution seems to have begun, however

the full potential of what is to come is still a socio-technological expectations. Anthony Townsend's 'Smart Cities' (2013) for example, details a wide variety of projects throughout the world turning this idea of hyper-connectivity into reality, as he makes predictions and projections to how future cities will look like. The internet is, naturally, one key aspect that brings this hyper-connectivity to reality.

However, although the internet has dramatically changed how we communicate, it is the smartphone which has played a key role in shifting the internet from a virtual sphere in the 1990's, to a key aspect of day-to-day reality in the 21st century, providing the way for this Third Industrial Revolution to be as defining as its two older brothers were. During the 1990's, most scholars saw the internet as an entirely virtual or cyberspace, seen as an escape away from the confines of reality and therefore, research through internet methods was seen as such – separate from reality. But at the turn of the millennium, geography started to matter a lot more and shifted the idea of the internet from the cyber to the real, as Richard Rogers puts it, "the death of cyberspace [came] through the revenge of geography" (Rogers 2013:40). As geolocation services became more widespread, *where* you accessed the internet started to change *what you found* – and *who found you*.

Livingstone (2003) for example, makes similar arguments about the changing state of *placelessness* and universalism in science. He argues the shift in the idea of science needing to be universal and placeless to be properly claimed, to exactly *where* the science was being practiced actually mattering and having an effect on how it is perceived. Place matters. Hence, by bringing the internet from the lounge room to the streets, we have brought the virtual to become reality, and the smartphone has developed as this mobile device, with capabilities of revolutions in many different industries.

3.2 Access all Areas

Although Wi-Fi and telecommunication advancement have enabled internet connection through a multitude of devices such as tablets and laptops in multiple areas, nothing quite beats the mobility of the smartphone allowing the internet to be carried in the palm of one's hand. Through this 'mobile internet' (in the sense of both mobile telephone internet access, and movement ability) changing discourses of knowledge accessibility and communications have impacted society in a multitude of ways. From ruining the pub debate through an instant Google, to giving the scientist a sea of resources at the touch of a button, to taking a *selfie* and having all of your friends see it instantly on social media, to *almost* never getting lost again, with GPS always sitting in your pocket, the extent to which people now rely on their phones is remarkable and has even changed how we function. Many people feel lost without their phones with psychologists even coining a name for the condition, *nomophobia*s (Clayton et al. 2015).

Although not quite yet being an 'access all areas', with even airplanes introducing Wi-Fi in recent years, the smartphone has indeed provided a world that is increasingly hard to imagine without internet capabilities – especially in city metropolises. The ability to always have access has developed a strong reliance on the smartphone and a shift from the human interaction to the nonhuman, for example, using GPS as opposed to asking strangers on the street for directions or restaurant recommendations or meeting romantic interests in bars. Increasingly the smartphone and the internet is relied on to do it all for us. As Townsend puts it;

> *"Cities used to be full of strangers and chance encounters. Today we can mine the social graph in an instant by simply taking a photo. Algorithms churn in the cloud, telling the little things in our pocket where we should eat and whom we should date."* (Townsend 2013:16).

As society moves towards the smart city and the 'quest for a new utopia', technology is increasingly seen as the answer to reaching this utopia, yet paradoxically, also seen as the death of human interaction; the result bringing a dystopia through advanced AI changing what it means to be human. But this changing discourse of human and non-human interactions and different expectations of the future has two schools of thought (see Latour [Johnson] 1988). On one hand, the smartphone and internet has seen to reduce human to human interaction by making us more reliable on technology and non-human interaction. But on the other hand, it has seen to have increased human to human interaction by bringing more possibilities to meet people, share information with people, and communicate with people than in all of human history. In chapter seven, these ideas of human and nonhuman interaction will be further expanded, but what is crucial to recognize here is that especially through smartphones, the mobility of the internet has increased dramatically.

The smartphone has brought the virtual to reality, by turning the internet into a mobile, moving supercomputer sitting in our pockets, and as *The Economist* optimistically puts it, "much as the car and clock did in their time, so today the smartphone is poised to enrich lives, reshape entire industries and transform societies" (The Economist 2015:para3). Through its geolocation abilities, and such personal attachment to its user (literally being able to monitor its users health and movement), the fastest-selling gadget in history has becoming a walking, talking, listening and monitoring device, able to translate ideas into innovations by literally putting them into the palm of people's hand.

It is this ubiquity and everyday movement ability of smartphones which is where the story of biometric expectations fits in. Once 80% of the planet have these devices by 2020 (The Economist 2015), the possibility of more features, such as biometrics, being adapted by wider society increases dramatically. With the ability to disseminate on mass such a product, the determinism of the

technology becoming ubiquitous and taken up by society becomes all the more extreme. Though chapter seven will debate how this determinism is only possible through co-production.

3.3 Rise of the Smartphone

As with many technologies, without the inventions and innovations from previous generations, the modern day smartphone would have never been possible. By looking at the history of Moore's law and processing power doubling every 18 months, on one hand the smartphone was determined to happen. As microprocessors got smaller, more powerful and cheaper; turning a 1950's room sized supercomputer into an exponentially more powerful and cheaper palm sized phone, was - although an unbelievable notion at the time - according to Moore's law, predicted, expected, and perhaps even determined to happen. However, if ever there was a strong argument against technological determinism, it is in fact the smartphone.

The rise, fall and eventual rise of the smartphone came about through a mix of design, engineering and social adoption. The Blackberry released in 2002, marked the rise of the smartphone and considered by many as one of the first true smartphones by offering internet capability equivalent in part to that of a desktop computer of the time. However it never truly caught on, largely due to the design and the physical keyboard taking up too much screen space for such a compact device. What changed in 2007 with Apple's iPhone was largely the way it appealed in a humanistic way through developments in touch screen technology.

For the teenager too young to remember, or simply the adult that has become so used to it, Steve Job's key note speech of the original iPhone would seem benign. But at the time, a simple gesture such as zooming in with 'the pinch' or scrolling through artists, was revolutionary as it was done in a way that felt human – no learning required, and has since been adopted by all smartphone manufacturers as the norm. Following the iPhone, other phone manufacturers followed suit and by 2008, the smartphone market has continued to grow exponentially throughout the world to be almost two billion smartphones today.

This humanistic style of technology was instrumental in making this product into a must have device throughout the world. However it could not have been possible without WI-FI and telecommunications infrastructure growth allowing access in all areas which really assisted the smartphone's increase in mobility and transformation of geography and communications. In essence it was only through a co-production (see Jasanoff 2004) between social adoption and technological innovations that allowed this technology to flourish. One could not have been possible without the other as chapter seven explains of this chicken and egg conundrum.

3.4 Touch ID:

From a distribution network held by millions of people, and battles for innovations in an already revolutionary device, biometrics seemed the next step to transform the possibilities of the smartphone. As more important data became held on these supercomputers in ones pocket, expectations grew during the early years of the smartphone that biometrics would one day be a mainstream verification system incorporated in the devices. Speculation increased dramatically for tech giant Apple when they bought biometric security company *Authentic* in 2012. Leading up to the company's announcement of the iPhone 5S on September 10th, 2013, further speculation began of the biometric feature due to a leak in Apple's newest iOS 7 operating system in mid 2013. The leak showed that the software supported a biometric reader which all but confirmed the feature in the eventual smartphone and increased discussions on the effectiveness of the feature as a secure verification system. The iPhone 5S was eventually release on September 20th, 2013 with a biometric verification fingerprint reader. The speculation and rumors will become important in chapter eight through the pair of media articles which were chosen before the actually announcement of the iPhone, and because of this, had slightly different expectations, due to the lack of specific information of the device.

Once the biometric reader known as 'Touch ID' was officially announced, many news sources began hyping the expectations of the technology as biometrics was seemingly brought into the mainstream. Following this, a twitter post by security researcher, Nick Depetrillo put out a challenge, "I will pay the first person who successfully lifts a print off the iPhone 5S screen, reproduces it and unlocks the phone in <5 tries $100" (Depetrillo September 18, 2013). A competition then began for hackers around the world as a website was created 'istouchidhackedyet.com' and crowd sourced donations were added to a pot for the eventual winner. It was less than 48 hours after the phone was released that Chaos Computer Club announced on their homepage that they had successfully hacked the device which they eventually accompanied with video recognition of the feat and received almost $20,000 in prize money.

3.41 The Hack and Touch ID's Technical Aspects:

Aside from Apple having the distribution power to bring biometrics into the mainstream, how did the technology change? Apple after all did not invent fingerprint verification. As the previous chapter indicated, the technology has been around for a while. Fingerprint verification was used over a decade ago in old laptop computers for example, but the amount of ridges in a fingerprint that were measured was low as well as the resolution used and overall the system did not work very accurately. Apple hoped to change this by increasing the accuracy of the device and making it more

'secure'. However, Starbug, the main hacker of CCC behind the hack believes, the only real difference from older fingerprint scanners is that Apple used a higher resolution in Touch ID.

As Touch ID is similar to fingerprint verification systems used in the past, techniques have already been developed for hacking the system, so it is not as if CCC came up with an original hack overnight. On their website and in their video, CCC explain their step-by-step process of hacking the device in a way that makes it sound simple to do at home such as saying, "materials that can be found in almost every household…" (CCC 2013:para5). They first take a 2400 dpi high resolution picture of one of their fingerprints smudged on an iPhone. They then clean it up and invert the colors to have white as the background so the print stands out. They then print the image onto a transparent sheet, smear pink latex milk onto the sheet, and then breathe on it to make it moist after it dries, before using it on the home-button sensor to unlock the phone.

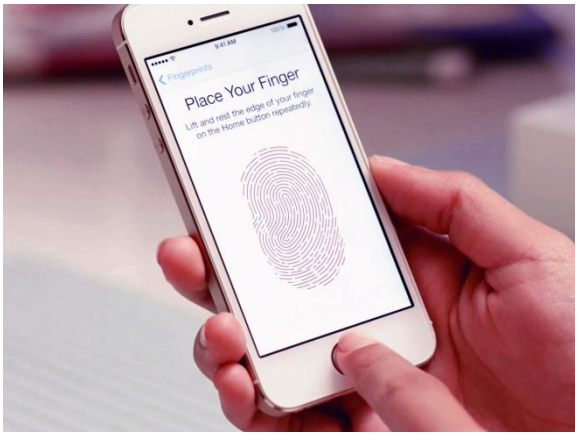


Figure 3: A Person sets up TouchID on their iPhone 5S by scanning their finger onto the home button. ***Source: (Perrot 2013)***

Although the hack seemed to be fairly straight forward and expressed in a very do-it-yourself fashion, experts were quick to criticize the simplicity of it by saying that it would require too much expertise and very expensive equipment for most people to be able to accomplish. Security expert, Marc Rogers thought, "Hacking Touch ID relies upon a combination of skills, existing academic research, and the patience of a Crime Scene Technician" (Goodin 2013:para2). Starbug was quick to retaliate, and still believed it was "very easy to do" with "inexpensive office equipment" (Goodin 2013:para15), however even with a strong skill set, and the correct equipment, one must ask why such a hack needed to be accomplished in the first place. How much value can the hack truthfully give to the security of the iPhone and using a fingerprint as a verification device in general? Or as the Guardian speculated, would people cut off your finger to access your phone (Campbell 2013)?

Starbug says that his main reasons for the hack were curiosity, to see if he could do it, as well as to prove that fingerprints are not a reliable verification system as people leave them everywhere and are too easy to copy. But Apple remains firmly confident in the technology as they mention (Arthur 2013) that although every fingerprint is unique, it is possible, but extremely rare (1 in 50,000) that two parts of different fingers are a perfect match thus fooling Touch ID. However, as they point out, that is five times stronger than the existing 4-digit PIN, so does this not mean that it is a more secure

system? This question comes down to the debate on casual biometrics and casual security which chapter eight and eleven will further discuss.

The last technical aspect of this system, or lack of, is a key to the commercial nature of Apple as a brand, and smartphone as a product, and of the overall security of the system. Some fingerprint scanners have been made which work at the sub-epidermal level, meaning that they scan both biometric features on the inside and outside of the finger. This technique is seen as more secure and harder to crack. When questioned about this feature, Starbug believes that Apple did use sub-epidermal scanning, however to try and increase convenience by making sure that the device worked more times than not, he believes they may have integrated a less secure threshold of depth for the scanner to scan at the sub-epidermal level, whereby the layer of tissue and outer skin are too similar.

These changing discourses and how society responds to such issues, is the direction of future debate of how and if biometrics will continue to increase as a trusted verification system. In short, is it security or convenience which is more important? If biometrics has a small fail rate, yet is 5 times stronger than a 4 digit pin, then what is all the fuss at the possibility of a hack, when the same can be said of the current verification system? Surely security and convenience wins here. However, as chapter two discussed, there is a distinct social change which must be addressed in changing verification systems from the inner mind, to the physical finger. People do not only worry about security and convenience, but also of privacy.

3.42 Privacy Concerns:

Another big concern finger scanning creates, is how ones biometric print is utilized and who has access to it. In the main timeline of this these, initially Touch ID allowed a user to both unlock their phone, as well as make a purchase on the App Store using their fingerprint. More recently though, they began allowing third parties to use Touch ID as well as with their new system, Apple Pay, used to make physical purchases. But there is also a market to expand this, to use Touch ID for many other everyday uses such as in logging into social media and online banking. Thus CCC, in their hack asked not only how secure fingerprint verification technology is, but also how well a person's identity and their biometric makeup can remain private.

CCC doesn't believe biometrics achieves this privacy protection. They believe that, "Biometrics is fundamentally a technology designed for oppression and control, not for securing everyday device access" (CCC 2013:para7). This refers to how the dominant arena biometrics are utilized at present are in forensics for criminal cases, as well as in government institutions for visas and passports. This is similar arguments made by biometric researcher van der Ploeg (2003) about biometrics creating

oppression and control as a form of classification system. She notes how biometrics are not just a new password, but rather something which embodies people more physically which changes the whole ontology of verification. Losing biometric information then becomes a huge problem, as it is nearly impossible to change, as opposed to a compromised password which can be easily altered. So by expanding this technology into the everyday, the technology, as CCC argue, increases this kind of government or corporate control of our important information which embodies who we are – our physical makeup. Hence, the hack not only asks a security question of accuracy, but also of our privacy, which is why CCC as a hacker group are very much against biometrics as an everyday verification technology, due to these flaws.

However, Apple responded to much of this privacy concern by saying that the fingerprint will never leave the phone. They believe that they designed a flawless system to combat hackers installing malware on people's smartphones who could try and create a database of fingerprints which would be detrimental to the company. Apple's head of software, Craig Federighi, states that, "no matter if you took ownership of the whole device and ran whatever code you wanted on the main processor [you] could not get that fingerprint out of there. Literally, the physical lines of communication in and out of the chip would not permit that ever to escape" (Arthur 2013). A case of maliciously obtaining a large amount of fingerprints from iPhone 5S users is yet to occur, but this begs the question, should it be done? Just as CCC hacked Touch ID to prove its lack of security, should it also be hacked on a larger scale to prove a lack of privacy?

3.5 The Politics of Hacking

Was it right for CCC to hack Touch ID? Most people, aside from maybe Apple would say yes. They have done nothing illegal, merely purchased an iPhone, used everyday materials, and shown the world how to gain access to something in a way that was not initially intended. On the whole of it, that is what hacking is; taking something be it digital or tangible, and repurposing it for another use. Jailbreaking for example, the term used to dignify removing limitations on a mobiles operating system to be more open source, has become common practice for many iPhone users, and although legal, Apple ensures that by doing so the device is void of all warranty. But just because something is legal, doesn't necessarily mean it is morally right. Just as when something is illegal, that doesn't mean that it is not morally right either. When deciding to hack or not, does the end justify the means?

When CCC hacked Touch ID, they took it upon themselves to influence public debate on the future of biometrics. Not only that, but they created a step-by-step guide of how to infiltrate (hack) someone else's property, their iPhone, and possibly use important information against them. This is

a pessimistic way to look at it of course, but it does raise the question of how hackers can influence others to use their techniques, perhaps in more malicious ways. What happens if someone uses the technique outlined by CCC to gain access and obtain precious data from someone's iPhone? A technique that, without CCC showing them how to do it, they would never be able to do. This is a common question in the internet age as it becomes easier and easier to share information, the problem lies if such information falls into the wrong hands. There was no clear malicious attempt in CCC's hacking, but there are other cases where a 'public good' hacking can been deemed questionable.

In US law, one is only breaking the law when gathering information, such as codes, if the information is used with intent to defraud. So does this mean that if someone were to hack a large number of user names and passwords, would it be ok as long as they don't post them online, or use them to defraud? Possibly, but this seems arbitrary. However, when looking at a recent hacking of 38 million Adobe accounts (Feinberg 2014), some interesting data comes to light. There is little doubt that the hacker who hacked these accounts did it with malicious intention; however, a small 'public good' did come out in the fact that the top 25 passwords were published. Without hacking, it would have been harder to gain a list of people's passwords to study. So by doing this, the issue of password security was raised and re-sparked debates on the need to have a strong, secure password, and/or the need for other verification systems.

In many other cases, this is what hacking does. Whether it be a good 'white-hat' hacker, or a bad 'black-hat' hacker, the result from a system being hacked is the knowledge that there is a flaw in the system which needs to be fixed. Hacking re-raises security concerns in otherwise believed to be tightly controlled systems. In the case of Touch ID, without it being hacked, it could be argued that too much emphasis would be placed on the perfection of fingerprint verification. This has been a strong issue in the mass production of biometrics in the problem with perfect matches. As Lynch discusses in his (2008) book, an inherent truth in DNA evidence and fingerprint matching has been adapted by the public over the years, yet as he says, this has been clouded by verisimilitude and he maintains the idea that a 'perfect match' doesn't exist, and that other forms of evidence are necessary to truly identify a person. This in turn raises the question of whether the Touch ID can be truly effective and secure. By CCC hacking Touch ID, it does at least allow people to remain cautious about their security as the results section in chapter eight will further develop.

4. State of the Art

The literature surrounding biometric technology can be separated into four main actors: academics, journalists, governmental bodies, industry bodies &marketers. Although each actor has their own biases and agendas, analysing each is important for an overall understanding of how the development and implementation of biometrics has occurred in the past, and its expectations for the future. As the aim of this study is to understand the media's framing of the expectations of biometrics, the overall focus will reflect this by analysing the affects of these actors on the media's expectations. Thus a section of this chapter will devote some time to literature on expectations. Although a deeper analysis of actual journalist debates will be undertaken in the empirical chapter of this thesis, this chapter will also include a brief summary of some of the prominent media articles to complement the literature from the other actors.

The literature can then be further sub-divided into topical areas of debate. The three debates which are discussed among the main actors are from the issues of privacy, security and convenience. The issue of privacy relates to how an implementation of mass-market biometrics could potentially hinder the privacy of individuals and it relates strongly with an assortment of literature on surveillance and identity studies which will be addressed prominently by the work of van der Ploeg (2003; 2005), Martin (2011) and Introna & Wood (2004).

The issue of security is then largely based on how successful different forms of biometric technology are in providing correct verification of individuals. The body of this literature makes up the large majority of studies on biometrics because of the discourse of biometrics in the past as explained by chapter two. Privacy was not as big an issue in past studies as the secure way of catching criminals was more important. Through the computational turn and increased accuracy in biometrics, the computer science disciplines became a prominent actor in biometric discussions (see Jain & Kumar 2010; Jain et al. 1997).

Lastly, convenience is also debated in a more social sense compared with the other issues and other possible verification systems such as passwords or physical keys to note the different strengths and weaknesses of each. This includes user adoption to the technology as well as debating the different forms of biometrics used i.e. fingerprint, iris etc., to see the possibility of how the social shapes technological adoption. Most of this literature is done through marketers and industry bodies who are trying to push convenience aspects of their product by focusing on the user experience (see AOpix 2012; Nok Nok Labs Inc. 2013).

4.1 Security

Currently the large majority of academic literature on biometric technology is through computer science studies into the actual effectiveness of the technology in verification. More closely, the literature looks at the accuracy of different biometric technologies such as iris scanners, or fingerprint recording machines, and ways of improving these systems for more successful matches. Some of this literature will be useful in regards to how the media portrays the negative aspects of biometrics such as its inaccurate qualities. But what is more useful is through the subsequent studies in law and STS from the early 1990's on the "CSI effect", and the increasing scepticism towards DNA and fingerprint evidence. Through studies by scholars such as Lynch et al. (2008), a lot of questioning of fingerprint and DNA being a 'truth machine' or 'gods signature' have debunked the accuracy of such measuring technologies be that in forensic investigation, or in biometric verification. The main problem lies in the fact that DNA and fingerprint identification have in the past created a strong sense of verisimilitude; that is that even though there is a very small fail rate in matches, the non-human biometric reader has been rather seen as providing a 'perfect match'.

As has been highlighted in *Wired* among other media sources, the new Touch ID has reflected these issues such as "phones that don't recognize when a finger is present to those that don't approve fingerprints they're supposed to approve" (Bonnington 2013:para2). The article notes that the main reason for the issues is because of Apple's desire of aesthetics, by making the fingerprint reader small and round they in turn made it harder to accurately read fingerprints without properly rolling ones finger across. Bonnington also concludes that some of the issues are caused by 'user error' and lack of biometric knowledge, and says that the biometric reader will improve over time. From troubles to solutions, the article begins by reflecting Lynch's ideas on the problems with fingerprint identification, but concludes with a rather optimistic outlook on how it will eventually work fine, ignoring the problems of perfect matches Lynch poses, to whom this thesis positions itself with.

Furthermore, Jain is one of the main actors of the security debate, as he has published much literature on accuracy and fail-rates with different biometrics. One of his papers (Jain et al. 2004) looks closely at soft biometrics to see what kind of influence they can have on improving accuracy. Soft biometrics as discussed in chapter two are not unique pieces of information to every person, but rather they are more of a casual distinguisher between two people such as the colour of one's hair, or their height. Jain et al. (2004) concludes the paper by noting that by adding soft biometrics to hard biometric systems, the match rate improves by 6%. But the problem is, in how systems such as this, which refers more to facial recognition biometrics, are actually designed. As the privacy literature (Intrana & Wood 2004) will further detail, by setting a nonhuman to interpret certain characteristics like skin colour, this creates strong bias in matches and a sense of discrimination in

classification. Thus the security and accuracy is not as strong, as it has different fail rates for different types of people, depending on how it is programmed.

Another paper, this time by a different author to the other Jain, (Jain et al. 2012) talks of the strong capabilities of fingerprint identification used in the past, and how computers have increased the impact of how they are used now. In doing so they mentions a strong uniqueness in fingerprints by saying an analysis of several print patterns must be made including, "patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns" (Jain et al. 2012:855). By doing this, he neglects the fact that fingerprints are not inherently unique as Cole (2002) and Lynch et al. (2008) heavily discuss. By looking at Apple's definition of unique with Touch ID for example, a 1 in 50,000 fail-rate rate when compared to a city like London of 8 million people would mean that 160 people would be considered as having the same print and could possibly access the same iPhone. Of course forensic work is under different conditions, but by Jain et al. simply mentioning uniqueness makes the analysis problematic.

4.2 Expectations

Moreover, it is not just security and accuracy which pose a problem with biometrics, but also the actual studying of the technology in a sociological perspective has been difficult and lacking. The thing about biometrics is that "biometric systems are often spoken about, but rarely experienced" (Martin 2011:24), at least in the past this has been true. They have been confined mostly to government institutions in border security, visa applications and in law through crime scene investigation. In normal day-to-day society, they have been dramatically limited (at least up until the release of the iPhone 5S) and even noted as 'invisible' technologies by Martin. It is then of no surprise that in the field of biometrics, "the empirically based social science literature is especially bare" (Martin 2011:24) as the institutions which actually have biometrics, provide limited access opportunities for study. This limited access further asserts the negative identity discourses of biometric verification mapped out by van der Ploeg (2003) as will be discussed later in this section.

In light of attempting to study these technologies, Martin strongly uses the sociology of expectations in his 2011 dissertation entitled, "Envisioning Technology through Discourse: A case study of biometrics in the National Identity Scheme in the United Kingdom" as it makes the study of such an 'invisible' or 'imagined' technology possible. The study is one of the closest pieces of literature to this thesis and thus will be used largely as a scope for analysis and comparison. The studies aim "is to explore *how* the UK government portrayed the role of multiple biometrics in its proposals for a national identity system" (Martin 2011:15). Two comparisons can immediately be made between Martin's study and this thesis. While he looks at the UK governments portrayal of a national identity

card with biometrics, this thesis looks into the media's portrayal of Apple's latest iPhone 5S and how such a private company is positioned at growing the biometric industry as opposed to government. Although in Martin's case the national identity system eventually failed and was never released, compared to Touch ID in the iPhone 5S actually being released, due to the timeline of this thesis, empirical analysis of user use of Touch ID was difficult. Thus this thesis' analysis comes from the theoretical scope of expectations for future, more wide-spread adoption of the technology of not just Touch ID, but also other forms of biometric technology.

In terms of these expectations, although based on biotechnology rather than biometrics, Brown and Michael's (2003) paper provides strong insight into the 'sociology of expectations' as they look at how the future of biotechnology was represented in the past, to get a clearer idea of what the future will look like. By using this literature a better understanding of biometrics' future is understood to see how changes have been made in the past, towards what the present state is like and how the media have predicted this. Chapter seven details this further in a theoretical sense but it is interesting to try and analyse where biometrics currently stand to predict the path of its expectations. In the Gartner Hype Cycle shown in chapter seven, figure 4, for example, Hyperion Consultant David Birch, placed it around the 'slope of enlightenment' with much optimism for the future of the technology, which seems rather telling of someone highly in favour of biometrics (Biometrics Institute 2013). However as Borup et al. (2006) critiques in another 'sociology of expectations' paper, all of this is quite arbitrary and difficult to conclude and that the hype cycle "fails to account for the way artefacts or technologies actually change over time in a continual and practical process of reconfiguring and being reconfigured in use" (2006:292).

In terms of past studies an interesting paper from (1994b) by Simone Davies, shows the hype and expectations of biometrics two decades ago with the title, "Touching Big Brother: How Biometric Technology will Fuse Flesh and Machine". It came at a time when preliminary biometrics were beginning to be used in customs and government situations, and where there was a lot of hype about national biometric identity schemes by many countries. In comparison to Martin's (2011) dissertation it is interesting to see how all these schemes haven't lead up to their hype and have failed to catch on.

Further, to contrast with Lynch et al. (2008), Davies mentions that in recent years (in the context of 1994), "biometric technology has attained a very high degree of sophistication, and accuracy has been achieved at a level which far surpasses all other forms of identification" (1994b:39). Even though this accuracy has been further disputed in recent times, it's interesting how he notes at the time that it surpassed all other forms of identification in regards to this accuracy including the

password. Because, although the 'password' has its many issues of convenience and security, it is still nevertheless accurate to within, dare it be said, perfection, as long as it is remembered correctly of course.

Moreover, what is most interesting is to directly analyse this article, and a newspaper report (Davies 1994a) he did for *the Independent*. With the title, "Computing: Forget the passport, let's see your hand: Biometric identification is putting an end to the long immigration queue" one can instantly see the difference in hype between his article with the fear of Big Brother, and the excited nature of his media report of a fast easy way through the queue in an airport.

However on top of these shortcomings, he does mention many issues still plaguing biometrics today such as how he notes the criminality stigma with classification systems in his article. Overall his article does provide a good analysis of advantages and disadvantages of the system but he concludes somewhat torn, noting that "biometry...is a natural extension of technological evolution" (1993b:46), but also that it needs to conform to standards and expectations of a privacy minded society. In that note, he foreshadows some of Ploeg's research onto the role of privacy and notes that standardization has a lot to do with how well the biometric system can be for it to be adopted by society. If Apple's Touch ID is to go by as a standard, perhaps day-to-day biometrics will continue to increase, but what of our privacy?

4.3 Privacy, Identity & Surveillance

To return to Martin's (2011) dissertation, he shows strongly the effect of media articles on projecting fears of surveillance and loss of privacy and eventually a big factor in the lack of user acceptance to the national ID scheme. He looks at an array of policy and media debates similar of which will be undertaken in this thesis in which he talks of many headlines framed around these privacy and surveillance issues, such as the UK being labelled as a 'surveillance society'. He notes that through the media debates, there was confusion at times between what exact technologies and policies were being talked about, and overall he notes a dystopian style hype framed by the media about losing privacy in terms of collecting the biometric signatures from millions around the UK and storing them onto personalized ID cards.

This can be compared to the articles which swirled around following the release of the iPhone 5S of a rumour about Apple giving the NSA access to the fingerprint database (Arthur 2013) and the subsequent privacy concerns. Although the rumour was debunked in a lot of articles as being satire, with many reasons explaining the absurdness of it, it did highlight the privacy debate prominently. The role of the media, although attempting to provide news and truth, also naturally has a means to entertain and to sell newspapers. In the empirical chapter, headlines of news articles will be

analysed with more scrutiny, but briefly, the position of this thesis is that the media creates hype and fear, regardless of how truthful their article may be. Just having 'fingerprint database' and 'NSA' in one headline can spark concern regardless of what else is said and therefore in this sense there seems to be a dystopian, privacy concerned framework presented in the article.

To continue with the privacy debate, at present only a few studies discuss the issue from this point of view sociologically (see Ploeg 2003; 2005), but they are somewhat outdated in regards to the fast paced evolution of social media, smartphones and tablets over the past few years. The mobile has been seen as the vector for mass-market verification systems, as well as many other systems due to the availability and convenience of a large proportion of the population having a smartphone with them. So although Ploeg's articles pre-date the smartphone boom, they do provide some interesting insight which not only embodies privacy issues, but dive further into ethical issues of how one's identity shifts and how one is categorized.

Ploeg is by far the key actor in the social sciences in regards to biometric technology, and as the crucial aspect of this project is to study how the media has framed biometric technology it is crucial to see more theoretically how the technology effects privacy and classification issues in regards to its implementation. In light of this, Ploeg argues that:

> *"In order to make sense of the normative and socio-political implications of this phenomenon [body-data], we may need to let go of the idea that this merely concerns the collection of yet another type of personal information... We may need to consider how the translation of (aspects of) our physical existence into digital code and "information," and the new uses of bodies this subsequently allows, amounts to a change on the level of ontology, instead of merely that of representation" (2003:58-59).*

Thus, this project will attempt to use a similar approach in analysing how biometric use cannot be simply associated with a replacement of a password. Rather, by translating the means for verification from password to biometrics, one is simultaneously translating one's own identity and how it is represented and therefore how one is classified, categorized, and ordered in society. How the media project this issue whether by glancing over the fact or highlighting the importance of this translation will be further discussed in the empirical chapter.

Furthermore, as has been discussed, the history of biometrical data is surrounded by crime and social ordering of criminals as it was originally a means to keep prisoners in check and know when someone had committed a repeat offence. Ploeg (2005) details how biometrical data can be used for profiling individuals and how the use of "machine readable bodies" (2005:7) provide major ethical issues in regards to racial profiling and anticipatory surveillance in which 'innocent' individuals may be targeted and have to prove their innocence rather than basic laws of innocent until proven guilty.

Although much of this particular study focuses on the use of biometric by governments and largely in airports and visa institutions, the theoretical means by what it means to be classified is useful in analysing biometrics on a more individual scale.

Furthermore, Introna & Wood (2004) present a case on the political nature of surveillance systems and how programming nonhumans to target minority groups through facial recognition technology dramatically increased in the US following 9/11. They mention that a shift occurred between security and privacy following the terrible events, in that privacy was slowly diminished for security, for the greater good. The argument was that it was worth people giving up their civil liberties if it meant being safe. This shift, as they say, is hard to directly analyse because designs of fail-rates and the software in facial recognition systems are black-boxed to the public. Overall though, the paper highlights the strong political nature of biometrics in the loss of privacy for the individual. This politicization of biometrics brings to light Winner's (1980) idea of artefacts having politics. In biometrics, it being a political technology depends a lot on context and discourse. In this thesis' arguments for a shifting discourse, the empirical section discusses further whether biometrics can actually fully shift this criminality, classification discourse, in certain contexts, into a more casual setting.

Lastly, Cole's (2002) "Suspect Identities" is a great foreshadow of his (2008) book with Lynch et al. on the contentious history of fingerprint analysis in courtrooms, where in his 2002 book he uses history of fingerprint debates to have a stronger focus on individual identities. What is notable, and compares similarly to van der Ploeg's articles, is how Cole looks historically at the development of identity systems and the translation of the difference between a biological identity and a mental identity. That is, he discusses how the appearance of criminal and law-abiding citizens can both be the same, and that it is not a biological factor but rather an inherent mental factor which defines who we are. This refers to how humans discriminate on how 'the typical criminal' looks such as having scars and facial tattoos, whereas no science has been able to prove that physical appearance can prove a criminal mind. In this sense, he discusses the many challenges with how to truly identify someone when biology may not be enough. The way we are surveyed, identified, all effects our privacy, and therefore this reiterates the strong debate of biometric systems on how and if they can be reasonably adopted by the public with a focus on protected privacy, whilst trying to avoid the discourse of biometrics as criminal.

4.4 Media vs. Corporations & Marketers

As mentioned before there is a lack of scholarly, sociological articles in regards to biometrics as a day-to-day device, and not many on the iPhone 5S and its Touch ID, due strongly to the recentness of it from the context in which this thesis was produced. However, from a media perspective, there

is a strong temporality as they produce regular articles which scholarly studies can't really keep up with. Although this thesis will broaden its media approach later in the study, *Wired* for example is a dominant actor in the tech magazine industry as it keeps up with the evolution of biometrics and provides feedback on user adoption aside from just the awe and 'coolness' of the technology. However it is more opinion based and lacks the in depth research scholarly articles could provide. So although it provides answers to this project's questions, its theoretical basis is limited.

In terms of fairly recent studies, a couple of years ago a new company AOpix (2012) emerged and provided preliminary biometrics to be used by smartphones, something which had been much published by *Wired* among many other tech publications. Yet in its White Paper (AOpix 2012), it unsurprisingly lists an array of features and amazing revolutions and possibilities in its 'benefits' section, but neglects the many problems and fears associated with the new technology. This is no doubt due to the commercial nature of the company and the study being essentially just an advertisement for it. Thus its main focus is on the convenience aspects of the technology by seeing how users would prefer to use biometrics over the inconvenience of having to use a password.

Furthermore, another recent example is a study (Ponemon Institute LLC 2013) which surveyed consumers from three different countries, the UK, US, and Germany, in regards to their trust with institutions and passwords, their opinions on passwords, and thoughts on biometrics. The results of the study dictated that many people are sick of their passwords and the majority welcome biometrics as a solution and place their most trust in banking and government institutions. Although this study provides some interesting research which would be quite useful towards this project, its problems can be described twofold.

Firstly, the study's methodology is only quantitative in that it lists an array of questions with multiple choice style answers and uses statistics to analyse the most popular results. The problem here is that people must choose something and there is no voice of further reason in terms of exactly why they chose certain things. Why do they trust banks more? Why do they want biometrics? Again, some questions do allow for this, except that they only provide a possibility for simple answers such as 'convenience', 'ease of use' or 'enhanced security' yet don't allow people to further explain their decision.

Secondly, similarly to AOpix's (2012) White Paper, this study seems to have been compiled from a commercial interest standpoint as it is sponsored by a company with similar interests to AOpix, Nok Nok Labs Inc. They are also a fairly new company and in their own White Paper (Nok Nok Labs Inc. 2013) it can be seen that an uptake of consumers in biometric technology will be very beneficial for

their company. The final conclusion made by the report that most consumers support biometric authentication therefore adheres to their interests, so the report must be understood under this bias, though that is not to say that the overall results weren't fully accurate.

5. Research Questions and Hypothesis'

In a general sense, the aim of this thesis is to develop an understanding of how biometric technology is being discussed, and portrayed in a contemporary context, as well as to debate how the socio-technical issues of security, privacy and surveillance form a narrative on expectations for the future of biometric technology as a mass distributed day-to-day verification system. The understanding of how exactly the conversation around biometrics is taking place, what exactly is being debated about, and the predictions of social adoption as well as government enforcement in differing areas, is crucial in order to evaluate the positives, negatives, as well as neutral thoughts on this continually emerging technology.

More specifically, as has been chosen as the case study for this project, fingerprint verification technology is the main source of scrutiny to be judged upon in the context of the iPhone 5S' Touch ID. As will be further elaborated in the methodological section, media and video analysis have been chosen as methods for study, with a timeframe being used around the release and hacking of Touch ID in September 2013. In light of this, the following has been formulated as the main question for study:

> *How was the release and subsequent hacking of the iPhone 5S' Touch ID reported in the US and UK print[4] media?*

As this studies main question, it has been used because it acts as an umbrella for the general goal of this project by doing four different things which the sub-questions will eventually build upon. First of all it focuses on the media debates as the crucial aspect for analysis. Secondly, it shows that this project will focus on two different timelines, which will aim to illustrate how the debate may have changed in this time and what factors were involved. Thirdly, it presents a comparison between two prominent western countries, The United States and The United Kingdom, to understand if or how the debates on security and privacy differ depending on geopolitical contexts. Lastly, it serves as an umbrella question for the analysis of the video of Touch ID being hacked. This is because the media initially speculated at the announcement of Touch ID, about the question of its 'hackability', before the 'hacking' was further reported on when it actually happened and the video surfaced.

[4] The term 'print' is synonymous with newspaper and magazine productions; however I also refer to print in the sense of online news and websites. That is to say print in the context of this thesis refers to both physical and online written news sources.

5.1 The Role of the Media

To begin, the first aspect detailed from the main question is the crucial use of media debates. A prominent aspect of user adoption to emerging technologies can be largely framed by the role of the media and how it represents these technologies. However technologists, futurists, entrepreneurs, scientists and academics discuss biometrics, and in this case, Touch ID, the media generally play one of the largest roles in user/public information, influence and potentially adoption due in large to their mass distribution networks and readerships. The media are the voices that project the information from the above mentioned actors and eventually frame it into their own discourse, one for the 'layman' to understand, yet potentially hidden in verisimilitude.

Thus, when answering a general question of how Touch ID was reported on by the print media, this project will be looking at a range of discourses including but not limited too; positive, negative or neutral, hyperbolic or realistic, useless or necessary, and helpful or just a cool gadget. These discourses will be discussed through a later sub-question however first the role of expectations will be debated through the following question:

> *How do they [US & UK print media] discuss the expectations of biometrics as a day-to-day, casual verification system?*

Of course predicting the future is not an easy task. It is not exactly easy to know whether it is realistic or not that in five years everyone will be withdrawing money from an ATM with their fingerprint. One can only look at past trends to have an idea of future outcomes. Therefore it is 'expectations' that are crucial, and hence this project will be using the theoretical framework of the sociology of expectations using Borup. et al. (2006) for analysis.

To hypothesise on these expectations, it is key to look at past trends of fingerprint technology, and the social aspect of user adoption. This thesis argues for a co-production model as detailed by Jasanoff (2004) of technological advancement and production whereby a strong relationship between technological growth and social adoption are necessary for new technologies to thrive. In that sense, the hypothesis of this thesis is that the expectations will be high for usability and convenience, yet questioned largely on security and privacy issues. This is largely in light of the NSA controversy occurring only a few months before the iPhone 5S' release, and a large feeling of scepticism in terms of how privacy and security is managed by much of the world. This also relates to

the importance of 'the social' in technological production, as in if these issues are too strongly rejected by the public, then biometric technology cannot thrive[5].

5.2 Media Discourses

How do the different genres and discourses of publications affect these expectations?

The previous section showed more a general hypothesis on the coverage of the iPhone and expectations, but as the above sub-question notes, this thesis will also look into how different genres through different discourses have reported on Touch ID. It is important to understand discourse and its role in knowledge production, and in this case knowledge distribution as it marks a crucial aspect of this thesis. Leeuwen (2005) says of discourse that, "there can be and are several different ways of knowing – and hence also representing – the same 'object' of knowledge". Hence, the Touch ID can be represented in a variety of different ways, depending on the context of the publication, and each discourse tells a different story of expectations and will be worth studying.

So by answering the above sub-question, not only are different perspectives possible on the expectations of TouchID possible to study, but also the media landscape in general, in terms of the difference between content of different genres of print media. These genres will be further detailed in the methodology section, but for an example hypothesis, this thesis predicts that the coverage of Touch ID will be no different to general assumptions about the respective media outlets.

To give some examples, this thesis believes from preliminary scanning of certain headlines that; tech websites e.g. *The Register* and *ArsTechnica* will have more of a positive hyped viewpoint about the expectations of Touch ID and mass distributed newspapers such as *The Guardian* and *The Washington Post* will be more sceptical and critical of privacy concerns. Further questions that will be asked to help analyse the respective discourses of the different genres as well as certain expectations are:

> *What are the key words used in the respective articles and how do they differ? What sources are the articles using/quoting? Are they more opinion based? Are there pictures used? If so what do they look like?*

The methodological section provides a more detailed overview of how these questions will be answered, however this section will briefly provide hypothesis' to some of the answers, and deliberate on the reasons of such answers, and their overall meaning in the context of this thesis. In terms of key words, similar to what was mentioned earlier, the expectation is that more mass

[5] This is aside from in current institutions such as governments where this technology is enforced as opposed to voluntary, which is discussed further in chapter nine

produced broadsheet publications would refer to the words privacy and/or security issues strongly[6], whereas tech magazines may refer to more technical jargon. In that sense, it is also hypothesised that some of the pictures will be more technical in these publications such as an inside look at the technical aspects of the iPhone and/or TouchID with diagrams, as opposed to other mass produced publications that could have more general photos of just an iPhone and/or someone using it.

Lastly, the style of writing, being opinion based or source based is one of the more important discourses to analyze. The hypothesis is that the majority of the articles in the tech magazines are more opinion based due to the prior knowledge of the technical aspects. That is to say this hypothesis assumes that the authors in the tech genre publications are already somewhat experts in the field of fingerprint technology. In contrast, it is hypothesised that the mass publications use more sources and quotes from so called 'experts' to justify their claims and expectations, as these journalists are seen as more laypeople in the field. Though again further analysis will help refute or confirm these claims.

This asks a big question on the field of expertise and how knowledge is distributed. In an argument for the deficit model, one could say that how expertise is enacted on the public in this sense, could affect their choices on the technology and how and if they choose to adopt it. However, it must be reminded that this thesis argues for a co-production model, so although the idea of expertise as a form of distribution in this context is hypothesized, a further look into user comments in a later question will attempt to correspond to this top-down argument.

5.3 Two Timelines

> *Does the discourse change between the release of the iPhone and the subsequent hacking? If so, how?*

The two distinct timelines were chosen as they were at a time when TouchID was most prominently spoken about, as well as to see the differences in discourses uncovered as a result of the two periods, as mentioned in the above question. The question here is referring to whether there was already a lot of privacy and security debate going on in the articles on the 10th to 12th of September 2013, when the iPhone 5S was first announced, and/or whether the debate increased, stayed the same, or subsided after the subsequent hacking on the 22nd September 2013.

The hypothesis is that the discourse did change in these two time periods; however that it changed between a privacy dominated discourse into a security dominated one. The reasoning for the initial

[6] This doesn't just refer to the exact words, rather words that correspond to each theme. The exact way this will be done will be discussed in the methodological section.

privacy dominated discourse has been discussed as a result of the privacy awareness issues being prominent following the developing Edward Snowden PRISM scandal. The subsequent hacking is then, although quite relevant to the privacy debate, hypothesized to create more worries on the security discourse of biometrics, following the ease at which TouchID is shown to be hacked, and the seemingly lack of security in the device.

The two different timelines are also crucial as they may be able to reflect how quickly hype around a new technology can change after a certain incident. If it is analysed that the initial fears about the hacking was quite prominent, and the actually hacking was not very surprising, then an idea of how expectations are judged between the differing news articles will be evident. However, if there seems to be a big difference in the hacking in terms of fear and scepticism as opposed to hype in the initial release, then this will further show the dominant discourse and the problems with expectations.

5.4 Comparing Geopolitical Contexts

> *Are the issues of security and privacy debated differently by the US and UK media? If so, how?*

The way a society is governed, including the laws that its citizens must follow and its policies on a range of issues, differs drastically from country to country. When comparing two countries like the United States and The United Kingdom; their share of the English language, capitalism, economic prosperity and democratic values seem to join them together, but there are many factors where they differ drastically, not limited to their history, cultures, and geography.

Livingstone (2003) demonstrates strongly how time and place matter in science. How science conducted at different points in time, under different conditions throughout the world, can largely affect results. He notes an example of Darwinism being taken to both America's South, and New Zealand, and how different the results were due to the previous traditions and religions of each respective land. "In one place it supported racial ideology; in another it imperilled it" (Livingstone 2003:4).

In the modern context, Livingstone notes how time has collapsed space, to a point where the 'faraway' is now the 'nearby', notably referring to globalization of the 20th and 21st century, mass-production and of course the impact of the internet. In the context of this thesis, this idea of a shrunken world enhances the differences strongly between the UK and US. In a world where technology produced can be disseminated globally and easily, a product like the iPhone can find its hands into two different countries with very different ideas about its capabilities, and its issues involved.

Thus, the discourse and context that each country adheres too is crucial in trying to understand their differing perspectives on the different issues. In Olsson's (2007) paper on power and knowledge relations, he quotes Foucault as saying, "discourse is inextricably tied to its particular sociohistorical context and cannot be studied or understood if divorced from this context" (Olsson 2007, 222). It is this sociohistorical context that he speaks of which will be analyzed closely, as it is a strong position on how the media is portrayed in either country, and hence the discourse of each issue that is more strongly debated.

This is all quite general, but it is important as it establishes a pre-conceived idea about how the US and the UK deal with privacy and security issues differently, and hence becomes a source of hypothesis for this thesis to attempt to prove. By looking at a historical perspective, this thesis believes that the narrative of security is more strongly represented through a US discourse, and that privacy is represented more strongly through a UK discourse.

This hypothesis is evident through the United State's strong stance on immigration and complex border procedures with every person entering the US having to succumb already to a type of biometric classification through fingerprint scanning and facial recognition technology. Although privacy is of course very relevant in this context as well, the reasoning for such a stark system implemented throughout the US is dominantly because of security issues, especially in a post-9/11 world.

The UK then, this thesis believes, has more issues with privacy as has been already discussed in the state of the art where Martin (2011) notes in his dissertation about a dystopian style hype framed by the media about losing privacy in terms of collecting the biometric signatures from millions around the UK and storing them onto personalized ID cards. This is furthered by the fact they have one CCTV camera for every eleven citizens in the entire UK and are often labelled a 'surveillance society'.

It will be interesting to test this hypothesis in the analysis, however it must be noted that it doesn't necessarily prove one way or another whether either country is more focused on a certain issue, as this study mainly refers the media's role in how these debates are framed. It may be that as a reaction to public opinion and governmental policies, the media takes the opposite stance in either country when discussing the issues of the iPhone, such as the US being more privacy concerned and the UK more security concerned. But that has to wait to be seen in the analysis.

5.5 The Role of Video

How does the video of Touch ID being 'hacked' contribute and affect the privacy and security issues of biometric technology?

Before the iPhone 5S had been released there was already a lot of speculation about fingerprint identification technology. It had been already around for many years in other devices such as laptop computers, and used in companies to monitor when employees arrived and left work. In this time, ways to be able to create fake fingerprints by pulling a print from a glass or other object and attaching it to some kind of silicone had already been well established, and hence the possibility and the desire to 'hack' the iPhone 5S upon its release was perhaps unsurprising. Yet it still received a lot of media attention, and contributes largely to the debate of privacy and security.

As will be detailed further in the methodological section, this thesis will not only analyze the different articles and the discourse they apply about the release of the video, but it will actually analyze the video itself. Due to the visual data, a hypothesis for the impact of said video on the privacy and security debate is that it had a strong negative impact on the uptake of Touch ID. From a brief viewing of the film, it was seen that it showed the iPhone was 'hacked' quite easily, and hence the ease, makes it seem that the security flaws in biometrics are great, as well as the privacy impact of someone being able to snare ones biometric data. A further hypothesis will be discussed in the methodological section as well as the actual empirical analysis in chapter eight.

5.6 Role of the public

> *From a public perspective, how have comments to the articles reflected their positions towards the articles? Are they in agreement or are they sceptical? Are they in favour of Touch ID or worried about security and/or privacy, or both?*

To continue along the line of expectations of future technology, this thesis' perspective has argued that the public are crucial in making technology mainstream through the co-production between both the technical and the social. Thus incorporating a question on the public's reaction to some of the articles is necessary to gain an overall perspective of how the debate has been framed.

What is interesting about this perspective is that the commenter's are not random, but rather they are people actively participating in the community of each respective online publication. What must be noted in answering this question however is that not all commenter's have actually read the article, and many may have just read the headline, as noted by Manjoo (2013). Therefore care will be taken in the eventual analysis of the comments to try and qualitatively analyse which comments were used in which context i.e. only headline readers, or readers with a sense of the entire article.

The hypothesis for these questions are context specific, as in this thesis postulates that although many people may in fact read the whole article, that user comments will engage strongly with the headline and the first few paragraphs of the article. It is hard to hypothesize on each article's

comment section that will be analyzed individually, but again in a context sense it will probably align with similar results as to which country the media outlet originates, as well as to the type of publication and tone of the article.

5.7 Compulsory vs. Voluntary

> *What reference, if any, do the articles give to current biometric technology already in use in government and other settings? How do they frame the difference between compulsory biometrics used by governments, and voluntary ones like the iPhone 5S?*

As has been alluded to before, there is a distinct difference around the issues of both privacy and security, between forcing a person to enter their biometric details, and asking them to do it voluntarily. Perhaps this is an issue that gets lost in the debate, and therefore an interesting issue worth looking into. When people discuss Touch ID and all its concerns, are they discussing fear of a public company like Apple gaining access to their fingerprint data, to perhaps sell to advertisers, or are they more worried about the government having access to it?

This debate is interesting as there may be many people who already have their biometric data on file in for example, the USA, if they have travelled there, because of US laws and foreigners needing to give their fingerprints to get visas. Yet the debate seems to be a lot stronger as Apple has done it[7], or maybe because the iPhone is a very mainstream mobile device used throughout the world, and therefore comes under a lot of scrutiny.

In any case, what these sub-questions ask is whether the articles are purely about Apple's TouchID, or whether they also talk about past, present and future expectations of biometric verification possibilities. The hypothesis is that most but not all will mention other biometric systems, and that if government systems are mentioned, they will be mentioned with more positive than a negative vibe. That is to say if Touch ID is compared with fingerprinting people applying for visa's, then the prediction is that the discourse on the government technology will be that of more secure and privacy conscious, though this will also depend on the different geopolitical contexts, and the different discourses of publications.

[7] It isn't as simple as Apple having access to someone's biometric data because the data is strongly encrypted within each device separately and the hacking has only been possible thus far by physically taking someone's fingerprint, rather than hacking a database of prints online – which Apple says is impossible

6. Materials and Methods:

The methodology to be used for this thesis was chosen largely for contextual reasons, as due to the recent timeframe of the case which will be undertaken, a media and visual analysis seemed most accessible. An initial idea was to conduct a series of interviews as well as a focus group to analyse user expectation to how the biometric fingerprint reader in the iPhone 5S may play to a person's security and/or privacy hopes and fears. However, it was seen as too problematic in finding a correct sample of people to analyse. The iPhone 5S was not that widely used at the time by people in relation to the location of this project (likely due to both the recent nature of the release as well as the expansion of Samsung among other smartphone giants). It was also difficult to choose which individuals to comment about the phone, as it was hard to define a specific context of sampling. As Riffe et al. notes, 'convenience sampling' is used when content is easily accessible and can be used "when little is known about a research topic" (2005:100). Little was known about user experience with Touch ID due to the recency of the technology, thus the project shifted from this difficult method of sampling for this project, to this convenience sample methodology of media analysis and video analysis, as these were more easily accessible.

However, just because video and media articles were easily available doesn't mean that sampling was not still necessary. Hundred of articles were generated across the internet in response to the iPhone 5S' release, so therefore a distinct time frame as well as specific news sources needed to be decided upon. Online Newspaper and tech websites were chosen as key media analysis as they enabled the most recent opportunity to discuss the iPhone on both the day that it was released, as well as the day 'Touch ID' was hacked. Nine US and nine UK online & distributed news publications were chosen with most having articles from both respective dates in order to see how the conversation changed from potential hype of the biometric reader, to the aftermath of the subsequent hacking. The US news sites chosen include The Wall Street Journal (WSJ), The Washington Post (WP), Ars Technica (AT) & CNET and the UK news sites are The Guardian, The Daily Telegraph, V3 and The Register.

Initially the methodology considered for this project was to seek only one newspaper from each country to do a direct cross-country analysis, and from each respective newspaper, gather an array of article about the iPhone 5S and the 'Touch ID' capabilities. However through further research it was seen that there was a lack of subsequent reporting about Touch ID in particular in the following months, and therefore it was decided to focus specifically on the two time frames. To then allow for

enough data analysis, an array of different sources from both the UK and US perspective were chosen to draw an analysis of how each produced their expectations, and what the prominent issues in each were.

In the US perspective a variety of news sources were chosen to see how agendas and policies differed from each context. The WSJ for example, generally has a business and economics emphasis on their articles, The Washington Post generally has a national political perspective emphasis, and the other two are more focused on technology news. Therefore by analysing the articles from their relevant perspectives, it will become clear how each performs news, and how each projects their opinions on the future of biometric technology and the issues involved.

In the UK perspective, a similar variety was chosen through both the different themes of the newspapers and political preference. Two tech news sources, V3 and The Register are included to see whether their tech-style hype is similar to their US counterparts. The Guardian and The Daily Telegraph are general circulation newspapers, but differ in political nature with the former favouring liberal with the latter being more conservative. This difference will be analysed to see how security and privacy issues are differently discussed.

In terms of techniques, a combination of content analysis, sources, and background agendas and contexts of each site will be analysed. The content will be analysed in both a qualitative and quantitative way as well as through manual and digital methods. Qualitatively, a close reading of each text will be undertaken, taking into account title, by-line, and some of the key emphasis' the article places on in regards to issues in privacy and security and to analyse what extent there is elements of excitement, fear and/or both. Quantitatively, although 18 articles is not a huge number of sources to analyse, nevertheless a key word analysis will be undertaken to compliment the qualitative reading for all of the text in the articles using Wordl software. Individual articles will be analysed to see what words are more prominent and what sort of differences are seen in terms of the context of each publication. After extracting the text into DMI (2015) software, the repeated words such as; the, at, and etc. will be taken out to leave a visual representation of the most talked about subject in regards to the case. This will show interestingly what ranks higher for example in terms of privacy and security among other issues.

In terms of the linking styles and sources used, this analysis was originally going to be done both manually (in a more qualitative sense) and digitally (in a quantitative sense) to double-check results, however the digital analysis was not successful, due to ironically both the lack of links in the texts, yet mass amount of links outside the texts. That is to say, the actually articles did not contain many

links but the website contained many unimportant links which made analysis quite difficult this way. Specifically, the goal of using such analysis was to see what sort of agenda each site has, and where their content and sources comes from. In the end a more manual approach was done by noting where each article was getting their quotes from, as well as the sources that they were paraphrasing. Due to the keywords used to search for the articles initially, there may be some bias in terms of links pointing to Chaos Computing Club's (CCC) website as a major source as well as Apple due to it being the main focus of each of the articles; however this will be addressed in the empirical section.

Special attention will also be placed on the visuals and style of presentation used in each article to see what aspects are highlighted. An analysis of the type of visuals shown in each article will be highlighted, in terms of what discourse is being projected, such as whether more attention is placed on the technical side looking at the Touch ID, or whether it shows people using the tool, whether it is a photo or drawing, and overall what each of these visuals mean to the overall article.

Furthermore, the comment sections of the articles will also be analysed using the same techniques to gather a user perspective, which was originally intended, to see how they react to certain issues explained in the article. One specific article will be chosen from each country, both based on CCC's hack; one from *ArsTechnica* and one from *The Register*, to conduct this analysis, and this will be done through keyword analysis using DMI tools and qualitative content analysis of a select number of comments.

The other data source that will be used for analysis will be a 3 minute and 33 second video of CCC demonstrating how they were able to lift a fingerprint from a phone and create a dummy print to use to access the iPhone 5S. The video is available to access on YouTube as well as embedded within an ArsTechnica article which discusses the implications of the hack, as well as containing a written interview with the chief hacker of CCC, a man named Starbug. The article will of course be analysed as well, as mentioned above, but a combination of how the video relates to what Starbug explains in his interview will be a source of further knowledge when analysed together. The next part will discuss this joint methods analysis.

The video contains no spoken words in it, and therefore there will be no need to transcribe it in the specific sense, however it does contain subtitles explaining each step of the process such as, "scanning fingerprint from display". The key analysis therefore of this video will be in terms of how different artefacts are utilized in the creation of knowledge, and how this affects the representation of Touch ID as a secure and privacy conscious tool. In video analysis, one can repeatedly and

succinctly analyse the most minor of details, and therefore in analysis, as Heath & Hindmarsh note how certain artefacts become relevant in certain situations (2002). Specifically this project will look at how the computer, phone, printer, photocopier, tweezers, glue etc. are used together, and how they are used by Starbug in creating a perspective of the hack. Further, Hindmarsh and Head note that "we need to examine the ways in which objects, artefacts and the like come to gain their particular significance at specific moments within courses of action" (2002:29). So the timing of each artefact being used and what action is occurring is important such as when he is photocopying the fingerprint or scraping the print sample off with a small scalpel.

A hypothesis, from a short previous analysis of the video, is that each artefact injects a particular discourse of the process of experimentation, and depending on how the text is read, evokes both curiosity and fear among other emotions. As Pink says "different people interpret the same footage differently, giving their own meanings to its content" (2001:111). Thus the video will be analysed in three different discourses; of a scientific experiment, of a black hat hacker illegally stealing someone's identity, and of an everyday person attempting the experiment for leisure, in order to see what are the major issues evident, and therefore what expectations there are of biometrics becoming a mainstream verification tool and future of the password.

The two main issues in which this thesis covers is the issues of biometrics in terms of security and privacy, both of which will serve as perspectives to see from whilst the video is being analysed. Thus not only will the artefacts seen throughout the video will be analysed, but also the surrounding background, the lighting, and the mise-en-scène overall. These visuals will be compared to the subtitles occurring to see how they complement one another, and to show how easy the hack is, the technique used, and the prospect of others replicating it.

Lastly, the combination of using video analysis and media analysis is useful to this project as it gives two different perspectives of source to criticize. The media articles are in the written form and therefore have time to be edited and presented in the best possible context for the publication. The video is also edited, however the results are more immediate, and the visuals enable a firsthand experience of what the media articles are talking about.

As the media articles describe the process, this can be cross-referenced with exactly how CCC completes the process in their video. This is also the case with the ArsTechnica article that contains both the video and a written Q&A interview with Starbug which can easily be analysed together to see whether what he says differs to what he does in the video. Also, the ease at which they achieve

this hack, the possibility for it to be replicated, and the overall expertise required can succinctly be analysed in comparison with the media articles to achieve the overall result.

By analysing both together, the aim is that they will be able to map out how the topic of the Touch ID has been discussed in regards to both its security and privacy issues. In comparison with a user perspective from the comments, a hypothesis on the expectations of biometrics as a future day-to-day verification system can be postulated. Further, the cross-country comparison as well as cross newspaper themed publication comparison will show how each of these report on the expectations of biometrics and how their different agendas, and geopolitical contexts differ and/or concur in perspectives.

7. Theorizing and Sensitizing Concepts

The theoretical basis for this thesis can be summarized through three ideas. The first theoretical framework is the sociology of expectations of how and if biometrics will flourish into a mainstream day-to-day system, replacing the password in many aspects of verification procedures. Through (Borup et al. 2006) this thesis looks at how the hype as accentuated by print media sources, could possibly predict the expectations of biometrics, using also the Gartner consultancy's 'Hype Cycle' (see Figure 3). This framework is strongly linked with the second theoretical basis for this thesis which looks at Jasanoff's (2004) co-production in a framework of Actor-Network-Theory (ANT). Arguing against technological determinism and social constructivism, this thesis projects the idea that expectations coming to fruition in biometrics is only through a combination of technology, nature, the social, human and non-human adapting together with one affecting and producing the other. The third framework which ties the expectations together is discourse analysis, in terms of whether the biometric discourse can extend itself from its original criminality notion to a more casual day-to-day basis, and how this changing discourse in a network of social and technological systems will help shed light on the future applications of biometrics

7.1 Sociology of Expectations

Predicting the future is no easy task, but by analyzing historical and economic trends, future and innovation studies, expectations become the glasses through which the future is seen and becomes a guide for predicting future scientific and technological trends. Even more so, ontologically, expectations actually self-reflexively create trends by being themselves predictive in the first place. As Borup et al. notes, "Expectations are both the cause and consequence of material scientific and technological activity" (2006:286). When expectations are created, this then fosters interest and investment to help boost the chance of the expectations coming to fruition.

One main source of expectations is science fiction, which has long been the basis for which future real-life innovations eventually transpire. It helps put imagined technologies in social settings, and forms a predictive story of how society adapts to these technologies. David Kirby (2010) calls such depictions of these technological expectations in science fiction, 'diegetic prototypes'. He argues that the social actions of film-makers create 'pre-product placements' from the diegetic prototypes and help generate real-world funding for technologies. Science fiction thus helps turn invisible technologies, visible, by projecting expectations into the public sphere.

However, the way that these technologies are presented in science fiction, can affect how they are perceived by society and be expected to function in real-life. This is how 'the social' becomes crucial in technological expectations. In the film *Minority Report* for example, biometrics like eye-scanners are shown very accurately to access computers, ignoring real-life fail rates which in many industries like banking or prison systems become serious issues. Projecting falsifying expectations of how the technology may well work in real-life can, in turn, affect how society envisions the technology and allows it to be further developed. But at the same time, by providing a source for testing the technology in a social setting, technological entrepreneurs, governments, and corporations can use these diegetic prototypes to create new products regardless. What is crucial then, as this thesis argues, is not just if the product is created, but how the public reacts, which as a result expands the product to become mainstream. This idea will further be developed in the next section on co-production and ANT.

A big factor of this then is not just science fiction, but also the media, which acts strongly in projecting technological revolutions and hyping or rejecting 'expected' technologies to the public. *The Economist* (2002) for example reacted to *Minority Report* with an article largely about the ineffectiveness of biometrics due to its fail rate. *EHS* (2004) had a more hyped view, even saying that "the technology [in real life] is advancing so fast, some parts of *Minority Report* may soon look outdated" (Brown 2004:para4). Both of these articles are from over a decade ago and biometrics have expanded a lot since then, but for some media articles in recent times, although the technology is constantly improving, skepticism has not necessarily changed, which the next chapter will discuss in detail.

Biometrics in a sociology of expectation framework then, is different to other future technologies, or what Kirby (2010) calls 'speculative scenarios', because it is already here. What is different is how it will continue to develop. Cynthia Selin's (2007) paper for example, looks at the expectations of nanotechnology by noting how the different actors involved like politicians and scientists with different agendas create a narrative on the emergence and possible future aspects of nanotechnology. Nanotechnology, like biometrics is already here, yet its potential applications are still considered quite speculative by many, especially Eric Drexler and his, as many scientists think, dystopian science fiction vision of nanotechnology.

In Selin's (2007) paper, she concludes that expectations and future claims are very important in solidifying a technology, "speculative claims, as ordinary claims, are powerful constructions that create legitimacy in a technological domain" (2007:214). However, she argues strongly for the relationship between actors and their agendas, in how they translate an expected technology into

reality. By analyzing the nanotechnology narrative, with Drexlererian visions, Selin uses ANT to concur with Latourian ideas that translation between actors is crucial in turning visions to reality such as she notes that "a successful translation involves enrolling other people to your interests" (2007:208).

How these interests' peak and trough in an expectation cycle is noted by the Gartner consultancy's 'Hype Cycle' (see Figure 4). The idea is that new technologies have a way of cycling between hype and disappointment. As Borup et al. (2006) point out; this model is quite reductionist as it is too general, too linear and doesn't take into account the different discourses a technology may be represented in. That is to say, in one aspect a technology may have succeeded, but another it may be considered a failure.

In the expectations of biometrics, through its history in a criminality discourse, as chapter two detailed, it rose largely to fame during the early 20th century as a solid use for identification. By the 1990's one could argue that there was much disillusionment as fingerprint evidence began to be questioned a lot more (see Cole 2002; Lynch et al. 2008), yet it still remains of dominate use in court rooms. Though, in a different discourse of computer verification such as scanning ones finger to access a computer, the expectations seemed to start later in the mid-to-late 20th century when science fiction began using biometrics as an ease of access, yet early attempts at putting them into laptops failed as the technology didn't seem ready.

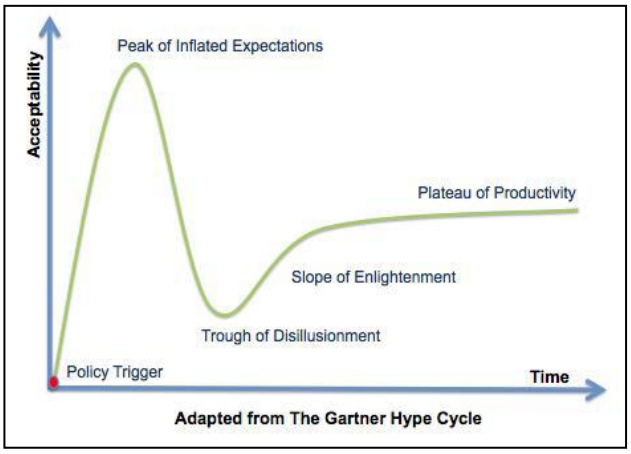


Figure 4: Gartner consultancy's 'Hype Cycle' ***Source: (Borup et al. 2006)***

This is but an example of how to use the hype cycle, and although this thesis agrees with Borup et al. about its being too linear, it still serves as a good broad example to try and explain the role of expectations. Hype and disappointment is certainly part of the journey for a technology, and in returning to Selin's point on how translation helps to enrol interests; hype and disappointment in this cycle, is largely generated by how these interests, from different actors, both create hype and disappointment.

7.2 Actor-Network-Theory

Expectations need to be analyzed away from the realms of technological determinism in which they often are at the start of a hyped technology as Borup et al. note, "early technological expectations are in many cases technologically deterministic, downplaying the many organizational and cultural

factors on which a technology's future may depend" (2006:290). Further than this though, as ANT illustrates, it is not just social and cultural factors that influence how technologies come from expectation to reality, but rather all possible actors and networks, human and non-human, social and natural which not only affect the expectations, but work together simultaneously in heterogeneous networks. This is the essence of ANT.

ANT is of great importance in the field of STS and as with social categorization, ANT is largely about, reducing all actors from their dominant discourse, to their socio-technical forms and viewing how they interact in this regard in different networks (see Latour 1988 and Law 1992). Crucially what makes ANT different to social order theory is that in ANT the social is not simply the driver of networks, but rather humans and non-humans co-produce and co-opt together, "order is an effect generated by heterogeneous means" (Law 1992:3).

Through this theoretical framework, biometrics cannot be fully understood and studied without then reducing each actor to their basic discourses. For biometric technology, this is a large network of actors including the devices being used to access the biometric data, the users using it, the place that stores the data, the different institutions that implement the technology, the actual fingerprints and DNA of oneself, the general public's opinions, the government's role, corporation's role, economic actors, media influence and many others actors networking with one another in the process of implementing the new technology. As chapter six outlined, the focus of this thesis will be the media's role as an actor, and to see how the media translates knowledge from the biometric communities between other networks, yet in ANT this means taking into account how all the other actors network together.

This creates a chicken and egg scenario whereby each actor is just as influential as the other. As Law (1992) notes, in ANT, the macro and micro can be analysed through equal power, "in effect, we should analyse the great in exactly the same way that we would anyone else". But that is only by reducing each actor to their smallest parts. Without the infrastructure of devices capable of reading ones fingerprint, how does the process of fingerprint verification get distributed? At the same time, how do corporations, governments and policy makers debate the uses of biometrics in a social setting, without first having that infrastructure to disseminate it? Biometrics, as this thesis argues, is only now becoming better known in the public sphere due to the release of Touch ID, yet how it will continue to grow relies heavily on all of the actors and networks around it.

Sheila Jasanoff describes a similar notion to ANT in her idiom of co-production stating that, "the ways in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it" (2004:1). By looking at the historical discourse of biometrics as

chapter two detailed, on the one hand the innocent individual is liberated by biometrics as criminals and recidivists are made easier to identify and catch. But on the other hand, the innocent individual begins to lose their own civil liberties by being encouraged to give aspects of their personal makeup e.g. fingerprints, to government agencies for civilian background checks, for example, which leads to increasing the ordering and classification of society.

This returns to the debate of power relations in ANT. As has been argued, in order for biometrics to continue to become mainstream and used in casual, day-to-day actions, all the actors involved in biometrics need to co-produce together. To do this, we note through ANT that by reducing each aspect of power to the minimal; and mimic micro and macro power alike, the public has as much power in influencing the development of the technology as the government does. Further, the nonhumans have just as much power as the human as they become increasingly relevant in dictating their own technological growth; through, still of course, a co-production with other actors.

As Latour [Johnson] details in his (1988) essay, the human and nonhuman actor are blurring, and in many instances the nonhuman actor is taking over from human jobs as skills programmed by human actors, enter the nonhuman repertoire (see also Winner 1980; Latour 1992). Just as Latour dictates that a door and its hinges are more productive and efficient than a human actor as they aren't distracted or take lunch breaks as a human would, biometrics change the role of identity analysis from something intrinsically human, to trust in machines. In the past, police arrested recidivists using soft biometric recognition, whereas the reliance is now on the nonhuman to catch suspects, and use such analysis in court rooms to convict suspected criminals.

Thus one argument for the nonhuman is that it does not discriminate, it does not associate looks with guilt as many human actors would. As a policeman might become suspicious of a person due to their dress sense or face tattoo, a nonhuman biometric reader simply looks for what it is told. That however is the problem when we try and separate humans and nonhumans. ANT argues against this and as Law (1992) says, one doesn't necessarily drive the other. Biometric nonhuman readers do indeed discriminate as studies (Introna & Wood 2004) have shown as they are programmed by human actors, and in certain cases like facial recognition software, profiling is used to target minority groups. But although programmed by the human, the nonhuman has just as much power in utilizing its position to catch perpetrators. Each have equal power in this theoretical notion, each affect one another.

In looking at facial recognition, it is hard to argue such technology is not askew in politics, but what of fingerprint readers, which is the case study of this thesis. How can one program a fingerprint

reader to profile possible perpetrators? Again this politicization of the biometric reader returns to the discussion of the arguments of Lynch et al. (2008) and Cole's (2004) on how DNA and fingerprint evidence has been interpreted over the years. In the court it has to do with language used by experts on whether a 'match' is legitimate. The forensic expert, the lawyer, the software programmer, the actual software, the surface where both the latent and ink print were taken and so on, all share in the power to produce an identification. So as all the actors network together in producing knowledge, what becomes crucial in ANT is the process of translation.

To return to Selin's (2007) paper, the sociology of translation is as Latour (1987) notes, moving from a claim of interest, to eventual acceptance. In epistemology this could simplistically be a theory which becomes empirically tested multiple times over a period of time until it eventually becomes accepted by the scientific community. This process is known in ANT as *translation* and it occurs as actor's network and attempt to suit their needs, agendas and purposes. As Selin notes, "if the claim circulates…the claim begins to stick, actors are enrolled and translation occurs" (2007:208). In Selin's case, she uses it to see how the narrative on the expectations of nanotechnology has been translated. Callon presents a similar example in his (1986) paper on the dwindling supply of scallops in St. Brieuc Bay.

By arguing for a *generalized symmetry* between the natural and social worlds, that is a network of nonhuman and human actors including the fisherman, scientists, scallops and consumers, Callon compares the scallops as natural actors, with the fisherman and scientists as social actors and suggests that all must work in unison and support each other's needs to repopulate the supply. Callon concludes by saying how the actors were all previously separate entities with no communication or networking with one another until the supply was in jeopardy and the actors banded together, "a discourse of certainty has unified them, or rather, has brought them into a relationship with one another in an intelligible manner"(1986:223).

At the cusp, ANT shows how any object, person, entity or thing, can relate to others when context and relevance is analyzed. Different institutions and infrastructure, like transportation and agricultural chains, lose their relevance to people, until problems occur and all of the actors and networks become relevant and the intricacies of how each system functions become highly important. To clarify, Law suggests an example of this with a television, "when it breaks down…it rapidly turns into a network of electronic components and human interventions" (1992:4). Through ANT, biometrics can be understood at the same level. For example, simplistically having a biometric reader on ones phone, that always works, could be seen as just that. One scans their finger, one gets access to ones phone. The story ends. However when issues occur, such as ones identity being

hacked or stolen or the biometric reader not working, the relevance increases the analyses of the network and suddenly Touch ID turns into an array of socio-technical actors all working in unison. Thus, suddenly through relevance, the macrosocial and microsocial actors of a network can be analyzed through equal power relations, each having importance and affecting the other.

However, as Foucault notes on the concept of power, "there is no power relation without the correlative constitution of a field of knowledge" (Foucault 1979, 464). Through lacking the knowledge of how these actors and networks function, power remains dominant on the macro scale. Through Foucauldian theory, this knowledge however is socially constructed, and how such knowledge is produced from the historical background of biometrics, for example, is through discourse analysis. This third theoretical component will serve to tie ANT and sociological expectations together in discussing the future of biometrics.

7.3 Discourse Analysis

When studying discourse, semiotic researcher Theo van Leeuwen argues that discourse analysis should inextricably use the plural – *the plurality of discourses* - as no object is without the possibility to be seen and analyzed in different ways, through different discourses. Discourses are as he draws from Foucault, "Socially constructed knowledge's of some aspect of reality" (van Leeuwen 2005:94) and therefore through their social construction, different contexts and different ways of seeing create different discourses. This social construction of discourse has two functions as a theory to this thesis. It provides both a means for analyzing how, if, and why the discourse of biometrics has shifted from its historical routes from identification to verification, as well as being used semantically in the media and video analysis in the next chapter.

In terms of history, in Olsson's (2007) essay on Foucauldian discourse, chapter five mentioned Foucault's argument that "discourse cannot be separated from its sociohistorical context. Thus, as chapter two presented, through this theoretical understanding, biometrics cannot be studied or understood, without the sociohistorical context of criminality, which gave birth to modern biometrics. A question this thesis asks then is although understanding biometrics cannot be done without analyzing its context, can its discourse actually shift, or will biometrics always be surrounded by a criminality discourse? Can biometrics actually be a casual, day-to-day, simple verification procedure, away from criminal identification?

This issue returns to the sociology of expectations. How can we look at the future of discourse? Discourses inextricably co-exist, as there is always a different way of knowing and representing an object so the expectations of the future discourse may still lie in a historical standpoint. In terms of biometrics, the way it is continually used as a surveillance tool by governments reflects one

discourse that may well be now co-existing with a more casual discourse. But as the next chapter will analyze, media reports and user comments have remained skeptical about how biometrics can shed its surveillance rhetoric.

Furthermore, van der Ploeg (2003 & 2005), as mentioned in chapter four, brings further discussion to the discourse of biometrics in how the technology functions in relations between the human and non-human, and the privacy issues of shifting identity, and how the machine-readable body acts as a 'truth' teller, and distinguisher between the criminal and innocent. As she mentions for example, the digitization of fingerprints into massive databases in the US and Europe has for example, shifted the discourse of how suspects are apprehended. As opposed to finding a suspect first and seeing if their fingerprints 'match' a crime scene, now, suspects are found *after* first searching a database of millions of fingerprints (van Ploeg 2003). Where before, the human discriminated against and profiled the suspects, now, this is done by the nonhuman.

Not only then does biometrics shift discourse from human to non-human identifiers in forensics, but the process of access and verification in other applications is also shifted from the personal, in the mind verification such as passwords, to something physical, displayed on the body for all to see. In these casual day-to-day settings such as monetary transactions, biometrics has to an extent, taken a full circle. In the form of soft biometrics, signatures used to be, and in many cases especially in the US still are, used to pay for goods and services. The idea was always about uniqueness, that one had unique handwriting and a signature which was hard to forge. PIN's have largely replaced that due to the lack of signature checking, but PIN's can also be forgotten, so services like Apple Pay through the use of Touch ID has joined the expectations, of bringing biometrics back in monetary transactions, this time hard biometrics.

Again, this changing to the way we pay, can, in the Foucauldian sense, be linked to a sociohistorical context. One could argue that the way people pay for things is both generational and cultural. As PIN's are standard for the young, signatures have been a long time user for the old. Perhaps biometrics as a payment procedure requires the same thing; a shift in culture and a shift in generation.

However, discourse changes are not as clear cut, and this thesis argues that 'the social' is not enough to mark this shift and therefore ANT is used as the dominant examiner. Foucault does in fact link discourse with ANT, by noting that discourse in terms of a text for example, can only be understood through analyzing the relationship between all the actors and networks; the ideas, the institutions, the semiotic structure of the text, the author, the text itself and so on. And how only through

analyzing these together, can a discourse be understood. So in the example of payments, it is not only important to analyze the culture and generational shifts in discourse, but also the actual technological infrastructure, and the institutions like governments and banks which bring 'forced technologies' or 'forced participation' on the public.

Nortje Marres (2011) makes reference to this idea in discussing how certain material objects seek to increase public participation in environmental movements such as through 'smart meter's' counting energy usage or by using excel programs or other technologies to keep track of one's carbon footprint and therefore help reduce it. In these instances, she discusses how material objects help to encourage engagement, which in turn can relate to how banks began encouraging engagement in switching to PIN identification over signature. This encouragement for participation then eventually led to a 'forced participation' in many countries whereby the PIN became standardised. Are Apple and the banks encouraging participation in biometrics over PIN now? How do the other actors and networks respond? Chapter nine will further discuss this changing discourse.

Lastly, the semantic discourse analysis will be based not only on Foucaldian power/knowledge rhetoric's, but on how the texts are presented by the media, to note the discourse they are projecting, and how the syntax, word choices and tone, effect the expectations each outlet is projecting. Fairclough (2003) for example, notes three different ways discourses are projected through texts; by ways of acting, representing and being. This multifunction of meaning that different texts project will be how the next chapter will approach textual discourse analysis. As Fairclough notes, this embodies looking at "the relationship of the text to the event, to the wider physical and social world, and to the persons involved in the event" (2003:27).

8. Empirical Work

As has been argued thus far in this thesis, biometric technology seems to be making an ever greater inroad into society. From its historical background, born from criminality, to its civil use for background checks, the question of present and future expectations of day-to-day casual applications of authentication and verification moving towards ubiquity has been created largely due to the development of the internet and the smartphone. From these discourses, and theoretical underpinnings on expectations, this chapter will now look closely at the specific case of Touch ID through UK and US print media and video analysis. The chapter has been divided into a summary of the major media articles under empirical analysis in a semi-descriptive, semi-analytical way, before further analysis in the following sections by relaying and attempting to answer the questions posed in chapter five in the order they were posed. This will then be followed by a video analysis embedded within one of the article. Both summary and theoretical analysis will be present throughout, with chapter nine then providing a scope for detailed comparative analysis of each article and question with one another, to attempt to answer the projects main question of how the US and UK print media reported about the release and subsequent hacking of Touch ID.

8.1 US Article Summary's

8.11 The Wall Street Journal

Yadron (Sept 9 2013) [WSJ1] and Yadron & Sherr (Sept 11 2013) [WSJ2] have made clear issues from the start of their respective articles. WSJ1 advocates the need for security, and questions whether Touch ID has solved this ever growing tech problem. WSJ2 is both about user privacy worries, on how data on Touch ID is actually stored, as well as how convenient the product actually is. The headline in WSJ1 states, 'Apples latest iPhone puts focus back on finger security'. The article clearly makes the point that passwords are increasingly problematic, even quoting past hacking of passwords and concerns with consumers trying to remember such long passwords. It is only at the end of the article where mention is made of possible security failures, but overall the hype developed is of a high, positive support for Touch ID, bringing a high sense of security and convenience

WSJ2 aggressively discusses privacy but seemingly in a positive light as it initially states that consumers shouldn't worry as fingerprints aren't stored, only encrypted data. It makes a passing mention on security and convenience, in regards to how fingerprint verification might actually work

if ones hand is 'sweaty', but overall doesn't provide much criticism towards Touch ID and rather just regurgitates points made by an Apple spokesman.

Marson (Sept 23 2013) [WSJ3] published after the hacking of Touch ID also discusses privacy and hints at more sinister possibilities of American government officials, in regards to the NSA hacking, taking Russian fingerprint identities, as postulated by Pro-Kremlin politician Vitaly Milonov stating, "There's no guarantee that fingerprints from the 5S won't end up in American security services' databases" (Marson 2013:para3).

8.12 Washington Post

Fung (Sept 10 2013) [WP1] clearly focuses on privacy in his piece calling Touch ID a 'gamechanger for privacy' in the headline. It poses problems of where and how Apple has designed the system to store the fingerprints, but that is because the article was written a few hours before the actual release. This caused a few users questioning the prematureness of the article. Nevertheless, it identified strongly the legal and government implications, questioning whether one could incriminate oneself through supplying ones biometric data, whereas a password in the mind is protected by the US Fifth Amendment right. It also questions privacy further about how 3rd parties could have access to the biometric data and the implications of this.

Peterson & Tsukayama (Sept 20 2013) [WP2] provide a better scope for analysis as it is written following the release of TouchID and hence has more information from Apple about the technical side of Touch ID. Nevertheless it still focuses on privacy issues like WP1, as well as security, through its headline, "Fingerprint scanner for iPhone 5s raises privacy, security concerns". It looks at how governments and companies responded to Touch ID suggesting that it may not be secure enough for such high-sensitive institutions. It mentions a letter by Sen. Al Franken to Apple about his concerns with what they will do with the fingerprint data saying, "…if hackers get a hold of your thumbprint, they could use it to identify and impersonate you for the rest of your life" (Peterson & Tsukayama Sept 20 2013:para7).

Furthermore, WP2 focuses on issues of law and how privacy can be maintained citing the US Communications Act and how police can currently issue a warrant to subpoena content data from corporations, and whether ones fingerprints would count as content data and be possibly supplied to authorities. The article concludes by noting that many companies would test Touch ID over a few months to check its security before allowing employees to use it, however at the very end it notes that in terms of security, Touch ID is still better than easily guessable passwords that employees tend to use. Overall the main thrust of the article is critical about how Touch ID can solve the issue of privacy and security and does it in the context of businesses as opposed to individuals.

8.15 Ars Technica

Goodin (Sept 11 2013) [AT1] outlines quite an unbiased viewpoint about both privacy and security of Touch ID, mainly due to the fact that no one had had a chance to try the fingerprint reader out by that point and therefore the exact functions of how it would work were unknown. The unbiased viewpoint comes as he clearly lists both pro's and con's about the fingerprint reader, listing first the pro's. This could be considered formal, as in the pros tend to precede the cons, but it still presents a positive viewpoint at the start of the article, which is what most people read, therefore it is skewed to a more positive hype.

In the pro section he speculates from Apple's technical description of Touch ID that it would not be prone to 'casual attacks'. Casual being the key term here, as it suggests there is more than one discourse of using biometrics and that in more secure situations, security may not be strong enough. Further he suggests that privacy would only be so secure, if what Apple claims is confirmed about the actual fingerprint data being encrypted. He does this by hinting about people's NSA fears saying that if it is securely encrypted, "Touch ID has been designed to store the information in a way that can't easily be accessed by malware, hackers, and possibly other adversaries such as three-letter government agencies " (Goodin Sept 11 2013:para5).

The con section examines the problems with the human body as a password, and how it is not easily changed if someone gets access to your biometric data. It also discusses, similarly to WP1 the legal implications of whether ones finger is protected from self-incrimination in having to access their phone, as their PIN number is. That is to say, authorities cannot 'force' you to reveal a password, but they could force you to use your finger for access. The con section concludes by looking at the detrimental aspects of a criminal being able to fool Touch ID and that, "The ability to pull a print off a stolen iPhone and use it to gain full access to the owner's device could spur a whole new wave of iPhone thefts." Though how this long process of hacking Touch ID can create more thefts than occur now when many people don't even use PIN's on their phone, or when they do they use simple passwords like 1234, makes this claim a little outlandish.

Goodin (Sept 24 2013) [AT2] not only provides a more concrete perspective on Touch ID because of the hands-on time people had had following TG1, but it also contains an actual interview with Starbug, CCC's main hacker. In revelations about how Starbug 'hacked' Touch ID, Starbug mentions that he doesn't believe fingerprints to be an effective form of verification, and that passwords are still very secure, as long as they are long enough, though he does mention the strong convenience issue with this. In discussing the sub-epidermal level the fingerprints are taken at, Starbug believes Apple, "chose usability and convenience over security" (Goodin Sept 24:2013:Para17), to ensure the

device worked a lot more often by not setting the sensors reading rate too deep within the skin. So overall the main argument presented in AT2 is that Touch ID has great convenience, but is not secure enough for more security conscious applications, as in the case with any biometrics, due to the fact that we carry our bodies and prints with us everywhere and therefore they are easily accessible for criminals to target.

8.16 CNET

Whittaker's (Sept 10 2013) [CNET1] is one of the most positive and hyped articles in this data set, reading almost as if it is written by an Apple employee. The headline teases the possibility of the replacement of the password by Touch ID and spends most of the first half of the article quoting Apple sources, and outlining Touch ID as the password killer, and being a deterrent for 'hackers' due to its high security – quite contradicting to other articles. CNET1 also mentions that Touch ID is safe from privacy issues due to Apple's 'secure enclave' data encryption. It does mention issues biometrics had in the past and how older laptops and older smartphones had biometrics but subsequently dropped the technology due to its unreliability. But it notes that Apple is hoping to change this, and concludes by arguing that even though passwords won't disappear overnight, "Apple has fired the starting pistol on what it sees as the future of security and online identity"(Whittaker Sept 10 2013:para23).

Following the hack, Musil (Sept 22 2013) [CNET2] presents an informative piece, with similar quotes from the other articles by Starbug about the ease of the 'hack', but what differs is the analysis of how genuine Starbug's arguments are. When Starbug mentions that he hopes the hack, "finally puts to rest the illusions people have about fingerprint biometrics," (Musil Sept 22 2013:para5), Musil calls it a 'blunt assessment' and notes that Touch ID is not meant to be a pure replacement for traditional passwords, especially as the passcode lock still comes into effect if the Touch ID sensor doesn't respond correctly.

8.2 UK Article Summary's

8.21 The Guardian

Campbell (Sept 11 2013) [TG1] uses scare tactics in an overhyped way of discussing security issues in Touch ID whereas Arthur (Sept 18 2013) [TG2] strongly focuses on convenience. TG1 is clearly written in an opinionated, entertaining aspect – being in the Guardians 'shortcut' section - strongly demonstrated by its click-bate title "iPhone 5S: would thieves really chop off your finger to access it?" The article continues by raising examples of criminality possibilities that Touch ID brings, and apart from a short point at the end saying that a victim would merely give up their password as

opposed to having their finger copped off, the majority of the article hypes the detrimental security possibilities.

TG2 details convenience by advocating problems with existing passwords, and questions the accuracy of Touch ID over previous biometrics used in computers. The piece does make a mention of NSA and privacy issues, but notes that these issues would probably not have been as important six months ago (before the Edward Snowden Incident), and overall supports a great convenience aspect for the product.

Arthur (Sept 23 2013) [TG3] then focuses on security and privacy issues following the hacking of Touch ID by CCC, shown by the focus of the security hacking and possibilities of ID thefts in the articles. TG3 is quite informative and describes the hacking directly and how the device may not be so secure, before supplying quotes by Apple, about how the device is still more secure than a PIN due to the 'match rate'. It also supplies an interesting quote by security specialist, Graham Cluely about casual security, "Relying on your fingerprints to secure a device may be okay for casual security – but you shouldn't depend upon it if you have sensitive data you wish to protect," (Arthur Sept 23 2013:para6). The article doesn't further develop an opinion on the quote, but it leads to some questions about casual biometrics and casual security which chapter eleven will further discuss.

8.22 The Daily Telegraph

Warman (10 Sept 2013) [TDT1] and Curtis (23 Sept 2013) [TDT2] show a clear difference in timelines before and after the hacking. In TDT1 no mention of security or privacy was made apart from saying that it is probably not designed for more advanced security features like online banking, and rather only more 'casual' features like accessing ones phone. Although the pieces are simply informative on the release of the iPhone, other articles on the release only roughly mention Touch ID and instead detail a lot of the iPhone's other new features. Overall TDT1 suggests Touch ID is more of a gimmick like Siri was for the iPhone 4S and that there are not many issues of concern with it.

In TDT2 however, much is made about the implications for security and privacy, with the article also describing CCC's hack. The headline, "iPhone 5S Fingerprint Sensor 'hacked' within days of launch" continues similarly to TG3 by describing how the hack occurred and quote's CCC on how 'stupid' biometrics is for security. At the conclusion of the article it does mention that no one has managed to take the actual fingerprint data from the phone, but rather they have only been able to access the phone through faking a latent fingerprint. This shows a defence in Touch ID's privacy, but this positive observation, being at the end of the piece loses the balance of the article. Being at the end clearly makes a big difference and remains common in these attempted 'two-sides of the debate'

articles because of the percentage of people who don't make it to the end, which the results section further evaluates. TDT2 also interestingly provides the same quote as TG3 by Graham Cluely about casual security vs. casual biometrics (see above), showing both articles have similar positions on how security and biometrics should be viewed.

8.23 V3

Bennet (Sept 10 2013) [V3-1] takes a business standpoint and immediately supports the security benefits of Touch ID as noted from the headline's use of the word 'safer', "Touch ID fingerprint scanner makes iPhone 5S a safer bet for businesses". The rest of the article is written in a very positive light, with no quotes from critics, rather only quoting Apple sources on the benefits of the technology. It further describes the ease of use, and the security from its sub-epidermal layer for verification and how the privacy aspect is very secure as it quotes Apple with no criticism or questioning, saying that, "All fingerprint information is encrypted and stored securely in the Secure Enclave inside the A7 chip on the iPhone 5s; it's never stored on Apple servers or backed up to iCloud," (Bennet Sept 10 2013:para4).

As a result of CCC's hack, Worth (23 Sept 2013) [V3-2] takes into account security issues with Touch ID and similarly to TDT2 and TG3, V3-2 is quite informative and outlines the process of the hack by CCC. It also uses the same quotes by CCC saying that fingerprints should never be used to secure anything. What differs strongly, yet subtly between the headlines of V3-2 and TDT2, is that TDT2 puts apostrophes around the word hack, "iPhone 5S fingerprint sensor 'hacked' within days of launch", whereas V3-2 emphasizes the more mainstream idea of hack being a bad thing, and emphasizing the fact that the team are 'hackers', ignoring the apostrophes, "hackers crack Apple iPhone TouchID Fingerprint Scanner". As discussed in chapter three on the politics of hacking, this headline pushes for more of a black-hat idea, and hence makes the 'hacking' sounds more detrimental to security.

8.23 The Register

Leyden (Sept 12 2013) [TR1] presents a position of trust in privacy, yet questions whether security is strong enough in Touch ID as the titles suggests, "iPhone 5S: Fanbois, your prints are safe from the NSA, claim infosec bods; But is it a decent authentication method? The jury's out..." Once again the NSA are discussed and the article mentions the absurdity of the fact that in past biometric readers on laptops, no one worried about Windows having our data, yet because of recent times with the NSA, the article claims people seem more sceptical, yet shouldn't be, as long as Apple's claim about its encrypted data is correct.

However, in terms of security, it mentions that problems with fingerprint systems are the reason many different data points are taken into account. Some measure just ridges, but as Leyden says, the good ones also measure heat, pulse and pores. It concludes by mentioning that being on a mobile, and a mainstream device, Apple has the chance to bring biometrics mainstream, yet it is still more a convenience factor presently. The article argues that the tech is just not sophisticated enough yet to combine strong security without compromising convenience and that perhaps another 10 years is needed before such mainstream biometrics in secure situations is possible.

In the following article discussing CCC's hack, Chirgwin (Sept 22 2013) [TR2] takes a different route in its headline from V3-2 and TDT2 by avoiding the word hack, and instead saying that, "Chaos Computer Club: iPhone 5S finger-sniffer COMPROMISED; Anyone can touch your phone and make it give up its all". By using the word compromised, TR2 lessens the blow of how detrimental the 'hack' could be for the future of Touch ID, though still projects fears of security and privacy being infiltrated. In general the piece is a regurgitation of Starbug's hack, mentioning the ease in which it was done, and quoting him saying that they only had to turn up the resolution of the scanned picture to achieve the hack.

8.3 Publication Discourses

Ignoring both geography and the timeline which will be discussed in later sections, the summaries of the articles above can be analysed further in regards to their respective publication discourse or more specifically, genre. As chapter six pointed out, the WSJ, the WP, TG, and TDT are all long lasting general circulation newspapers, founded in print form in the 19th century and published internationally, as well as having increasingly moved to the online sphere. CNET, AT, V3 and TR, on the other hand were all established in the mid 1990's in the initial booms of the internet, have dominantly been published online and specifically target news in science, technology and consumer electronics. By returning to Foucault's notion that discourse is inextricably linked to its sociohistorical context, as well as looking through the scope of the sociology of expectations, the following section will analyse how the history and context of these publications have affected the expectations of Touch ID.

8.31 'General Circulation' Expectations

As a paper based on business and economics, the WSJ looks closely at how Touch ID affects businesses, and by mentioning the likes of Google and Samsung following Apple's introducing of Touch ID, WSJ hints that the other tech giants may well eventually follow Apple's lead, bringing biometrics further into the mainstream. Furthermore, WSJ3 shows its international context by bringing a foreign government perspective into issue when it relates to how the Kremlin sees issue

of privacy with Touch ID, as well as showing a political stance by mentioning Sen. Al Franken's comments on privacy issues.

The Washington Post looks closely at national politics which can be clearly seen in the tone of WP1 and WP2 as it looks at a political aspect of Touch ID in regards to laws of whether governments or police could request biometric data from ones iPhone as 8.12 discussed. Further, as the WSJ does, by bringing up comments by Sen. Al Franken about privacy issues of fingerprint data, the publication further reiterates its national political context and shows its liberal political views. By quoting and paraphrasing Franken, the paper clearly shows they ask the same questions of how privacy can be protected through this device, and shows without such protection, the expectations of biometrics replacing the password aren't as strong, though it does mention that the technology could be good for company security.

TG takes a mixed view looking at both individual user concerns as well as companies. It notes in TG2 that, Touch ID could, "create concerns for businesses which see users intending to use the phone to access corporate accounts" (Arthur Sept 23 2013:para3). It also looks at individual security issues of one's finger being chopped off, and shows research on how identity theft could occur, by bypassing Touch ID and stealing account information like Apple ID among other passwords. Being more general of a newspaper, with a mixed focus as opposed to the other two papers above, TG's context reiterates this mixed view of expectations in both individual and company settings, though it ignores government issues.

TDT is considered more of a conservative publication, though overall it seemed to have a similar stance with the other general circulation publications. Where it differed though seemed to be its timeline. Section 8.5 will detail this shift further, but where TDT raised similar issues of security and privacy following the 'hack', the initial article had a more positive tone, especially in regards to security, through it made mention that only in casual security terms would it be effective.

8.32 'Online Tech' Expectations

Being dominantly tech based publications, it is unsurprising that CNET, AT, TR and V3 tend to go into more detail on the technical aspects of Touch ID as opposed to political or government issues. CNET looks at a historical view of biometrics from how Apple acquired the deal by AuthenTec, and how other earlier laptops and smartphones failed to attract the right market and that they failed in security and convenience, which CNET1 hypes of Touch ID having huge expectations towards the future of biometrics.

AT shows similarly more technical discussions, and provides more opinion than the 'general circulations' which seem to be more informative. AT1 details the 'secure enclave' Apple mention by noting that,

> *"Assuming the enclave is truly secure—meaning it contains some sort of trusted platform module designed to store sensitive cryptographic materials—all of this means that Touch ID has been designed to store the information in a way that can't easily be accessed by malware, hackers, and possibly other adversaries such as three-letter government agencies" (Goodin Sept 11 2013:para5).*

By detailing further the technical discourse of Touch ID, AT bring forth the opinion that privacy will be secure, if what Apple says is true, and that it is, 'truly secure'.

V3 also details the 'security enclave' and puts emphasis on the fine technical details of Touch ID such as noting that, "The Touch ID sensor is only 170 microns thin, just thicker than a human hair, with a 500ppi resolution to take a very detailed image of fingerprints" (Bennett Sept 10 2013:para9). This detailed context attempts to give secure legitimacy through numbers to help justify the strength of Touch ID. TR also strongly mentions the technology which as noted in 8.23 is not secure enough yet. Similarly to CNET, TR1 looks at a historical sense of how other biometric technologies have been implemented and failed, such as talking about a mouse with an optical scanner in the past which, when one breathed on it, produced the previous persons fingerprint and granted access.

8.33 Publication Discourse Comparisons

It is difficult to make concrete conclusions about how the genre differences in the publications affect their expectations, though there are some aspects which seem more clear-cut. In terms of how much detail about the technical aspects are given, although the online tech publications seem to detail them more, the WSJ and the WP do mention some of the details about the sub-epidermal layer of security and resolution Apple used. The technical aspects however are more evident overall in the second timeline through all genres, with the articles describing the hack, focusing on quoting CCC on how they explained the 'hacking' process.

To an extent, the general publications tended to focus more politically on government and corporate issues, where as the online tech articles seemed to look more at the individual level and how users would react to both security and privacy concerns. This can be evident in each publications socio-historical context. With the general circulations appealing to a wider audience, each respective publication had discourse relating to its own agendas, such as political affiliations. These can be seen from the sources which they link to in terms of both who, how many, and how they criticize the differing opinions which 8.4 will further detail.

The online tech articles first of all seemed to be more opinionated than the general circulation ones and hence had to do more so with the author's tech experience, and their previous opinions on certain companies, such as CNET1 which seems as if the author has a clear love for Apple products. This seemed to effect how much expectation was hyped on the possible success of the product, and lessoned the blow that other discourses were projecting on the privacy and security issues.

Overall though, the genres alone don't reveal much, and instead need to be looked in other parts of their context – timeline and geography – to further this discussion. Security, convenience, and privacy are discussed by all genres regardless of affiliation, yet to a small extent it could be said that the general publications focus on the corporation, and the tech focuses on the individual user.

8.4 Hype Analysis: Key Words, Style & Sources

The following section takes a more quantitative and visual approach to try and illustrate some of the qualitative analysis done so far on the articles. By looking at the keywords, it will show what issues are the most important, by visualizing the style of hype; positive, negative or neutral, as well as looking at what sources are used and shared. Further, this section will analyze through the keywords the extent to which Touch ID is hyped and predicted as an up and coming technology, and what is seen as its biggest challenges.

8.41 Key Words

US	UK
WSJ1: Apple, security, Fingerprint	TG1: iPhone, Fingerprint, Security
WSJ2: Apple, Fingerprint, Scanner	TG2: Fingerprint, iPhone, Apple
WSJ3: TouchID, Fingerprint, Security	TG3: iPhone, Fingerprint, Authentication
WP1: Fingerprint, Privacy, Password	TDT1: iPhone, Apple, Devices
WP2: Apple, iPhone, Fingerprint	TDT2: Fingerprint, CCC, Security
CNET1: Security, Fingerprint, Apple	TR1: Fingerprint, Apple, Security
CNET2: Fingerprint, iPhone, Security	TR2: Fingerprint, Resolution, CCC
AT1: Apple, TouchID, Security	V3-1: TouchID, iPhone, Fingerprint
AT2: TouchID, Fingerprint, Security	V3-2: Fingerprint, TouchID, Security

After taking away common words such as 'the' and 'and' etc., the above is a list of the top three words mentioned in each respective article, the most mentioned word being shown first. From a pure quantitative standpoint it is hard to ground results in these top mentions, especially as some of

the articles were not of a length sufficient enough to make a big difference in key words, with the top words in some of the shorter articles only having as many as 5 or 6 mentions. Nevertheless, from the data seen, a couple of points can be made, which will then be grounded with some of the qualitative work previously discussed.

'Apple', 'Fingerprint' and 'iPhone', are the dominant words throughout almost every article, which is unsurprising as those are the main things the articles are discussing. However if 'Apple' is looked at more closely, one could ponder that not only is Apple being talked about, but rather Apple is talking. That is to say, especially the articles which have Apple as the most dominant keyword, this can be not only because Touch ID is approached from a company point of view, constantly relating the technology back to its owner in the articles' discussions, but because a lot of the quotes are from Apple. Hence, this makes the article use Apple's voice a lot more, which obviously due to their agenda would show Touch ID in more of a positive light on its expectations.

This becomes clearer by looking at the tables below in 8.42. In WSJ1 and WSJ2 for example, the expectations seem to be more positive; both examples where Apple is the top key word. Then in WSJ3 where Apple is not mentioned, a negative light is shown. Other examples of this can be seen whereby the initial article has 'Apple' as the top or second top word such as AT1 and TR1 and the tone of the article is quite positive. Then in the following articles from the different timeline, AT2 and TR2, Apple is not a key word at all, and the articles are written in a more negative tone.

Furthermore, one of the key issues, the keywords show, is that when taking away 'Apple' as a source and 'fingerprint' and 'iPhone' as the system used for the device (of which all 3 words would be expected to be common), one can see that 'security' becomes the dominant issue which is spoken about. In 10 out of the 18 articles, security is in the top three of words mentioned, yet privacy and convenience, two other key issues in the biometric debate, are barely evident. Chapter nine will detail this further in the privacy vs. security debate.

8.42 Style Analysis

The following tables are an illustration of how each issue is discussed, and in what tone and style they are discussed in. In the table, green represent an overall positive light, yellow looks at both sides of an issue equally, and red looks at the issue as having a detrimental effect. The one-sided section simply refers to the article having overwhelmingly just a positive or negative vibe, whereas the two-sided section can be interpreted as to which side is more spoken about in the article i.e. green but two-sided means the article is positive, but negative issues are still presented. Further, this is also to do with which tone, positive or negative, comes first, as chapter nine will further detail on the importance of order of opinion in an article.

US	WSJ1	WSJ2	WSJ3	WP1	WP2	AT1	AT2	CNET1	CNET2
One-sided									
Two-sided									
Security									
Convenience									
Privacy									
NSA									
Picture/video									

UK	TG1	TG2	TG3	TDT1	TDT2	V3-1	V3-2	TR1	TR2
One-sided									
Two-sided									
Security									
Convenience									
Privacy									
NSA									
Picture/video									

The NSA is included in the table, as a key hypothesis from chapter five was about how much the NSA may have affected the issues of privacy within the articles. In this context, red is used if Touch ID has been looked at it in a negative light to do with the NSA, whereas green shows that the article mentions the NSA, yet doesn't make a huge issue about privacy. The NSA was surprisingly only mentioned in four of the articles, and more in a positive or neutral fashion. This is largely because of Apple's 'secure enclave' which has created a positive tonality out of the privacy issue as has been previously mentioned.

Figure 5: A Fingerprint. *Source: (*Curtis 23 Sept 2013)

In the UK perspective, it can be seen that privacy is almost always discussed in a positive light, where it is more mixed in the US perspective, though that is clearly domineered by the two 'general circulation' newspapers the WSJ and the WP, and comes about from their discussions on the privacy of law, companies access to data, as well as government access to data to do with fifth amendment rights.

Lastly, picture/video has been included as it plays a small role in how each article is seen and interpreted. The analysis of whether a video or picture had a positive or negative vibe will come clearer in the video analysis section which details the impact of the hacking video, but to a small extent it is worth noting here. The negative images were ones that had a dark image of a fingerprint with a black background such as in TDT2 (see figure 5) and AT1.

These images bring immediately back the sociohistorical criminal discourse when seen in such dark colours and such a data centred gaze of the human makeup. The more positive imaged on the other hand were ones such as in TG1 which showed a finger on Touch ID and the word, 'success' appearing (see Figure 6), showing a discourse of convenience and security, projecting the idea that Touch ID is a success. Even though the pictures make another interesting point of study, no conclusion could be made as they did not correspond to any kind of pattern with the differing tones of the articles.

Figure 6: Touch ID in use. *Source:* (Campbell Sept 11 2013)

8.43 Source Analysis

The following is a list of companies and individuals that are either quoted or paraphrased in each article.

US

WSJ1: Apple, Kevin Mahaffey at Lookout inc., RSA, Cisco systems inc., PayPal

WSJ2: Apple

WSJ3: Apple, Sen. Al Franken, Vitaly Milonov

WP1: Security researcher Bruce Schneier, NSA Chief Gen. Michael Hayden

WP2: Apple, Sen. Al Franken, New Signature, Unisys, Agilex

CNET1: Apple, PayPal, New York Attorney General Eric Schneiderman

CNET2: CCC, Sen. Al Franken, CNET

AT1: Errata Security, 'Bitweasil' password expert, Cigital, KeyMe, TG, WSJ

AT2: Marc Rogers security expert at Lookout inc., CCC Starbug

UK

TG1: Huffington Post, Mar Rogers security expert at Lookout Inc., Consult Hyperion

TG2: Apple

TG3: CCC, security specialist Graham Cluley, Apple, Craig Federighi Apple's software head

TDT1: Apple, Paul Schiller Apple marketing vice president, Tim Cook Apple CEO

TDT2: CCC, security specialist Graham Cluley, Apple, Craig Federighi Apple's software head

V3-1: Apple, Paul Schiller Apple marketing vice president

V3-2: CCC's Starbug, Kaspersky

TR1: Ovum, Rapid7, Trend Micro, Lumension, Security researcher Bruce Schneier, SecurEnvoy, Webroot, Bluebox, Naked Security Blog

TR2: CCC

As was suggested from results of the keyword section in 8.41, Apple is the dominant voice in many of the articles as seen from the above sources, especially the ones which speak of Touch ID in a positive, hyped expectation context. Some of the articles simply mention an Apple spokesman, while others actually quote either Tim Cook or Paul Schiller. From simply looking at the sources it is hard to say exactly how they are written though. Just because Apple is quoted a lot does not necessarily mean that they have the dominant positive voice. However, by comparing this data on sources with the previous qualitative data, as well as seeing how many outside sources each publication used, a better understanding of how the different contexts created the different expectations can be made.

WSJ2, TG2, and V3-1, all only mention Apple sources, in combination with the respective authors' possible criticism, which as has been discussed in these articles were more 'informative' rather than opinionated and critical. Returning to the above table and previous analysis, these three articles corresponds dominantly with a positive expectation for almost all issues of Touch ID, and hence, it critically reveals how influential the sources are as a form of actor in the debate.

Furthermore, it is clear that the large majority of sources are dominated by security experts and different security firms, which adheres to the keyword section about how security seems to be dominating the debate as opposed to privacy or convenience. What is noteworthy is that the US articles present clearly show that more interest is put onto government sources in their publications as opposed to the UK sources which make no mention of any government figure, aside from a passing note on the NSA. Although the US does only mention two, Senator Al Franken and New York Attorney General Eric Schneiderman, Franken is mentioned in three of the articles, and a strong issue of privacy emerges, at a different angle to ones emerging in the UK, as has been suggested due to law difference between the countries.

A few other sources also double up such as Craig Federighi's quote about Apple's secure enclave in TG3 and TDT2, both of which was used to try and reassure readers about privacy concerns, though they were contained at the end of the articles, and both had more of a negative tone. Marc Rogers also made multiple appearances in the sources. TG1 and AT1, both show quotes describing his scepticism towards the security of Touch ID; with his quote in TG1 used a little stronger in comparison to the article when he discusses past examples of criminals mutilating people's fingers for access. Whereas in AT2, his quote is not as hyped about detrimental possibilities and instead notes that although CCC had 'hacked' Touch ID 'easily' Rogers did not quite agree. Although used for different issues, it is clear that the quote used in each circumstance presented a clear difference in how much hype was being projected on the expectations and the problems each issue posed.

8.5 Timeline and Shifting Discourse

In terms of the timeline, the goal was to include articles from each publication at both the announcement of Touch ID and following CCC's hacking of it. While most of the articles analysed fit this criteria, unfortunately a couple of them, WSJ1 and WP1 were published before the release of TouchID, as has been briefly discussed, and hence some of the authors' opinions negate a crucial announcement from Apple about the 'security enclave' which shifted how privacy was analysed of the Touch ID. These earlier articles were chosen because this thesis wanted to use articles that mainly focused on Touch ID rather than just on the iPhone and some of the pre-announcement articles had a good in depth analysis of the, at the time, predicted fingerprint sensor as opposed to the focus of the iPhone on the announcement date. Nevertheless, this point has and will continue to be used in analysis.

Further, another difference in the attempted 'black and white' timeline (one article at the announcement, one at the hack) came about when a difference was seen in the articles at the announcement and *before* the actual release. Although at the announcement Apple's secure enclave' created hype about secure privacy possibilities, there was still scepticism discussed until people actually got to test out the Touch ID, and see if it could be hacked as CCC eventually did. Though what this hack actually is, is the subject for further debate of privacy and security in the next chapter.

Either way, this timeline shift can be well seen between AT1 & AT2 as there is a clear difference in how the author hypes the expectations of TouchID, shown from the author's surprise that it was hacked so quickly and easily. As Goodin says of himself and the publication, "Ars expressed surprise on Monday that a hacker was able to bypass fingerprint protection less than 48 hours after its debut in Apple's newest iPhone" (Sept 24 2013:para1). From initially bringing a two-sided argument to the debate, by interviewing CCC in AT2, they change the discourse of issue to a higher distrust in the security of Touch ID.

Furthermore, the shift in timeline contained the same author which can't be said of the other articles used in this thesis, aside from WSJ1 and WSJ2, therefore with the other articles it is not possible to analyze whether a particular author has shifted in perspective from the time of the announcement, release and/or hacking of TouchID. However, how and if the dominant discourse shifts in the publication is still worthy of analysis.

Firstly though, in regards to WSJ1 and WSJ2, both by Yadron, they are written a few days apart, however not after the hack. WSJ1 is written before the announcement, therefore included more speculation and rumours, to WSJ2, written the day after the announcement when all of the

information was available. Not much seems to shift in the authors perspective between the two timelines, aside from the positive outlook of privacy in WSJ2 following Apple's discussion of the secure enclave.

Interesting to note, is that both WSJ1 and WP1 are both written before Apple's announcement, yet seem to be written in an opposite tone, one with hype and excitement, and the other with fear and problems. WP1 without knowledge of the secure enclave makes grave discussions about how ones fingerprints could be truly hacked and lifted off the device to steal ones identity. WSJ1 barely even mentions any privacy issues though, which may be why it is in such a positive light, simply as it doesn't mention the issue. From this we can argue that before the announcement and at the announcement, the discourse changed from privacy being more of an issue, to other factors taking control.

In terms of some of the other articles between the announcement and hack, by looking at the tables in 8.42, it seems pretty clear that the discussion in general went from positive hype to negative. This is obviously because of CCC being the dominant source quoted in the second timeline, as seen in 8.43. While not all of the articles about the hack show they agree with CCC about how biometrics are too insecure to be a password replacer, overall there does seem to be an increased discussion on the security discourse in the latter timeline. However, chapter nine will further deliberate on how the hack has created a security rather than privacy issue, in contrast with the hypothesis that privacy would be the main discourse in discussion.

8.6 Geopolitical discussions of security and privacy

As chapter 3 discussed, although revolutions in internet capabilities have globalised the world, place still matters. From geo-blocking websites, to gaining access to publications through local credit card details, geography still makes a difference in the direction, tone, and process of how ideas get published. However, this is only to a certain extent. The publications are international, and the way people gain information through multiple sources such as social media or Google searching, makes it sometimes difficult to even know what country a website comes from.

Looking at both these arguments, the data generated from the articles show that although generally, the difference between the US and UK perspective is not as great as was hypothesised, there are still distinct differences worth noting, which come inherently from the geopolitical landscape. There is no clear-cut way of revealing whether the US articles focused more on security, or the UK more on privacy, as each article, each publication and each timeline had different perspectives in the way they approached the issues. One clear note however was in terms of privacy and the law which was only dominant in the US discussions and absent from the UK.

The discussions on the Communications Act, and issues with the Fifth Amendment, were discussed in AT, the WSJ and the WP, as well as *Forbes* and *Wired*, two other US publications which were briefly analysed but chosen not to be imputed into the thesis for lack of time and comparison with UK sources. These privacy issues came about from a US senator, which was a shared source for the WSJ and the WP, and hence took a different angle than the UK. As the UK does not have the same law system on self-incrimination and Fifth Amendment rights, the discourse of which privacy was discussed showed a bigger dominance in the US geopolitical landscape.

For example, if a person was to be arrested in the US, they can enforce their Fifth Amendment rights whereby they do not have to say anything which could incriminate themselves. This could b, for example, a password to a laptop computer with evidence against them which they are under no obligation to give up. However the law could get tricky if the laptop could be accessed through finger verification, as the finger is not in the mind and not subject to ones Fifth Amendment rights. In the UK, although they have a right to silence, it is in no way as strong as in the US system, and one can even have silence used against them in court if they fail to provide knowledge of evidence, such as, perhaps a password to a computer. So the clear point seen from the different geographies is how the US has approached the law and biometrics.

8.7 Forced vs. Voluntary Discussions

This question was in regards to whether comparisons were made between Touch ID and other historical uses of biometrics outside consumer electronics, in more forced institutions. None of the articles in fact mentioned how people currently use biometrics in visa applications, border security, or how forensic investigators use it as a one of the golden keys in identifying a subject. This was both surprising and understandable, as although the sociohistorical context of biometrics is important to understand, almost all of the articles' main aim in looking at the expectations of Touch ID was whether it would catch on in a social sense for the consumer, and how fingerprint biometrics could work in other mobile electronics.

Only really in the WP's discussions about the Communications Act, as well as some light hearted mentions of the NSA, did the articles hint at a wider implication of user Touch ID, such as the possibility of a database forming with all of societies fingerprints. Issues are also raised about whether fingerprint identification could be used in online banking institutions, but understandably, they focus on user friendly ways, on convenience. Thus in a user sense, especially for companies like Apple using Touch ID as a product to return investment, forcing such a technology as opposed to voluntarily providing it would be bad for business, hence why Touch ID can be switched off. But there is still more to this idea of forced consumer biometrics as the next chapter debates further.

8.8 User Comments

To see how the user responded to articles about the hacking of Touch ID, a list of comments was taken from AT2 and TR2 to see if a difference in US and UK commenting could be made, as well as to see what kind of discourse the commenting community puts on the hacking. First, a quantitative methodology was taken to search for the top-ten keywords of the comments in each article including:

US AT2: iPhone, fingerprint, security, Apple, unlock, hack, safe, access, sensor, theft

UK TR2: iPhone, fingerprint, security, Apple, latex, access, thief, keys, perspective, door

Evidently, there is no real difference between the key-words of the comments in the different geographies, as even if each article has a different tone, they both are discussing the same issue. As mentioned before, there is no big difference evident between the two geographies, aside from a law perspective which was not mentioned in the articles where these comments were taken. Just as the keyword was used in the majority of the articles above, once again is security the highlight of conversation by the commentators.

The other top-words in TR2 such as 'keys' and 'door' can be explained by the fact that a debate went on between the commenter's about comparing a physical key to biometrics and how it could be copied. This was further generated by many commentators arguing for 'perspective' in regards to how Touch ID was hacked. Commentator, MegaTech, highlights this perspective by writing a fictitious, satirical news article saying how keys are unsuitable to lock the doors of the house, because criminals could, using a difficult forensic process, eventually be able to copy the key and access the house. He concludes by noting that, "Determined criminals will be able to access your property regardless of your front door key, of course. But for opportunistic criminals - which represent the vast majority - front door key technology is a strong deterrent" (Chirgwin Sept 22 2013). In relation to Touch ID, this user gets many comments of praise, as to the perspective this provides. That is that, the most important thing for Apple introducing Touch ID was not to be a full-proof, unhackable system, but rather a convenient casual system which would be a deterrent for the casual criminal.

In AT2, the word hack is also quite high on the list of keywords, and this can be explained due to the long discussions which go on about the use of the term 'hack' to describe what CCC actually did. They argue that all that was done was that the fingerprint reader was fooled into believing a fake, was a legitimate fingerprint, and most believe it was pretty obvious that this would happen as it has

been happening for years in fingerprint systems. They mention that the process CCC used was nothing new.

Similarly to the comments in TR2, one of the main points that is made, is that because over 50% of people don't have a PIN on their phone (a statistic many refer to in the comments), just having Touch ID, even if it is 'fakeable', makes it a lot more reliable because the product is only reliable if people actually use it. A lot of the debate that goes on actually seems fairly trivial because it is in regards to where a thief can actually take a sample of your fingerprint versus being able to look over someone's shoulder to see them type in their password. Many mention that your fingerprints are all over your phone anyway, and that they can extract them from there, but others simply argue that, similarly to the perspective mentioned in AT2, only a determined criminal could do the process that CCC does. As the video analysis in the next section shows, the process is not as easy as it is made out to be.

Lastly, by noting that thief and theft are in the top-ten of both comment sections, one could postulate that they speak more of the thief rather than the criminal. The term thief does in the present time have a much softer term than criminal, and could be generally considered for more petty crime. Thus, the main points that are being made is that Touch ID is 'good enough' against the average thief who doesn't have the time or will to go through the process set out by CCC, and therefore the security is good enough for Touch ID to continue to be a useful, convenient and secure enough password replacer, but only in casual settings.

8.9 Video Analysis

To add a further level of analysis on the expectations of TouchID, the following will analyse CCC's video, which is posted on AT2, alongside an interview with Starbug, showing the exact process the group used to 'hack' TouchID. Firstly, one of the most striking elements is the anonymity of the video, which adheres strongly to this black-hat hack culture, of hiding behind illegality. Throughout the whole video, only a small, half angle shot of a person's face is seen at one point, whereas the majority of the time only a person's hand is seen, assumed to be Starbug as he claims it is he who first did the hack. This anonymity also supports Starbug using an alias rather than his real name. But the fact that it seems so anonymous, especially with the term hacker used, it connotes a sinister sort of vibe, as if something illegal is happening and the person does not want people to know who he is for fear of legal action.

Furthermore, this criminal discourse is emphasised in the lighting used and lack of vocals and background sounds. A lot of the video is presented with dark shuddery shots of Starbug following the step-by-step instructions which are projected in white across the screen. The use of subtitles as

opposed to vocals explaining the steps is most likely for it to be more universal, linguistically, but it adds a further layer to the anonymity, illegal connotation. No voice, barely a face, no consequence to ones action. The silence throughout a lot of the video also creates a level of mystery, which is culminated in the slow removal of the dummy print with a knife, something which would be more reserved for a spy movie. Through this, it becomes hard to see it in the context of a DIY hacker tutorial, especially as the copying of a fingerprint is surrounded by the discourse of illegality.

Further in regards to this illegality, a crucial point throughout the video is that certain objects shift their discourse through the translation process that Starbug is projecting on them. Objects like the photocopier, scanner, graphite, and wood glue, all shift their everyday discourse in their moment of relevance as Heath & Hindmarsh note, "talk is inextricably embedded in the material environment and the bodily conduct of the participants, and how objects and artefacts such as paper and pens become momentarily relevant" (2002:7). So although speech is absent from the video, the objects interacting and networking together, brings together meaning, and helps project this criminality discourse of black-hat hacking, and stealing ones identity.

Furthermore, the video must be looked at as a 'situated action', it is not the reality of daily life of the CCC group, but rather a constructed scene, whereby the frames and time changes without any indication of what has happened in reality. Through ethnomethodology, it can be seen that Starbug's actions in the video is helping to create context. His hand shakes uncontrollably at stages as he attempts to interact with a tiny piece of graphite, placing wood glue on it to mimic a fake print. He is translating an everyday object into a nonhuman copy of a human finger, as a process to then translate his identification onto another nonhuman, TouchID, which then verifies if the process of translation is successful. Each object, each actor, becomes relevant at certain stages of the translation, which inherently changes the discourse of what is being projected.

To compare this video with the article, comments and interview with Starbug, is to analyse the sociohistorical context of biometrics which is inextricably absent from many of the other discussions. Security is constantly echoed as the issue with which the hack is proving. Starbug has hacked the security of Touch ID, penetrated its walls, and taken over the fort. However, the argument for privacy is simply diminished; rightly so in the context that the fingerprint data doesn't actually leave the phone. However, the video, through this forensic, identity stealing context, reiterates the privacy argument, for the video forgets the simple verification which is actually going on. Although the ultimate success is that the finger has been verified by a nonhuman, it does it in a way that sees the identity being stolen, ones identity which is clearly linked with the issue of privacy.

Lastly, to return to the time frame of the 'situated action', the ease at which the hack takes place is questionable, especially through the many cuts used throughout the video. It is hard to get a sense of how much time is taken between each step, as well as whether there were any failed attempts. This is further noted in the comment sections, as well as by security research Marc Rogers about whether it really was as easy as it says. This adds to Starbug's argument that the hack was very easy for the average person, as the video makes it look very clean and unproblematic. This appearance of ease the video projects is however quite problematic, as it makes it seem as if anyone with a printer and a couple of other materials could fake a fingerprint, which in reality as many critics have said, would be much more difficult for the average person. So overall, the video projects an anonymous, criminal, and simplistic discourse, which could be interpreted to pose strong arguments to the debate on biometrics as a secure verification system. This video really makes fingerprint scanners seem very unsecure, just as CCC hoped for, something which may not be as clear cut as the video suggests. But it also brings the debate of identity and privacy back into the picture, which the next chapter will further discuss.

9. Results Discussion

This chapter will provide an expanded analysis of the data gathered from the previous chapter, as well as analysing the results obtained in comparison with the hypothesises discussed in chapter five to postulate on some possible overall results the data has achieved. An analytical comparison will also be made between the video, content and discourse analysis, as well as how the different sub-questions fit into the main question on how TouchID has been reported in the US and UK print media. The main issues of security and privacy, and how they are dealt with will begin this discussion, to bring clarity into their similarities and differences, and be used as a guide for the rest of this chapter's analysis.

9.1 Privacy vs. Security

What does the data analysed thus far reveal about the relationship between privacy and security? Are they really that different? Do both issues affect one another simultaneously? Both issues no doubt play a big role in the expectations of biometrics increasing as a widely-used verification system, and the research from this thesis, has shown that the difference between the two issues is not always clear-cut. Although some of the research relied on keywords to illustrate the importance of the respective issues, such as noting that security was an issue most often written about, it neglected to reveal how both security and privacy can be seen to co-produce as actors simultaneously when analyzing the interaction in biometric expectations.

In many aspects security and privacy can be considered the same issue, though they are also quite different. Importantly, you cannot have one without the other. Take the sources for example in 8.43, almost all of the sources are security experts, security advisers, security consultants, security firms etc. but none are from privacy companies or privacy firms. That is because they don't exist, or at least in not in the principle way security does through the above examples. This is because without security, privacy doesn't exist. Security is the force field surrounding privacy from the dangers of identity theft and fraud. As security grows, so does privacy with it. Conversely, privacy dictates security. The more confidential and top-secret something becomes, the more security is needed to surround it. If privacy is not protected, it fails to be private. So to an extent, one could say that privacy was also an important source being referred to, at least in how security firms can protect privacy. In that sense both could be seen on equal terms.

In terms of biometrics, day-to-day verification systems can only become wholly mainstream if they can be reliable, secure and keep privacy in check. If the security fails then so too does the privacy, or at least that is a principle argument behind the two terms. However by looking at CCC's hack, we can see that there are two different contexts of security and privacy being represented. On one hand, the security is protecting the phone from access to personal data such as email logins or private photos. By CCC creating a fake print, they broke through this security and gained access to the private data on the phone. On the other hand though, the security protecting the biometric data was not compromised thanks to Apple's 'secure enclave', and so ones digital fingerprints remained private. But what is the big deal then with someone having your fingerprint anyway?

Does it really matter if someone gets access to your fingerprint? The whole point of CCC's hack was that the hacker had your fingerprint in the first place from a latent grab. It is not just that the whole process is quite complicated to do, as has been argued against CCC, but is it not redundant to find a person's fingerprint on a glass, take the latent print, turn it into a fake finger to use to access their phone, to then get their fingerprint data? You already have the data in the first place? Thus is it your privacy, or security that is being stolen?

The problem is more in terms of Big Data when one can access fingerprints through online hacking and then gain a large amount of fingerprint data from people they never had to meet before. This is like stealing cash versus stealing credit card information. Before credit cards and the internet, the only way to steal ones fortune was physically do it. If biometrics grows as a device for many other applications, yet is not encrypted well enough, then it leads the way for hackers to steal peoples fingerprint information and other data online. It is at this point that if these data sets are used for secure things like online banking that a problem occurs.

It also is a chicken and the egg problem with biometric systems and personal data co-producing together. Without the system the data doesn't exist, without the (digital) data the system doesn't exist. In the past, even if one was good enough to manually identify someone from their fingerprint, they could not access anything with it. They could not use it for verification. Yes, the many problems of fingerprint identification in the courts has been arduously written about in this thesis, but it is the digital verification possibilities that modern biometrics develop, whereby the fingerprint and/or other biometric qualities, could be something to protect more closely than before. It is at this stage that the security, of the privacy, of the biometric identity is of great importance. So which is it then that is of great importance in this debate? Is it security or privacy? The content analysis seems to say it is security, but the video analysis questions this assumption.

9.3 Comparing Methods and Results

In the second timeline, it is clear that much negative hype on expectations is presented in almost all of the articles, in strong relation to seeing a security breakdown in Touch ID through the hacking, and hence showing it is not as reliable in keeping secure information. But the saving grace seems to be the 'secure enclave' in the device, as it is the main reason privacy is not scrutinized as much. However, what most of the articles don't discuss is the array of personal data on ones phone, and that this second discourse of privacy is actually made available, through the security hack. The 'security enclave' only protects the fingerprint data, not all of one's other private data stored on their phone.

This is something that is brought up in user comments and hence this method revealed a different discourse than the content analysis of the articles. Many mention that the phone has access to online bank accounts, social media, and that someone gaining access to them would be detrimental for ones privacy. However, they mention this, not in criticism of Touch ID, but more so in how the hack was called a 'hack' as they saw the articles hyping an oversight which it wasn't.

In AT1 for example they use the term 'bypassing' TouchID, a much more casual way than calling it strictly a 'hack' which many other news articles did. This term hack immediately conjugates notions of privacy and identity being stolen, even though in principle, it is security that has been stolen, or at least overcome. It has already been mentioned that V3-1 and TDT2 also used the term hack in different ways in their headlines which created similar negative hype. This is crucial to the debate as the headline is the most important aspect of a news article.

Many studies have shown that people only read about 50% of an article (Manjoo 2013) with something like 38% leaving after only the headline. This is why articles which did give both sides, received a positive or negative colour style in section 8.42 of this thesis depending on which order the sources and hype was projected in. If only 50% of people read an entire article, then the second side of a debate only presented at the end of the article, will only be read and understood by half the public. Thus the headlines and first few paragraphs were crucial in why each respective article was rated as positive or negative hype. But what is so important about how the articles are framed?

As has been continually discussed, it is this thesis' position that the framing of the media has a large affect on how different technologies develop and are adapted by users. By seeing what issues are debated and in which contexts a better idea about the positive and negative expectations can be understood. If all the articles had put Touch ID in a very positive light, and argued that its security, privacy and convenience factors were strong and secure, then that would make the expectations

that biometrics could truly be the password killer high, and become key in developing the technology further into a mainstream authorization/ verification system. Conversely, if all of it was contrived as negative, then that is both the media expecting the technology to not catch on and fail, which as a result can affect how society adopts to it.

Furthermore, the use of video and print media together caused an interesting dichotomy worth reflecting on, especially in light of AT2, which had the video embedded within the article. By being actually able to 'see' the hack occurring 'in situ' as opposed to just hearing about the bias opinions of Starbug, more light could be drawn onto the process, and as a result, more scepticism could be made. As the analysis in the previous chapter dictated, the overall mise-en-scène of the video showed a much stronger negative discourse of criminality than the article and interview with Starbug, which seemed to show more of the 'greater good' aspect of the 'hack'. That is that he was doing it to warn people of the dangers of biometrics and their insecurity.

The video also sheds light on the privacy discourse more so than many of the articles. The way it politicized everyday artefacts, into identity stealing devices, accentuated this black-hat discourse, away from that of a mere security issue. As van der Ploeg (2005) arduously argues, the body and identity are very closely intertwined, and any way of using nonhumans to mimic the body, creates drastic identity issues, and hence privacy issues. Overall both methodologies complimented each other by mixing security and privacy issues as the next section will further detail in how they helped answer this thesis' questions.

9.2 Comparing Hypothesis' to Results

From the empirical analysis it is clear that while some of the hypotheses were quite far from what the results suggested, others seemed to be quite accurate. One of the main hypotheses on the general expectations from all the articles was that expectations will be high for usability and convenience, yet questioned largely on security and privacy issues. This was very accurate, as seen that almost all of the articles spoke of the convenience aspect very highly, even referring to the fact that because convenience was so high, a lot more security precautions would be taken by users as opposed to PIN codes, which not as many people used because of the inconvenience of having to remember them, and the time it takes to type them in.

In terms of the two time periods, the original idea that the discourse would change from privacy to security was only half proven. Security was definitely the most common issue discussed in the second timeline shown from keywords and sources, but the first timeline did not make a huge issue in general with privacy, and instead also focused more on security, which is something that has since

modern biometrics developed, as seen in the state of the art, been the main source of scrutiny. Further in terms of privacy, the discussions and links to the NSA were not written about as much as hypothesised. What was especially interesting was that the ones that did mention the NSA, did not so in a negative light, but rather used the reference to note the absurdity of privacy issues in biometrics, and hyped the positive expectations.

In light of the geopolitical differences, the hypothesis was that the US would focus more on security due to its strong borer and visa security programs following 9/11, and that the UK would focus more on privacy due to the country being dubbed a 'surveillance society' by Martin (2011). As section 8.6 showed however, it was difficult to make any kind of underlying statements about how each geographical region of publication discussed each issue differently. The best result from these boundaries was the difference of law in Fifth Amendment rights from the US perspective as the previous chapter detailed. It was because of this that the WP looked the most negatively at the expectations of Touch ID, and hence overall the US perspective had a slightly more negative view from the articles selected, but not enough to make any concrete conclusion about the differing expectations by geography.

Lastly, conversely to the expectations that in the user comments they would mainly discuss the headline, many of the users extended the boundaries and brought up several strands of debate from both articles as a whole. In both geographies the users were quite critical of how the term 'hack' was used, and the overall tone was that biometrics in a casual setting was a great improvement of previous uses of the password. They noted that despite the possible security flaws, Touch ID has improved security due to it having more chance of users using it. However the majority of users remain sceptical about using Touch ID for banking or other secure uses.

10. Current Context and Further Research

The inspiration for this research project begun actually before Apple had released Touch ID, and was originally about the general expectations of biometrics and the possibilities of their dissemination through mobile devices. From Apple's acquisition of Authentic in 2012, the possibilities of Apple using biometrics became a strong possibility. A talk at the Biometrics Institute Technology Showcase (2013) by consultant, David Birch from Hyperion, a security and IT firm based on secure electronic transactions, furthered this expectation and brought the changing discourse angle to this thesis that is looking at the difference between verification and identification. Birch noted that we need to stop sharing our "real" social identity when we don't need to, and rather we want biometric 'tokens' as opposed to mass databases.

Luckily for the timing of this project, Touch ID was released at the beginning of the research phase, and hence the timeline was chosen as such. Although a lot of interesting data has come out of the initial expectations of the device, due to the fast expansion of technology and the benefit of time, there would be many more angles the research project could begin from, had it started presently. With over two years passing since this project has begun, people have had ample time to use Touch ID, as well as for other companies to further implement similar systems. From this, a few more research opportunities could be utilised to extend this thesis' work.

Now that Apple Pay is slowly being introduced internationally to be used for purchases, Touch ID is clearly becoming more mainstream, and hence the possibility to examine fraud in financial cases in regards to using TouchID would be worth note. This could be done through interviews or focus groups with people who regularly use Touch ID, and with people who have had their phone stolen.

A general consumer survey could also be made, to try and see whether Touch ID has increased the percentage of people who actually have some kind of 'lock' on their phone, to see if the Touch ID is being utilized more than passwords in the past, because of its convenience. Surveys could also assess how many users had problems with Touch ID failing multiple times, and whether their friend's fingerprints managed to access them.

Further, a cross-comparison research could be made with other systems similar to Touch ID such as Samsung's smartphone fingerprint reader, to see which device seems to have more convenience, security and accuracy. Further, this can be expanded into looking at the multitude of third party

apps, especially many concerned with financial transactions, which are now adopting Touch ID as a verification and identification tool.

Lastly, the main case this thesis looked as was in fingerprint sensor technology, and while it did mention a few other biometric techniques, it did not go into much detail about them. Another interesting research approach would be to look at different biometric techniques used on mobile devices such as comparing Samsung's facial recognition with Touch ID. Of course, when analysing a different biometric technique, one must take into account the different bias issues which occur. But overall, different techniques in a changing discourse say, from CCTV scanning for terrorist suspects through facial recognition software, to simply using facial recognition in casual ways of accessing ones phone, surely poses an interesting comparison on its expectations of how society may adapt to it, conversely to Touch ID.

11. Conclusion

From the start, this thesis has been dealing strongly with expectations. With the release of Touch ID on a device used by millions of people daily throughout the world, the expectations were high that the fingerprint scanner would be used in a more mainstream casual way than it had been in the past. With the popularity of Apple, it was almost certain. The question then was not going to be, whether a mass amount of people would have access to a biometric scanner, to use for daily verification and keeping their phone secure, but rather *if* they used it, how often they did, whether they saw security or privacy issues with it, and ultimately, whether the introduction of the device paved the way for many other companies and institutions to follow. And follow they have. Although due to the timeline this thesis dealt largely with expectations, by looking at the present context one can see many smartphone companies have also included biometrics as well as even credit card giants Visa and MasterCard currently implementing biometrics verification into their credit cards, thus biometrics has clearly become a lot more popular in the past few years. That is not to say that there are not still expectations worth analysing of biometrics continually increasing in use and being adapted by more countries. Although millions now have a fingerprint sensor in their smartphone, the large majority that still have older or cheaper smartphones do not. So there is still time and expectations to see where biometrics will end up. They still have a lot of issues to answer for, and a lot to grow.

Either way, where expectations were the initial discussion of this thesis, through looking at the birth of modern biometrics from historical issues and the criminality discourse, to showing how technological mobile revolutions have begun the way to change this discourse, this thesis is less about expectations and more about discourse. Can biometrics be casual? Can biometrics ignore identity? Can verification co-exist with identification? These questions seem to be the crux of this thesis. With all of the data gathered, the expectations, hypothesis' and analysis' in the news articles and user comments, a key point that comes out, is that biometrics must be seen in its respective discourse, and how it is used as verifying to access ones iPhone has been a large debate into what discourse this is.

In forensic investigations for example, biometrics has the strongest possible need to be accurate and secure. Privacy and convenience is not so much an issue as is accuracy as this discourse is inherently about identification. The problems with perfect matches aside, as long as two prints can be verified to match one another, identification can be made through a database. If this same discourse was

thought about in terms of Touch ID, this creates privacy issues with the user, that doesn't pose as strong an issue in governments and police forces looking at classifying and ordering people in society. Consumer electronic companies have to prioritise different elements of their technologies. That is not to say that innocent people don't worry about their privacy and how they could be subject to criminal investigation through fingerprint identification. The point is that this discourse is strongly there and this thesis is not arguing to change the forensic discourse of biometrics. Rather it uses this discourse, to analyse how it has affected the more casual discourse of using biometrics in ones phone, and asks whether this can actually be considered casual.

11.1 Casual Security vs. Casual Biometrics

There is no doubt that Touch ID is not a full-proof system, shown clearly from CCC's hack, as well as many discussions in the articles and even Apple's admitting that its fail rate is 1 in 50,000, though still five times more accurate than a 4-digit PIN. However, this question of needing to be full-proof and problems with security is one which keeps coming up in the discussion. The questions that many raise such as Graham Cluely, is that Touch ID is ok for casual security, but shouldn't be relied on to secure sensitive data. As the user comments suggest in the articles, Touch ID is secure enough for the 'casual thief' but not for the 'determined criminal'. Thus Touch ID, as well as other forms of biometric verification, must be understood in this casual discourse.

But can biometrics ever be truly casual? Sure many people mention, such as discussed in the user comments, that they don't have much personal information on their phone. If a thief wants their phone they only get a few SMS's and some phone numbers as one user commented in TR2. But just like the argument people pose of other privacy aspects such as, 'if I have nothing to hide, why does it matter', the amount of data in an ever connected, mobile world, questions whether privacy can ever be a casual thing, as it not only contains information *about* our identity, but the nonhuman iPhone merges into our *actual* identity, being part of our identity.

Therefore we must understand which discourse is relevant for which biometrics. Not just whether it be fingerprint, or iris scanning, but also the intricacies of how the systems are designed. In terms of fingerprints, this could be how deep the system looks into the sub-epidermal fingerprints, how many pores it counts, how deeply it looks at differences, whilst compromising the success rate. Essentially, depending on the context we need to look at how convenience and accuracy overlap. Currently a compromise has to be made, and in consumer electronics, as Apple has done, this has occurred, and they have chosen user friendliness, over a more heightened security. As Jain and Kumar (2010) illustrate, "the choice of a specific biometric modality typically depends on the nature and

requirements of the intended identification application" (2010:50). Thus depending on how secure, or privacy conscious an application is, the modality of the biometric capabilities must reflect this.

With Apple Pay now being introduced, biometrics has been continually adopted as payment methods by banks, in ATM's as well as in iPhone Apps to login to bank accounts. These biometrically verified monetary transactions, changes the actual form of payment to more of a casual way by simply pressing a button with ones finger; however the reaction is anything but. While many argue the 'novelty' of accessing ones iPhone means security isn't a huge issue with Touch ID, this modality shifts from casual in principle, to the need to have stronger security requirements when looking at more complex networks the Touch ID utilizes when 3rd party apps begin being introduced. Although the actual action seems simple, the underlying process is complex, and in privacy conscious industries, Touch ID may not be up to standard, as said in TR1, the technology to provide strong security and convenience is probably still 10 years away.

This 'novelty action' further reiterates the issue in high-sensitive situations. The simpler something is to do, the more casual it seems. Even if one had the most full-proof system which accessed something fast and simple, versus a fairly secure system, but which took a lot more steps, the casual nature of the former and the more complicated nature of the latter, suggests that the latter would be harder to crack. Therefore, ironically, it would seem more secure, when in this hypothetical scenario, it is clearly not. For example, to access ones online bank one must type in a cryptic password with a symbol, capital letter, number and be minimum 10 digits with no digit repeating. One must also remember a cryptic client ID, and then receive an SMS to their phone with another code to enter to finally access their bank account. Compare this action, with touching ones thumbprint to a smartphone and achieving the same thing. The extra layers of protection from the former make the action seem less casual, more formal, and more secure. The process of each step psychologically creates a feeling of security in the user.

Conversely, by simply pressing ones thumb for payment, the action seems more relaxed, more human and more casual. As Apple hype, the best password in the world is your finger as you have it wherever you go. Fingerprints, as has been argued, are no means as secure as this two-factor authentication mentioned in the above example, but even if hypothetically they were, the action of the user, and the physical nature of the finger creates a differing dichotomy; the password being in the mind, and the finger being physical, revealing your password to the world. This returns to van der Ploeg's concept of the 'machine readable body', and the issues with the finger as a verification device.

Van der Ploeg mentions that 'body data' such as what is used in biometrics is not limited to just identify someone, but rather a whole embodiment of both digital data and the physical body interacting together. As she says, "embodiment is central to individuality and identity in a way that my social security number or my car rental records are not" (2003:69). Here she refers to other physical things that make-up our identity, but are not part of our actual physicality, and instead part of our social identity. Thus according to her, biometrics are inexplicably linked to our physical identity. She argues that it is not just the fact that passwords and house keys can change and fingerprints can't, it is the fact that the body cannot be used for authentication without 'embodying' the body; without revealing identity.

While this thesis does not disagree with this notion, it does however argue that casual biometrics are possible in a certain discourse. In principle, biometrics will always have a relationship with identity no matter how removed it seems. However, if security is not a huge priority, then to return to some of the user comments, Touch ID is more of a deterrent to casual interactions. From friends checking your messages, or a wife checking your call log, a simple, easy, casual biometric reader suffices. But one must realise that even if the function is casual, the background is still surrounded in identity. It is therefore about finding a balance between the socially constructed identity and the technologically constructed nature of biometrics. It is about finding the balance between the human and non-human. And this balance differs from each context. It differs from identification and verification.

So has there been a discourse shift in the function of biometrics from identification to verification? Yes and no. Many functions are now possible in verification procedures through biometrics, removed from identification, but many of these are no less absent from identity as a password is. In fact, passwords have been more verifiers than identifiers since they begun. They have been utilized anonymously, with a password having very little tying to your social or physical identity. This then returns to the expectations of biometrics and how their convenience, security and privacy differ from the password, or physical keys, and whether biometrics are the 'key' to moving into a passwordless society.

The debate rages on, and the short answer is that with current technology, there is no full-proof way of having the trio of verification; security, convenience and privacy, without sacrificing in part at least one or the other. In casual settings, the fingerprint may be enough, but where Touch ID began its journey as such, Apple's push for it to be used in more secure applications, means that it is shedding its casual discourse already. It is still using verification, but through secure conscious environments, Touch ID is becoming less casual. Thus many commentators have argued two-factor

authentication seems to be the minimum standard for secure transactions in the future. This may well be the case, and the expectations looks to see biometrics increasingly taking part in such two-factor authentication through both verification, as well as identification. If biometrics becomes secure and accurate enough, perhaps two or three-factor biometrics alone will be the norm, away from physical or mental passwords, such as a fingerprint, voice recognition, and iris scanning all being simultaneously verified to grant access to something. Either way, the technology is only as good as the user and system that adapts to it. If past trends are to go by, both technology and society will continue to adapt and affect one another.

In conclusion, expectations are clearly no easy guide to the future. The paperless society still seems but a dream as does the cashless society. The more technology seems to push for change, the more society holds back, though simultaneously pushing forward at the same time. We fight for simplicity, yet can't help but be overcome by complexity. The passwordless society may be a long while away yet. While discourses may change and casual verification seems possible, overall it seems identity and biometrics seem forever intertwined together. Thus, just as paper and cash have done so in wake of their eulogies, the password seems destined to live on for many years to come.

12. Bibliography

Ackerman, S. (2013, April 9). *Now Your iPhone Can Read Fingerprints, Scan Irises and ID Your Face*. Retrieved June 14, 2013, from Wired: http://www.wired.com/dangerroom/2013/04/iphone-biometrics/

AOptix Technologies, Inc. (2012). *Revolutionizing Biometric Identity Verification*. Retrieved May 11, 2013, from Aoptix : http://www.aoptix.com/assets/docs/resources/Smart_Mobile_Identity_White_Paper.pdf

Apple. (2015). *Security and your Apple ID*. Retrieved April 2, 2015, from Apple: https://support.apple.com/en-us/HT201303

Belz, A. (2012, November 20). *As society sheds paper, an industry shrinks*. Retrieved April 2, 2015, from StarTribune: http://www.startribune.com/business/179601951.html

Biometrics Institute. (2013). *Biometrics Institute Technology Showcase Europe 2013*. Retrieved April 2, 2015, from Biometrics Institute: http://www.biometricsinstitute.org/events.php/472/biometrics-institute-technology-showcase-europe-2013

Bonnington, C. (2012, October 11). *Apple Patent Expands on Biometric Identification Implementations*. Retrieved June 06, 2013, from Wired: http://www.wired.com/gadgetlab/2012/10/apple-patent-biometric/

Bonnington, C. (2013), "The trouble with Apple's Touch ID fingerprint reader", *Wired,* December 4, London.

Borup, M., Brown, N., Konrad, K. & van Lente, H. (2006): The sociology of expectations in science and technology. *Technology Analysis & Strategic Management* 18 (3/4), 285-298.

Brown, N. & Michael, M. (2003). A Sociology of Expectations: Retrospecting Prospects and Prospecting Retrospects. *Technology Analysis and Strategic Management*, 15(1), 3-18.

Brown, A. (2004, September 23). *Biometrics: From Science Fiction to Practical Fact*. Retrieved April 2, 2015, from EHS Today: http://ehstoday.com/fire_emergencyresponse/ehs_imp_12454

Callon, Michel (1986) "Some Elements of a Sociology of Translation Domestication of the Scallops and the Fishermen if St Brieuc Bay", in Law, J. (ed.), *Power, Action and Belief*. *A New Sociology of Knowledge?* London: Routledge & Kegan Paul, pp. 196-233.

CCC. (2013, 09 21). *Chaos Computer Club breaks Apple TouchID*. Retrieved 02 27, 2014, from Chaos Computer Club: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

Clayton, R. B., Leshner, G., & Almond, A. (2015). The Extended iSelf: The Impact of iPhone Separation on Cognition, Emotion, and Physiology. *Computer Mediated Communication vol 20. no. 2* , 119-135.

Cole, Simon A. (1999): "What Counts for Identity? The Historical Origins of the Methodology of Latent Fingerprint Identification". *Science in Context*, Vol. 12, No. 1, 139-172.

Cole, S. A. (2002) Suspect Identities: A History of Fingerprinting and Criminal Identification. Boston: Harvard University Press.

Davies, S. (1994a), "Forget the Passport; Let's See Your Hand", *The Independent*, 15 August, London.

Davies, S. (1994b) *Touching Big Brother How Biometric Technology Will Fuse Flesh and Machine.* In Information Technology & People Vol. 7 No. 4, pp. 38-47.

Davis, A. (1997) *The Body as Password* . Retrieved April 19, 2013, from Wired: http://www.wired.com/wired/archive/5.07/biometrics_pr.html

Depetrillo, Nick (@NickDepetrillo). "I will pay the first person who successfully lifts a print off the iPhone 5S screen, reproduces it and unlocks the phone in <5 tries $100". 19 Sep 2013, 06:37 UTC. Tweet.

DesMarais, C. (2013, May 31). *Three great alternatives to two-factor authentication via text-message*. Retrieved June 14, 2013, from PCWorld: http://www.pcworld.com/article/2040436/three-great-alternatives-to-two-factor-authentication-via-text-message.html

DMI. (2015). *DMI Tools*. Retrieved April 2, 2015, from Digital Methods Initiative: https://wiki.digitalmethods.net/Dmi/ToolDatabase

Economist, The. (2002, October 24). *Biometric fact and fiction*. Retrieved April 2, 2015, from The Economist: http://www.economist.com/node/1389565

Economist, The. (2015, February 28). *Planet of the phones*. Retrieved April 2, 2015, from The Economist: http://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones

ezbordercrossing. (2015). *What They Know About You*. Retrieved April 2, 2015, from ezbordercrossing: http://www.ezbordercrossing.com/the-inspection-experience/what-they-know-about-you/#.VR05kfnQqSp

Fairclough, N. (2003). *Analysing discourse: textual analysis for social research.* London; New York: Routledge.

Feinberg, A. (2014, January 20). *The 25 Most Popular Passwords of 2013: God Help Us*. Retrieved February 28, 2-14, from Gizmodo: http://gizmodo.com/the-25-most-popular-passwords-of-2013-god-help-us-1504852434

Felt, Ulrike (2013) *Keeping Technologies Out: Sociotechnical Imaginaries and the Formation of a National Technopolitical Identity*; Pre-Print; Published by the Department of Social Studies of Science, University of Vienna, February 2013. Available at http://sciencestudies.univie.ac.at/publications

Foucault, Michel (1979) Discipline and Punish: the Birth of the Prison, Penguin, Harmondsworth.

Gonsalves, A. (2013, May 26). *Twitter's stronger security isn't bulletproof, experts warn*. Retrieved June 14, 2013, from Tech Hive: http://www.techhive.com/article/2039753/twitters-stronger-security-isnt-bulletproof-experts-warn.html

Heath, C. Hindmarsh, J. (2002) *"Analyzing Interaction: Video, ethnography and situated conduct"*, in May, T. (ed.), Qualitative Research in Action. London: Sage, pp. 99-121.

Home Office, (2004). Legislation on Identity Cards: A Consultation, Home Office.

Honan, M. (2012, November 15) *Kill the Password: Why a String of Characters Can't Protect Us Anymore*. Retrieved April 19, 2013, from Wired: http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/all/

Hussain, A. (2014). *How multimodal biometrics improves border control security*. Retrieved April 2, 2015, from BetaNews: http://betanews.com/2014/10/30/how-multimodal-biometrics-improves-border-control-security/

Imperva. (2012) *Consumer Password Worst Practices*. Retrieved April 19, 2013, from Imperva : http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

Jain, A., Hong, L., & Bolle, R. (1997). On-Line Fingerprint Verification. *Ieee Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 4,* pp. 302-314.

Jain, A. K., Dass, S. C., & Nandakumar, K. (2004). Can soft biometric traits assist user recognition? *SPIE Vol. 5404*, pp. 561-572.

Jain, A.K, Kumar, A. (2010) "Biometrics of Next Generation: An Overview" in *SECOND GENERATION BIOMETRICS,* East Lansing: Michigan State University, pp. 1-36.

Jain, S., Gupta, S., & Thenua, R. K. (2012). A review on Advancements in Biometrics. *International Journal of Electronics and Computer Science Engineering Vol. 1. No. 3*, pp. 853-859.

Jasanoff, S. (2004) "The Idiom of Co-production" & "Ordering Knowledge, Ordering Society", in Jasanoff, S. (ed.), *States of Knowledge. The Co-production of Science and Social Order,* London: Routledge, chap. 1, pp. 1-12, & chap. 2, pp. 13-45.

Johnson, J. [Latour, B.] (1988) "Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer", in *Social Problems*, *Vol. 35, No. 3, Special Issue:* The Sociology of Science and Technology pp. 298-310.

Kirby, D. (2010): The Future is Now: Diegetic Prototypes and the Role of Popular Films in Generating Real-world Technological Development. In: Social Studies of Science, 40(1), pp. 41-70.

Kuhn, T. (1962). *Structure of Scientific Revolutions.* Chicago: University of Chicago Press.

Kwek, G. (2013, April 27). *How a fake tweet sent stockmarket into free fall*. Retrieved May 11, 2013, from The Age: http://www.theage.com.au/business/how-a-fake-tweet-sent-stockmarket-into-free-fall-20130426-2ik0e.html

Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In W. L. Bijker, *Shaping Technology/Builiding Society* (pp. 225-258). London/Camebridge: The MIT Press.

Law, J. (1992) "Notes on the Theory of the Actor Network: Ordering, Strategy and Heterogeneity", Lancaster: Lancaster University, Centre for Science Studies, pp. 1-11.

Lianos, M., & Douglas, M. (2000). Dangerization and the end of deviance. *The British Journal of Criminology*, pp. 261-278.

Livingstone, D. (2003) *A Geography of Science?* In: Putting Science in Its Place. Geographies of Scientific Knowledge. Chicago/London: University of Chicago Press, pp. 1-16.

Lynch, M., Cole, S. A., McNally, R., & Jordan, K. (2008). *Truth Machine: Contentious History of DNA Fingerprinting.* Chicago: The University of Chicago Press.

Manjoo, F. (2013, June 6). *You Won't Finish This Article*. Retrieved April 2, 2015, from Slate: http://www.slate.com/articles/technology/technology/2013/06/how_people_read_online_why_you_won_t_finish_this_article.html

Marres, Noortje. (2011). The costs of public involvement Everyday devices of carbon accounting and the materialization of participation. Economy and Society, 40(4), pp. 510-533.

Martin, A. K., & Whitley, E. A. (2007). "Managing Public Expectations of Technological Systems A Case Study of a Problematic Government Project", in *Spontaneous Generations. 1*, pp. 67–77.

Martin, K. A. (2011). *Envisioning Technology through Discourse: A case study of biometrics in the National Identity Scheme in the United Kingdom*. Retrieved June 14, 2013, from LSE Thesis Online: http://etheses.lse.ac.uk/181/1/Martin_Envisioning_Technology_through_discourse.pdf

Megreya, A. M., & Burton, A. M. (2008). Matching faces to photographs: Poor performance in eyewitness memory (without the memory). *Journal of Experimental Psychology: Applied, Vol 14(4)*, pp. 364-372.

Nok Nok Labs Inc. (2013, February). *Authentication... and why it's not working*. Retrieved May 12, 2013, from Nok Nok Labs: https://www.noknok.com/sites/default/files/whitepapers/nnl_authentication_whitepaper.pdf

Oates, J. (2011, June 24) *NATO Site Hacked*. Retrieved April 19, 2013, from The Register: http://www.theregister.co.uk/2011/06/24/nato_hack_attack/

Olsson, M. (2007) Power/Knowledge: The Discursive Construction of an Author. *Library Quaterly*, 77 (2) pp. 219-240.

Pink, S. (2001). *Doing Visual Ethnography.* London: Sage.

Leeuwen, Theo van. (2005) *Introducing Social Semiotics*, New York: Routledge, pp. 94-104.

Perrot, D. (2013, October 18). *Does iPhone 5 TouchID Matter And Why*. Retrieved April 2, 2015, from InWebo: http://www.inwebo.com/blog/does-iphone-5-touchid-matter-and-why/

Ploeg, I. Van Der. (2003) "Biometrics and the body as information: Normative issues of the sociotechnical coding of the body". In D. Lyon, *Surveillance as Social Sorting,* London: Routledge, pp. 57-73.

Ploeg, I. Van Der. (2005) "The Politics of Biometric Identification Normative aspects of automated social categorization". *Biometric Technology & Ethics*, *no. 2*, pp. 1-16.

Ploeg, I. Van Der. (2011) "Biometrics and Privacy A note on the politics of theorizing technology, *Information, Communication & Society*, 6:1, pp. 85-104.

Ponemon Institute LLC. (2013, April). *Moving Beyond Passwords: Consumer Attitudes on Online Authentication*. Retrieved May 12, 2013, from Nok Nok Labs: http://go.noknok.com/rs/noknok/images/NokNokWP%20FINAL%202.pdf

Reid, D. A., & Nixon, M. S. (2011). Using Comparative Human Descriptions for Soft Biometrics. *Pattern Analysis and Machine Intelligence, IEEE Transactions on Biometrics Compendium Vol. 36 No. 6* , pp. 1216-1228.

Riffe, D., Lacy, S., & Fico, F. G. (2005). *Analyzing Media Messages: Using Quantitative Content Analysis in Research.* London: Lawrence Erlbaum Associates.

Rifkin, J. (2011). *The Third Industrial Revolution.* New York: Martin's Press LLC.

Rogers, R. (2013). *Digital Methods.* Cambridge: MIT Press.

S and Marper v United Kingdom [2008], 1581 (The European Court of Human Rights December 4, 2008).

Schneider, J. (2011, March 17). *Biometrics, Smartphones and the E-Wallet*. Retrieved April 19, 2013, from Ultra Scan: http://www.ultra-scan.com/Portals/16/BiometricSmartphonesforEcommerce.pdf

Selin, C. (2007): Expectations and the emergence of nanotechnology. *Science, Technology, & Human Values* 32 (2), pp. 196-220.

Sellen, A. J., & Harper, R. H. (2003). *The Myth of the Paperless Office.* MIT Press.

Steblay, N., Dysart, J., Fulero, S., & Lindsay, R. (2003). Eye Witness Accuracy Rates in Police Showup and Lineup Presentations: A Meta-Analytic Comparison. *Law and Human Behavior Vol. 27, No. 5*, pp. 523-540.

Townsend, A. (2013). *Smart Cities.* New York: W. W. Norton & Company, Inc.

Winch, J. (2013, July 8). *End of chip and Pin? Shoppers test payment by fingerprint*. Retrieved April 2, 2015, from The Telegraph: http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/10166776/End-of-chip-and-Pin-Shoppers-test-payment-by-fingerprint.html

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus, Vol. 109, No. 1, Modern Technology: Problem or Opportunity?*, pp. 121-136.

13. Empirical News Articles

13.1 The United States of America

WALL STREET JOURNAL

Apple's Latest iPhone Puts Focus Back on Fingerprint Security
September 9, 2013 19:45 ET – Danny Yadron
http://online.wsj.com/news/articles/SB10001424127887323864604579065440953246958 <last accessed 01/04/2015>

Apple: New iPhone Not Storing Fingerprints, Doesn't Like Sweat
September 11, 2013 15:08 ET - Danny Yadron and Ian Sherr
http://blogs.wsj.com/digits/2013/09/11/apple-new-iphone-not-storing-fingerprints-doesnt-like-sweat/ <last accessed 01/04/2015>

Avoid Touch ID, Says Kremlin Ally
September 23, 2013 12:25 CET – James Marson
http://blogs.wsj.com/emergingeurope/2013/09/23/avoid-touch-id-says-kremlin-ally/ <last accessed 01/04/2015>

THE WASHINGTON POST

The new iPhone might have a fingerprint scanner. That's a gamechanger for privacy.
September 10, 2013 13:19 – Brian Fung
http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/10/the-new-iphone-might-have-a-fingerprint-scanner-thats-a-gamechanger-for-privacy/ <last accessed 01/04/2015>

Fingerprint scanner for iPhone 5s raises privacy, security concerns
September 20, 2013 – Andrea Peterson and Hayley Tsukayama
http://www.washingtonpost.com/business/technology/fingerprint-scanner-for-iphone-5s-raises-privacy-security-concerns/2013/09/20/0992cbee-222f-11e3-966c-9c4293c47ebe_story.html <last accessed 01/04/2015>

ARSTECHNICA

Fingerprints as passwords: New iPhone Touch ID gets mixed security verdict
September 11, 2013 18:35 CEST – Dan Goodin
http://arstechnica.com/security/2013/09/fingerprints-as-passwords-new-iphone-touch-id-gets-mixed-security-verdict/ <last accessed 01/04/2015>

Bypassing TouchID was "no challenge at all," hacker tells Ars
September 24, 2013 21:03 CEST – Dan Goodin
http://arstechnica.com/security/2013/09/touchid-hack-was-no-challenge-at-all-hacker-tells-ars/
<last accessed 01/04/2015>
[Includes Video]

CNET

iPhone 5S fingerprint sensor: The end of passwords?
September 10, 2013 12:27 PM PDT – Zack Whittaker
http://www.cnet.com/news/iphone-5s-fingerprint-sensor-the-end-of-passwords/ <last accessed 01/04/2015>

Hackers claim to have defeated Apple's Touch ID print sensor
September 22, 2013 12:47 PM PDT – Steven Musil
http://www.cnet.com/news/hackers-claim-to-have-defeated-apples-touch-id-print-sensor/ <last accessed 01/04/2015>

13.2 The United Kingdom

THE GUARDIAN

iPhone 5S: would thieves *really* chop off your fingers to access it?
September 11, 2013 17.59 BST – Duncan Campbell
http://www.theguardian.com/technology/shortcuts/2013/sep/11/iphone-5s-thieves-chop-off-fingers <last accessed 01/04/2015>

iPhone 5s review: Apple shows its touch
September 18, 2013 14.51 BST – Charles Arthur
http://www.theguardian.com/technology/2013/sep/18/iphone-5s-review-apple <last accessed 01/04/2015>

iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club
September 23, 2013 08.50 BST – Charles Arthur
http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked <last accessed 01/04/2015>

THE TELEGRAPH

Apple iPhone 5S and 5C: fingerprint sensor and plastic make iPhone 5 debut
September 10, 2013 07:31 BST – Matt Warman
http://www.telegraph.co.uk/technology/apple/iphone/10300495/Apple-iPhone-5S-and-5C-fingerprint-sensor-and-plastic-make-iPhone-5-debut.html <last accessed 01/04/2015>

iPhone 5s fingerprint sensor 'hacked' within days of launch
September 23, 2013 09:33 BST – Sophie Curtis
http://www.telegraph.co.uk/technology/apple/iphone/10327635/iPhone-5s-fingerprint-sensor-hacked-within-days-of-launch.html <last accessed 01/04/2015>

V3

Touch ID fingerprint scanner makes iPhone 5S a safer bet for businesses
September 10, 2013 – Madeline Bennett
http://www.v3.co.uk/v3-uk/news/2293892/touch-id-fingerprint-scanner-makes-iphone-5s-a-safer-bet-for-businesses <last accessed 01/04/2015>

Hackers crack Apple iPhone 5S Touch ID fingerprint scanner
September 23, 2013 - Dan Worth
http://www.v3.co.uk/v3-uk/news/2296293/hackers-crack-apple-iphone-5s-touch-id-fingerprint-scanner <last accessed 01/04/2015>

THE REGISTER

iPhone 5S: Fanbois, your prints are safe from the NSA, claim infosec bods
September 12, 2013 09:05 BST - John Leyden
http://www.theregister.co.uk/2013/09/12/iphone_fingerprint_scanner_gets_cautious_thumbs_up_from_security_bods/?page=2 <last accessed 01/04/2015>

Chaos Computer Club: iPhone 5S finger-sniffer COMPROMISED
September 22, 2013 23:09 BST - Richard Chirgwin
http://www.theregister.co.uk/2013/09/22/iphone_5_touchid_broken_by_chaos_computer_club/
<last accessed 01/04/2015>

Jack Kerr - Curriculum Vitae

Tertiary Education:

Master of Arts: Science-Technology-Society (STS)

October 2012 – April 2015 (expected) University of Vienna, Austria

Master Thesis on the expectations of biometric technology as a mass market verification system using a media study through the iPhone 5S as a specific case

Other Modules included:

- The Emergence of New Research Fields
- Social Science Research Methods
- Grant Writing and Project Management
- Digital Methods

Bachelor of Arts in Communication (Writing and Cultural Studies)
2009 –2011 University of Technology, Sydney, Australia

Modules included:

- Regulating Communication: Law, Ethics, Politics
- Communication and Cultural Industries and Practices
- Creativity and Culture
- Communication Practice Project
- Understanding Communication
- Contemporary World Cinema

Global Exchange Program (German Language Studies and English Literature)
September 2010 – February 2011 University of Konstanz, Germany

Secondary Schooling:

2003 – 2008 Holy Cross College, Ryde, Sydney
High School Certificate (HSC) Electives: English Extension 1, Mathematics, English [Advanced], Modern History, Extension History

Languages:

English: Native Speaker
German: CEFR Level C1/1