Information, Security, Privacy, and Anonymity:

Definitional and Conceptual Issues

Björn Lundgren

Doctoral Thesis in Philosophy
KTH Royal Institute of Technology
Stockholm, Sweden, 2018
Abstract


This doctoral thesis consists of five research papers that address four tangential topics, all of which are relevant for the challenges we are facing in our socio-technical society: information, security, privacy, and anonymity. All topics are approached by similar methods, i.e. with a concern about conceptual and definitional issues. In Paper I—concerning the concept of information and a semantic conception thereof—it is argued that the veridicality thesis (i.e. that information must be true or truthful) is false. In Paper II—concerning information security—it is argued that the current leading definitions suffer from counter-examples, and lack an appropriate conceptual sense. Based on this criticism a new kind of definition is proposed and defended. In Paper III—concerning control definitions of privacy—it is argued that any sensible control-definition of privacy must properly recognize the context as part of the defining criteria. In Paper IV—concerning the concept of privacy—it is argued that privacy is a normative concept and that it is constituted by our social relations. Final, in Paper V—concerning anonymity—it is argued that the threat from deanonymization technology goes beyond harm to anonymity. It is argued that a person who never is deanonymized can still be harmed and what is at stake is an ability to be anonymous.

Keywords: definitions; distinctions; conceptual analysis; philosophy of information; philosophy of risk, security; information; information security; semantics; semantic information; veridicality thesis; informativity; appropriate access; CIA; privacy; control; context; pro tanto good; social relations; anonymity; deanonymization; ability to be anonymous
Thesis composition

This doctoral thesis consists of an introduction and the following research papers:


III. Björn Lundgren (under review) “Privacy as a Relational Concept”.

IV. Björn Lundgren (under review) “A Dilemma for Privacy as Control and Why the Context Matters”.

V. Björn Lundgren (under contract for publication) “Beyond the Concept of Anonymity: What is Really at Stake?” In K. Macnish and J. Galliot Big Data and the Democratic Process.

TRITA-ABE-DLT-1811.
© 2018 by Björn Lundgren.

* Paper I and II are reproduced here with kind permission from Springer Science+Business Media B.V., under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The versions in this thesis have been adapted to the style of the thesis, which also includes changes such as the placement of acknowledgment and copyright information, style of reference, and numbering of headings. The funding note is also removed (see acknowledgement). Both papers also include some corrections (see the added errata note for each paper).
Table of contents

Abstract ................................................................................................................................. 2
Thesis composition .......................................................................................................... 3
Acknowledgement ........................................................................................................... 7
Svensk sammanfattning .................................................................................................. 9
Introduction ...................................................................................................................... 13
  1. Introducing the introduction ................................................................................. 13
  2. Methodology ........................................................................................................... 16
  3. Themes ................................................................................................................... 26
  4. Future research ..................................................................................................... 50
Appendix: Definitions .................................................................................................... 56
References ...................................................................................................................... 67

Does Semantic Information Need to be Truthful? ......................................................... 73
Abstract ............................................................................................................................. 73
  1. Introduction ............................................................................................................. 73
  2. Background and specification ............................................................................. 75
  3. A liar paradox for a veridical conception of semantic information .......... 81
  4. Is false information genuine information? ......................................................... 83
  5. Must information be informative? ....................................................................... 89
  6. Conclusions ........................................................................................................... 97
Appendix: Further arguments on the information liar paradox ......................... 98
References ...................................................................................................................... 107

Defining Information Security .......................................................................................... 113
Abstract ............................................................................................................................. 113
  1. Introduction ............................................................................................................. 115
  2. Counter-examples to the CIA definition ............................................................. 120
  3. The Appropriate Access definition ..................................................................... 129
  4. Further arguments for the AA definition ............................................................. 140
Acknowledgement

I wish to thank my supervisors Niklas Möller and Sven Ove Hansson for giving me the opportunity to write this doctoral thesis and for helpful criticism and encouragement during the process (and thanks to Niklas, again, for co-authoring Paper II with me).

I also wish to thank the members of the SECURIT research program, which this thesis research was a part of, and The Swedish Civil Contingency Agency (MSB) for funding SECURIT and my Ph. D. SECURIT—Security Culture and Information Technology—is a research program addressing issues relating to information security culture. The program encompassed nine research projects, which included over twenty researchers from various research fields and institutions.¹ Amongst these researchers, I would especially like to thank Jonas Hallberg, Peter Johansson, Fredrik Karlsson, Ella Kolkowska, Teodor Sommestad, and Marianne Törner.

The introduction to this thesis and most of the papers has been presented at the research seminars at the Division of Philosophy. I want to thank John Cantwell and Tor Sandqvist who have chaired the seminars in philosophy (and thanks to John, again, for serving as the internal reviewer for this thesis). I also want to thank Linda Schenk who chaired the seminars in risk, safety, and security, before I took over that responsibility. I am grateful for the comments I have received from my colleagues during these seminars. During my time at the division of philosophy these two seminars have been attended by people such as: Jesper Ahlin, Patrick Baard, William Bülow, John Cantwell, Karin Edvarsson Björnberg, Robert Erdeniz, Barbro Fröding, Henok Girma Abebe, Till Grüne Yanoff, Sven Ove Hansson, Karim Jebari, Jesper Jerkert, Payam Moula, Niklas Möller, Björn Nevhage, Maria Nordström, Maria

Tor Sandqvist, Linda Schenck, Karl Sörenson, Anna Wedin, Sofia Wikman, Per Wikman Svahn, and Li Zhang.

There are more people that deserve to be acknowledged; separate acknowledgements are included for each of my individual papers. Lastly, I like to thank Betty Jurdell—who is the administrator at the Division of Philosophy—for making everything behind the scenes run smoothly. I also want to thank the rest of my colleagues, not previously mentioned, as well as friends and family.

Finally, I dedicate this thesis to my two nieces: Lovisa and Kerstin.
Svensk sammanfattning


Artikel 1 rör frågan om vad information är, specifikt givet en semantisk förståelse av information eller sådan information som begreppsligt är av en semantisk natur.

Artikeln kritiserar *the veridicality thesis* (ungefär: sanningstesen) som förfäktas av bland andra Luciano Floridi. Tesen innebär att (semantisk) information måste vara sann/sanningsenlig.


Informationssäkerhetsbegreppet är mångtydig, det kan åsyfta exempelvis informationssäkerhet som praxis eller som akademiskt ämne. Vi har fokuserat på att definiera när någon information eller något informationssystem är säkert (skyddat).
Vi kritiserar den klassiska definitionstypen – så kallade CIA definitioner. CIA står för de tre egenskaperna *confidentiality* (konfidentialitet), *integrity* (riktighet) och *availability* (tillgänglighet).²

I artikeln lägger vi fram några motexempel till varför dessa kriterier varken kan vara nödvändiga, tillräckliga eller ge oss begreppets mening på ett adekvat sätt. Vi föreslår sedan följande definitioner:

Säker information:

Informationen I är säker för intressenten H om, och endast om, för varje agent A gäller att A har rätt accessrelation till varje del av I, relativt H.

Säkert informationssystem:

Informationssystemet S är säkert för intressenten H om, och endast om, för varje agent A gäller att A har rätt accessrelation till varje del av S, relativt H.


² De svenska översättningarna som brukas ovan är vanligt förkommande (se t.ex. SOU 2015:23). De kan dock kritiseras (se, exempelvis, Lundgren 2015a, 2017).
Den senare och längre av de två artiklarna (artikel 4) innehåller mitt personliga bidrag rörande hur man bör begreppsliggöra och definiera privatitet, medan den kortare artikeln (artikel 3) innehåller en del av de argument mot alternativa begreppsliggöranden som inte fick utrymme i den längre artikeln. I huvudsak kan sägas att jag argumenterar för rimligheten för tesen att privatitet är ett värde som är *pro tanto* gott, vilket ska förstås som att den är *prima facie* bra/dåligt att ha mer/mindre privatitet. Privacitet förstås således som något gott som man kan ha mer eller mindre av. Givet denna premiss (vars rimlighet jag först etablerar för att sedan låta begreppsliggörandet av privatitet fungera som ett ytterligare pro-argument för), argumenterar jag för att privatitet ska förstås som att det är konstituerat av våra sociala relationer. Specifikt analyserar jag villkoren för hur mycket av det goda värdet privatitet som något har, vilket jag definierar på följande sätt:

\[ A \text{ har privatitet för privatsaken p relativt till B till den grad B:s tillgångsrelation till p inte är olämplig i kraft av Az:s och B:s sociala relation.} \]

Som synes har definitionen ovan uttryckts i form av vilka kriterier som minskar någons privatitet. Skälen för detta utgörs bland annat av att privatitet förstås som ett *pro tanto* gott, vilket gör det relevant att definiera under vilka villkor—och till vilken grad—någons privatitet minskas relativt ett optimalt tillstånd.

Definitionen ska förstås med avseende på att någons tillgång till dina privatsaker (t.ex. information om dig eller din kropp) påverkar din privatitet (förstådd som något som är *pro tanto* gott) negativt beroende på vem och under vilka omständigheter denna person får tillgång till dina privatsaker. Ett exempel som illustrerar rimligheten bakom denna tes är skillnaden mellan att tillgängliggöra något ur vårt privatliv med någon som vi har en intim relation med och tillgängliggöra det samma för en arbetskollega.

Artikel 5 fokuserar på begreppet anonymitet. I huvudsak argumenteras det för att vi inte bör fokusera på begreppet anonymitet utan på förmågan att vara anonym. Det senare begreppet svarar nämligen
rimligare mot de utmaningar vi möter i samhället genom informations-aggregation och avanonymiseringstekniker. Vår förmåga att vara anonym förstås i detta sammanhang som vår förmåga att ha en rimlig kontroll över vad vi kommunicerar.
Introduction

1. Introducing the introduction

After the industrial revolution, the socio-technical society has evolved. For the last fifty years or so, one of the most expansive societal changes concerns the transfer of information. With the increased power and presence of digital technology, this trend has increased. Although it is hard to pinpoint precisely when it happened, it is fair to say that we are in an ‘information society’. The information society, especially in the Internet-age, poses various challenges to humans and humanity (i.e. both individually and collectively). The purpose of this doctoral thesis is to address some such challenges by introducing and defending philosophical accounts relating to four central topics or themes for the informational society and its challenges: the concepts of information, security, privacy, and anonymity. While the contribution of the thesis is about fundamental conceptual issues and as such relate to an enormous variety of questions, the below three categories of questions can serve as illustrative examples of the importance of the four topics:

- *In the era of ‘false news’ the thesis addresses questions such as:* What is information? Specifically, what is semantic information? Does it require truth? That is, is false information information? Is information necessarily informative?
- *In an era of hacking, informational leakage, and security risks, the thesis addresses question such as:* What does it mean that some information is secure? Which conditions must be satisfied for some information (or information system) to be secure?
- *In an era of Cambridge Analytica, NSA, Google, and Facebook the thesis addresses question such as:* What is privacy? Is privacy important? Is it valuable? What about anonymity: is it also important? What are the threats from information aggregation and deanonymization technologies? What concept is most suitable in order to analyze such challenges?
In response to these questions, the aim is to contribute with improved analysis, conceptions, and concepts relating to the four themes. Simply put the aim is to contribute with the best possible analyses of the most relevant concepts (relating to the four themes). For example, in several of the articles, I show how improved conceptions or new concepts can resolve previous problems and counter-examples, or I show that old concepts cannot address the current challenges and—in response—I suggest new concepts or conceptions to resolve this. Better conceptions and concepts are important since they allow us to better analyze reality using new or improved categories. This, in turn, increases our ability to deal with, or approach, problems of both a theoretical and practical nature. This is because concepts and conceptions supply the most fundamental tools for all other analysis. Thus, the aim of this thesis is to provide such fundamental tools.

The purpose of this introduction is to supply a relevant contextual basis for these topics, as they are presented in my papers. Furthermore, the purpose is also to provide some background for readers who are not familiar with all relevant aspects of the philosophical approaches to conceptual analysis and definitions—and, for those who are, I aim to present my approach to conceptual analysis and definitions, as I have applied it in my thesis. To help the reader, I will also provide explanations of relevant terms as the Introduction proceeds (to avoid over-loading the text with explanations these are often added in a footnote or within parentheses). However, since many terminological or technical issues concern definitions as such, an Appendix, which presents a brief over-view of this topic, have been added (it also

---

3 The concept-conceptions distinction is not without complication. I will use these terms in a very simplified manner in this introduction. For example, information, privacy, and anonymity are different concepts. Each of these concepts can be conceptualized in various ways, which implies that there can be more than one conception of a concept. Often philosophers agree on what the important concept is—e.g., privacy—but disagrees on how it ought to be conceptualized—e.g., in terms of control or limited access. Of course, sometimes philosophers also disagree about which concept that is the important one—e.g., privacy or the right to privacy.
includes some brief comments on what kinds of definitions I apply in my papers).

In this thesis, you will find five research papers with a varied intended readership, dealing with different subject matters. Despite their differences, the essays are interconnected through both their themes and method. The thematic and methodological connections between the papers are quite clear; all papers discuss or contribute to conceptual analysis and definitions of relative to the papers inter-related topics. Paper I discusses whether the criterion of truth (or truthfulness) is necessary for semantic information. Paper II supplies a definition of when some information (system) is secure. Paper III addresses a dilemma for so-called ‘control definitions’ of privacy. Paper IV proposes a definition of privacy, conceptualized as a \textit{pro tanto} good, and constituted by our social relations. Last, Paper V addresses conceptual issues concerning the concept of \textit{anonymity}, arguing that the relevant concept to define is \textit{the ability to be anonymous}, and it proposes how to define that concept.

The remainder of this introduction will be structured as follows. First, in chapter 2, I will discuss the methodological basis for this thesis. Next, in chapter 3, I will deal with the four themes; each section will include a brief summation of some of the main points of the papers, as well as a minor contextualization of the topics. After this, in chapter 4, this introduction will end with some brief concluding remarks on possible future research. Finally, you will find the mentioned appendix, which introduces some fundamental technical and terminological aspects concerning definitions. After this, the papers will follow.
2. Methodology

The basic method—if we can talk of ‘method’ in philosophy—applied in all five papers is conceptual analysis (or simply: analysis). Conceptual analysis is about how we carve out reality. A minimal requirement of any conceptual analysis is that it addresses what kind of concepts we need to be able to meaningfully talk about and address issues of concern. My analysis goes beyond such a minimal requirement and asks which concepts are the most relevant and which are the best conceptualizations thereof.

Conceptual analysis often uses definitions in two ways (or, at least, I do). First, definition(s) or definitional criteria are often the result of conceptual analysis. In all of the papers of this essay I either try to give a satisfactory response to the question what is the definition of $x$?, I argue that $c$ is (not) a necessary criterion for $x$, or I argue that $y$ is not the concept we should focus on. Second, definitions serve as part of the method of conceptual analysis. Definitions offer a way to test possible conceptions because they offer—if used correctly—a clear and precise formulation of the concepts or conceptions that can be tested against possible examples and counter-examples. Thus, definitions both serve to present the result of and as part of the method of conceptual analysis.

Below, in section 2.1, I will aim to explain how I approach conceptual analysis as a normative endeavor (i.e. aiming to provide the best possible conceptions of the most relevant concepts). Next, in section 2.2., I aim to explain what makes one conception better than other conceptions or one concept more relevant than other concepts. After that, I turn to explain the role of definitions for conceptual analysis, in section 2.3, and the role of distinctions for conceptual analysis, in section 2.4. That ends the method chapter. However, as previously mentioned, in the appendix you will find an expanded discussion concerning definitions (which goes through some elementary technical and terminological issues, beyond section 2.3).
2.1 Conceptual analysis as a normative endeavor

Conceptual analysis can be explained in various ways. I will explain it in a way that makes sense given what I have done in my papers. As such, there will be a strong focus on definitions. More importantly, despite what I said above, there are various competing views on conceptual analysis. One view, which goes back to Plato and the earlier natural philosophers, is that conceptual analysis is about revealing deep truths about reality, that is: carving nature (or an abstract reality) at its joints (cf. *Phaedrus* 265c-266a in Plato 1997: 542).

This relates to so-called real definitions. According to Richard Robinson (1950) a real definition is a thing-thing definition—in comparison to word-word and word-thing definitions—that is, a real definition is a definition of a thing in terms of another thing. However, despite their prominent role in philosophy, real definitions have also been heavily criticized in various ways. Many philosophers find the concept of real definition confusing and flawed. As Gideon Rosen (2015), notes “[g]enerations of analytical philosophers were taught: it is a category error to ask for the definition of a non-linguistic thing” (p. 189). According to Robinson real definitions are an empty class. He argues that there are many activities or things that have been confused with real definition (e.g., analysis), but none of which are definitions. Others think that philosophy is about real definitions (see, e.g., Bernadete 1993, Rosen 2015, both which provide defenses of real definitions, see also Lundgren [2016: 30-35] for a brief defense of real definitions).

Because of the controversy over real definitions, I will leave that issue aside (see Appendix B for some further discussion on the topic). Thus, while it is not unreasonable to read my papers and think that I attempt to carve at the joints of nature (or an abstract reality), it is much less controversial to think of what I do as involving a normative analysis. More importantly, I believe that I can give an account of what I do that retains the merit of real definitions while avoiding any metaphysical or epistemic worries. The attractiveness of real definitions is that they give an account of how things really are. While I hope that I
reveal genuine truths in my papers, what I do can—and should—be viewed as purely normative: I aim to present the best possible conceptions or definitions of the most relevant concepts (in the given context).

A virtue of this approach is that it ought to be attractive both to those who believe and those who do not believe in real definitions. Those who do not believe in real definitions only have to accept the possibility of a normative ordering of concepts, conceptualizations, and definitions (given a distinct purpose). Conversely, if there are real definitions, then those definitions ought to be the best possible definitions (of the most relevant concepts). Thus, this approach ought to satisfy both believers and non-believers in real definitions. Of course, whether I have succeeded with this ambitious aim remains to be evaluated. However, before turning to this question, we must first address what it means to supply the best possible definitions or conceptions (of the most relevant concepts) and the method aimed at achieving this goal.

2.2 Best possible definitions and most relevant concepts

To give a complete account of criteria for when a conception or definition is better than other conceptions or definitions and which concept that is most relevant to define is beyond this thesis. Instead, I will present a few important criteria, complemented by illustrative examples from my papers. However, we first need to consider two distinctions relating to the concept-conception distinction (cf. fn. 3, p. 14). On the one hand, when we discuss what the best possible conception or definition is, then we are concerned with competing conceptions of the same concept (i.e. we are concerned with situations when the proposal of one conception competes with and aims to replace other conceptions). For example, in a particular discussion we may agree that the relevant concept is semantic information, but disagree about how it ought to be defined. On the other hand, when we discuss what the most relevant concept is, then we are concerned with
what kind of concept that is most relevant to focus on. Saying that one concept is more important than another does not necessarily mean that one should replace or remove the other concept from the terminology. Rather, what it means is that, in the relevant context, this, rather than that, is the concept that we need and/or should use. This distinction is not necessarily mutually exclusive. Indeed, a conceptual discussion often addresses both issues in tandem. For example, in Paper I semantic information is re-defined so that it includes non-informative information. This also implies that if we focus on informative information, we necessarily focus on another concept. Based on the above-explained distinction, three important evaluating criteria are introduced and discussed below.

**Counter-examples.** Concerning two competing conceptions of a concept, a conception C₁ is, *ceteris paribus*, better than another conception C₂ if C₂ suffers from counter-examples. A discussion of counter-examples presupposes either that we have a sufficient agreement about the extension (or intension)⁴ of a concept (i.e. that analysis does not start from scratch) or that we can supplement our counter-examples with arguments whenever there is disagreement. Counter-examples usually comes in two forms, they attack either the necessity or the joint sufficiency of the criteria of a conception. For example, in Paper II it is argued that the leading definition of information security fails to define when some information is secure because it's criteria are neither necessary (making it the case that secure information is classified as insecure), nor jointly sufficient (making it the case that insecure information is classified as secure). Counter-examples of both kinds are discussed in most of the papers. Furthermore,

---

⁴ The extension of a concept refers to all objects that fall under that concept. For example, the extension of *horse* is all horses. In comparison, the intension of a concept refers to the meaning or essence of the concept. It is often the latter that we aim to capture by conceptual analysis (e.g., by defining precisely which properties x must have in order to be y). But we often use the former to test the latter (i.e. the extension of an object often serve as a counter-example to a proposed analysis of the intension, showing that it does not properly define a concept so that it correctly includes those objects that should fall under it).
counter-examples can be used both against the extension and the intension of the proposed definition (cf. fn. 4, p. 19). For example, in Paper II, the standard definition of information security is criticized using counter-examples that aim to show that it gives the wrong meaning of the concept of security (confusing the state of security with possible consequences of an attack against an insecure system). The aim of many of the main concepts, conceptions, and definitions that I propose is that they should be free from both actual and possible counter-examples and that they should also have the right sense (see p. 61f). For example, in Paper II it is argued that information (system) security cannot be defined by a list of properties, but ought to be defined in terms of what counts as appropriate access. Appropriate access is determined relative to the needs of a stakeholder. As such, appropriate access will relate to any possible needs, avoiding both actual and possible counter-examples (see 3.2.4 for a brief explanation of the definition), while also providing the right sense (or analysis) of the concept.

Conflation. Concerning two competing conceptions of a concept, a conception $C_1$ is, \textit{ceteris paribus}, better than another conception $C_2$ if $C_2$ conflates two distinct concepts. This is standardly seen as a problem. However, whether a conception (or a concept) is a conflation, or not, is often a topic for discussion. More importantly, it can be debatable whether a conflation matters (i.e. whether a distinction is important or not). For example, in Paper I it is argued that proponents of the veridicality thesis have conflated the concept of information with the concept of informativity (i.e. they have conflated the information with informative information). It is argued that disentangling these properties is an important part in resolving potential counter-examples against an alethically neutral conception of semantic information.\footnote{I will explain this concept in section 3.1, when I present the details of Paper I.}

Purpose. Concerning two competing concepts, in a given context, a concept $C_1$ is, \textit{ceteris paribus}, preferable to another concept $C_2$ if $C_1$ serves a given purpose, in the given context, better than $C_2$. Arguably, this is a
vague criterion. However, an illustrative example can be found in Paper V. In the paper, it is argued that while previous conceptions of anonymity may be fair—given a common sense understanding of the concept of anonymity—anonymity is not the concept that we ought to focus on given what is at stake (which is harm from deanonymization technologies). Instead, it is argued that there is a broader concept, which I call our ability to be anonymous, that covers more relevantly the possible harms that can follow from deanonymization technologies. Furthermore, in Paper IV it is argued, on the one hand, that a normative conception of privacy is useful beyond (i.e. without replacing) the concept of the right to privacy. On the other hand, it is also argued (or implied), that a normative conception of privacy ought to replace a descriptive conception of privacy.

We can judge a concept, conception, or definition by many other qualities; I will expand on it in the sections below (and, to some extent, in the Appendix).

2.3 The role of definitions in analysis

I have already indicated and discussed the fundamental role of definitions in conceptual analysis. We may specify this role by asking what the specific value of definitions are and when they are valuable (supposing that everything is not worthy of definitional analysis).

Let us begin with the former question: What a definition does, irrespective of its kind, is—if it is successful—to supply a special form of clarification of a concept. If you have a theory about, e.g., information, then a definition of information offers, relative to your theory, a clarification of the scope of your conception of information. For example, given such a definition, the question of what actually belongs to the extension of the concept—supposing its formal rigor—ought to be clear. It, thus, becomes easier to reason about potential counter-examples to your theory, and as such, it becomes clear when further arguments are needed.
The value of definitions does not end with that since just as the extension of a concept can be used to evaluate a definition, a convincing definition can be used to evaluate a concept's extension.\(^6\) It should be noted that this not an empty circle of analysis, for the relation is—or should be—that of mutual explication until it reaches equilibrium: definition \(\equiv\) extension.\(^7\) Of course, as before, arguments are needed to support each modification of the definition/extension. The question of the balance between the supposed extension of the terms and the extension according to the definition is not easily settled; and it is not to be further discussed here. Either way, a definition helps us to clarify and identify (1) that there is a conflict, and (2) the (precise) nature of that conflict (e.g., relative to the evaluating, or quality, criteria that were discussed in 2.2).

So definitions may be motivated by a need, or desire, to clarify what it is that we talk about when we talk of x. This brings us to the related question: which concepts should we analyze and/or define? Just because analysis and definitions can help to clarify conceptual issues it is not clear that all conceptual issues are worthy of discussion—and therefore it is not clear that all clarifications are worthy of consideration. Consider, e.g., information—which subclasses of information are worthy of definitions? Now, there are many subclasses of information that we could define, e.g., we could make a definition of a subclass such that all information that can be expressed in English using only 47 letters will hence be known as ‘E47-information’. However, a general principle for giving definitional and analytic attention to a specific distinction, or

\(^6\) What I said above is a simplification that requires further clarification. For example, in first order predicate logic what makes a formula satisfiable is clearly defined. However, there is no generalizable method for determining whether any formula is satisfiable or not. Thus, what I said above should not be interpreted as indicating that the clarity that definitions can bring will allow us to determine the extension of any concept using only mechanical methods; thinking it still needed.

\(^7\) When I talk about equilibrium between definition and extension, I mean something stronger the Rawlsian notion of reflective equilibrium (see, e.g., Daniels 2018 for an introduction to the concept of reflective equilibrium). The theoretical goal is that the definition should be optimal in relation to all possible considerations. This includes aspects relating to the intension or sense of the concept.
subclass, should be that it would be of some (philosophical) interest to do so (i.e. either the subclass or the demarcation of that subclass, needs to be of some [philosophical] interest). Clearly, E47-information would neither supply us with an interesting subclass, nor with an interesting demarcation. This relates to the issue of purpose and illustrates why the purpose—in itself—must be analyzed. In practice, of course, many philosophical debates already address a distinct problem and the relevant concepts therefore often have a pre-defined purpose. However, as philosophers, we should never take that pre-defined purpose for granted. In some of the papers in this thesis, I aim to re-define such a purpose. The most illustrative examples are probably Paper IV and V (as already exemplified). However, it is also evident in Paper I, e.g., when it is argued that the property of being informative is distinguished from the property of being information, we could say that there is a conflation not only of concepts but of purpose.

The role of definitions are thus to help the analysis and—as previously noted—in the end, to present the result of the analysis in a precise manner. Thus, to ask why we should care about definitions (and distinctions) is to ask why we should care about conceptual analysis. However, we also need distinctions, so to this issue we now turn.

2.4 The role of distinction in analysis

The role of distinctions in conceptual analysis is essential: for to say anything about anything, we need to be able to distinguish one thing from other things. In order to discuss the relation between distinctions and analysis, I will start by addressing a mistake. The mistake is to suppose that since analysis requires distinctions and result in a definition, we should conclude that distinctions supply defining criteria. This confusion can be found in various applications of the Aristotelean

---

8 It should be noted that I am not conflating analysis with definitions or defining (as Robinson [1950] claimed that many have done when it comes to so-called 'real definitions'). What I am saying is that when we embark on a goal of analyzing a certain concept, we often express the result of such an analysis by a definition of the analyzed concept.
system of classification. For example, in Porphyry’s *Isagoge* (*Introduction*), a text that is mainly an introduction to Aristotle’s predications. The *Isagoge* explains the Aristotelean system of classification, in which a *genus* (a fundamental object) is subdivided into *species* (parts of a genus distinguished from each other by dichotomous properties). One species (such as animal) can be a genus for another species (such as man). Men, as a species, however, are not a genus for anything, but under it are only *individual* men (such as Plato, or Socrates). While Porphyry recognizes that there are different ways in which one thing can differ from another and that some differences can be accidental, he still argues that:

divisive differences of genera are found to be completive and **constitutive of species**. (Porphyry 2006: 10, 10:9-10, my bolding).

The idea here is that part of what distinguishes one kind from another also gives us necessary criteria for that kind. However, this is not necessarily the case. For example, the distinction in Paper I between informative and non-informative information, says nothing about how these concepts ought to be defined.

Nevertheless, distinctions are central in philosophy and are fundamentally necessary for definitions in the sense that if we cannot distinguish one thing from another, then—epistemically—there is nothing for us to define (even if there may be something there, ontologically). Thus, the role of distinctions—in this context—has to

---

9 In the *Isagoge* Porphyry aimed to introduce the fundamental logic of the old masters, mainly in the form of Aristotelian predications. However, the standard scholarly interpretation seems to be that Porphyry thought that Plato and Aristoteles were pretty much in agreement: Porphyry’s “writings on Aristotle’s logical works [...] contain attempts to harmonize Aristotle’s logical writings with Platonism” (Emilsson 2015). Note that I am not mentioning the *Isagoge* because I believe it to be the most excellent interpretation of Aristotle’s predications; on this I am silent. Rather, I use it as an example because it serves my purposes well and because it was an extremely influential text, serving “as a standard introductory text [to philosophy] in Byzantium, the Arabic world and in the Latin West through Boethius’ translations and commentary [...] for at least 1000 years” (Emilsson 2015, cf. Barnes 2006: ix).

10 Ontology is the study of what there is, while epistemology is the study of knowledge and belief. Something can exist, even if we fail to know that it exists. Thus, in the
do with providing base-concepts for us to define (i.e. it provides the basis for the definiendum). As such, it is both the start of analysis and a partial result of the analysis. Distinctions serve to help us avoid conflation of both concepts and (when applied to it) defining criteria. In this three-part effort, a definition can be viewed as the semi-formalization of the result of the analysis. However, as previously noted this process is cumulative: analysis starts with distinctions and results in a definition; the definition is then scrutinized, requiring more analysis, further distinctions, and new definitions; until—hopefully—one ends up with a final, superior—or, at least, satisfactory—definition.

That completes the method chapter (although the appendixes on definitions remain). Now, we turn to the four themes of the thesis.

---

11 Definiendum is the part of a definition that contains the term or concept that is defined. See Appendix Part A and Part B, especially p. 56f.
3. Themes

In this chapter, I address the four themes of the thesis: information, security, privacy, and anonymity. For each topic, I aim to—by a varying degree—provide some background and context as well as brief summations of the papers. Part of this chapter is of lesser interest to those readers that intend to read the papers (given that a large part of the sections serves to summate the papers). Section 3.1 and 3.3 offer the most interesting additions to the upcoming papers, while section 3.4 is, more or less, a brief summation. Below I will discuss the topics in the following order: information (3.1), security (3.2), privacy (3.3), and anonymity (3.4).

3.1 Information

In my first paper, I discuss the concept of information, specifically in the context of a semantic conception of information. In this section, I will start to give a brief background to the topic (3.1.1). Next, I will address the relevant issue of whether or not the concept of semantic information is worthy of studying (3.1.2). Last, granted that it is worthy of studying I will turn to a brief summation of the arguments found in the paper—relative to the question of how we ought to define the concept of semantic information (3.1.3).

3.1.1 Background and context

The concept of semantic information was introduced by Bar-Hillel and Carnap in the 1950s (see Bar-Hillel & Carnap 1964 and Bar-Hillel & Carnap 1953). It was introduced in a context dominated mainly by approaches to information that viewed semantic issues as non-issues (semantic issues broadly relates to questions of meaning in language). A central contribution was their analyses of how informative some information is. According to Bar-Hillel and Carnap, the less probable a statement is, the more informative it is. Thus, there is an inverse relation between the informativity and probability of some information. That this is a sensible analysis can easily be illustrated if you consider that
providing more information standardly imply that we exclude options. For example, saying that I am 33 years old excludes more options about my age—and, hence, makes it less probable and more informative—than saying that I am between 25 and 45 years of age.

In the last twenty years or so the notion of semantic information has been re-actualized, especially by Luciano Floridi; who—contrary to Bar-Hillel and Carnap—argued for the veridicality thesis (i.e. that [semantic] information must be true, or truthful). In the first paper, I focus on debunking this thesis, arguing in favor of an alethically neutral conception of semantic information.

According to Floridi, semantic information is “the kind of information which is essential for epistemic purposes” (Floridi 2011: 82). Another way to characterize semantic information is as ‘propositional information’ (i.e. in the sense that semantic information is the kind of information that we can assign truth-values to). These characterizations may be compared with what Floridi calls environmental information (e.g., rings on tree trunks, see Floridi 2011: 91f).

The concept or conception of semantic information may also be compared with other kinds of conceptions or concepts of information. According to Pieter Adriaans (2013), there are at least six types (whether these are conceptions of the same concept or different concepts is prima facie12 a topic of discussion):

1. **Fisher information**: the amount of information that an observable random variable $X$ carries about an unknown parameter $\theta$ upon which the probability of $X$ depends (Fisher 1925).

2. **Shannon information**: the entropy, $H$, of a discrete random variable $X$ is a measure of the amount of uncertainty associated with the value of $X$ (Shannon 1948; Shannon & Weaver 1949).

---

12 *Prima facie* is Latin for at first sight. It is used in that literal meaning, but also to indicate that the thing that holds *prima facie* (i.e. at first sight) can be trumped by other considerations.
3. **Kolmogorov complexity:** the information in a binary string $x$ is the length of the shortest program $p$ that produces $x$ on a reference universal Turing machine $U$ (Solomonoff 1960, 1964a,b, 1997; Kolmogorov 1965; Chaitin 1969, 1987).

4. **Quantum Information:** The qubit is a generalization of the classical bit and is described by a quantum state in a two-state quantum-mechanical system, which is formally equivalent to a two-dimensional vector space over the complex numbers (Von Neumann 1955; Redei & Stoeltzner 2001).

5. **Information as a state of an agent:** the formal logical treatment of notions like knowledge and belief was initiated by Hintikka (1962, 1973). Dretske (1981) and van Benthem & van Rooij (2003) studied these notions in the context of information theory, cf. van Rooij (2004) on questions and answers, or Parikh & Ramanujam (2003) on general messaging. Also Dunn seems to have this notion in mind when he defines information as “what is left of knowledge when one takes away believe,[sic] justification and truth” (Dunn 2001 pg. 423, 2008).


Adriaans list gives an excellent, but brief, summation of the context of the discourse of information. In the rest of this section, I will not discuss any of the alternatives in detail. Instead, I will turn to the highly relevant question of whether the last kind of information is really worthy of study.

**3.1.2 Is 'semantic information' worthy of study?**

It has been questioned whether we need a concept of semantic information or a semantic conception of information (see Adriaans...
2010, cf. Floridi 2010: 259f). In response to this question, I offer three replies.

First, irrespective of whether the topic deserves study the work of Bar-Hillel and Carnap, and Floridi has had great effect on the discourse. Thus, for this reason alone, it is worthy of a critical discussion.

Second, as previously noted, Floridi himself motivates the focus on semantic information by characterizing it as “the kind of information which is essential for epistemic purposes” (Floridi 2011: 82). This characterization makes the concept of semantic information worthy of consideration. (In my paper, I accept this basic characterization, but deny one of the criteria of Floridi’s definition.)

Third, and most importantly, as can be seen in Adriaans’ short descriptions above, a lot of the different conceptual approaches to information focus on measurements of informativity. This was the case for the semantic conceptions as well (both for Bar-Hillel and Carnap, and for Floridi). One of the main distinctions that I make in Paper I is to point out that the property of being information is separate from the property of being informative (i.e. information is not necessarily informative). This is an important point on which definitional issues rest, and a point on which there has arguably been some confusion. The fact that so many approaches to information are linked to informativity makes it plausible to argue that Paper I is valuable beyond the discussion of semantic information. However, the question of its wider applicability partly has to do with the relation between semantic information and information. This is one of the questions, which for various reasons, was avoided in Paper I (see section 4.1, p. 50f, for a brief discussion).13

13 The question was avoided mainly for two reasons. One, reasons of space. Two, because the aim was to present arguments that are compatible with as many other presumptions or theories as possible.
3.1.3 How should we define semantic information?

The question in Paper I is broadly the question of how we should define semantic information. The specific focus, however, is on one criterion alone, that of truth or truthfulness. What I do in Paper I is to argue against the veridicality thesis (the thesis that [semantic] information must be true/truthful). Floridi thinks of semantic information as data that is well-formed, meaningful, and truthful (in that order, see, e.g., Floridi 2016 for an introduction). I question the last criterion (i.e. I argue for an alethically neutral conception of semantic information). I do that by presenting both arguments in favor of an alethically neutral conception of semantic information as well as arguments against a veridical conception of semantic information. The latter argumentation begins with an attempt to show that a veridical conception of semantic information leads to inconsistencies or counter-intuitive results. This is done by adapting a point I previously made in Lundgren (2015b, c). I show that if we adhere to the veridicality thesis, then there are sentences that are semantic information if, and only if, they are not semantic information.

Next, my arguments focus on defending a neutral conception of semantic information, by attempting to show how Floridi’s counter-arguments against such a conception can be resolved. First, I deal with Floridi’s so-called ‘splitting test’, which attempts to show that ‘false information’ is not information that is false, but that is not information at all. I argue that this test fails for various reasons. For example, part of Floridi’s argument for the test is that ‘false information’ is like ‘false alarm’, but clearly, a false fire alarm is an alarm even if there was no actual fire.

Second, I argue against Floridi’s semantic arguments, with the main focus on what he calls BCP (Bar-Hillel-Carnap Paradox), which is

---

14 By ‘alethically neutral conception of semantic information’ I mean a conception of semantic information that is neutral as to their truth-status (i.e. whether something is information does not depend on it’s truth-value).

15 By ‘veridical conception of semantic information’ I mean a conception of semantic information according to which something must be true in order to be information.
the counterintuitive conclusion that false information is maximally informative. I argue that this paradox can be resolved by distinguishing between the property of being information and the property of being informative. Contrary to the *prima facie* assumption, I argue that not all information is informative.

That completes the brief over-view and contextualization of Paper I; we now turn to the topic of Paper II.

**3.2 Security**

In this section, I start by supplying the background and context of Paper II, co-authored with Niklas Möller (3.2.1). The focus will be on the standard definition of information security. Next, I will very briefly present a small selection of some previous criticisms of the standard definition (3.2.2), our criticism (3.2.3), and finally our proposal for a new definition (3.2.4). Omitted from the discussion are questions such as the broader applicability of our proposal (e.g., our definition can be expanded to an analysis relating to the resilience of information systems, see Lundgren 2015d). I will return to some such issues in chapter 4 when I discuss future research (in section 4.2 and 4.5).

**3.2.1 Background and context: the CIA definition**

The standard definition of information security—, which can be found in standards, handbooks, articles, legal codes, etcetera—defines information security in terms of three basic properties: Confidentiality, Integrity, and Availability (see, e.g., p. 117, fn. 8, for a list of references). To these properties, other properties are sometimes added, but it is in virtue of the three basic properties that these kinds of definitions are called ‘CIA definitions’. These properties, which make up the CIA-triad, have been somewhat stable since at least the 1980s (see, e.g., Meijer et al 2007: 641).

While the term ‘information security’ may refer to many different things, it was clear—for us—that the most pressing and interesting issue to define was the conditions for when some information (system) is
secure. In many standard definitions it is evident that CIA-definitions are used to define just that, even though there is—as noted in Paper II—a lot of disagreement about the exact role of the CIA-triad and the CIA-definitions (cf. p. 117, fn. 8).

Thus, to be able to critically evaluate the CIA-definition, we must first specify it. Our specification has two functions. Firstly, we contextualize it by adapting it to the relevant aim (i.e. that it defines conditions under which some information is secure). Secondly, we formalize the definition so that it fits the standard formula for a definition:

The CIA-definition of secure information: some information I is secure if, and only if, all parts of I retain the properties of confidentiality, integrity, and availability. (p. 118)

### 3.2.2 Alternatives and previous criticism of the CIA definition

Just as there is a lot of disagreement about the exact role of the CIA-triad, there is also a lot of previous criticism of the CIA definition of secure information. A standard form of criticism is the idea that the CIA-triad is insufficient, but can be complemented by other properties. For example, Parker (1998) presents a few actual cases of security breaches/incidents that he argues were not breaches of confidentiality, integrity, or availability. To resolve this, he suggests adding three more criteria: Possession / Control, Authenticity, and Utility (see Parker 1998, 2009). Discussions of whether the CIA-triad needs to be complemented by other properties are not uncommon. In standards such as the ISO-definition, this is recognized by noting that other properties can be included (ISO/IEC 27000 [2016: 6]).

There are various examples of proposals to complement the CIA-triad or to exchange some of the three basic properties for others. However, such forms of criticism are less interesting since our counter-

---

16 In the upcoming examples (section 3.2.3, p. 33f; Paper II, p. 120-128) we discuss both when an information system or some information is secure. Although both are of interest, we have merely specified CIA related to the latter. Our examples, however, are such that if the system is insecure, the information is insecure too.
examples against CIA definitions aim to show that these types of definitions are analytically wrong—i.e. security is not a matter of satisfying a specified list of properties (at least not in this colloquial sense).

More interesting are proposals that suggest other approaches to security, such as that of James M. Anderson:

I propose the following definition of enterprise information security:

A well-informed sense of assurance that information risks and controls are in balance. (Anderson 2003: 310, underlining in original)

While Anderson's definition is interesting, it suffers—amongst other problems—from a conceptual confusion of the ontological state of a thing (security is, arguably, a state of affairs) with the question of what we know about that state (having a well-informed sense of assurance is, arguably, an epistemic notion). Arguably, something can be secure even if we do not know that it is secure. Nevertheless, an epistemic conception of information security is—of course—not without interest. However, once we know what security is (ontologically), the epistemic conception can be defined relative to the ontological.17

### 3.2.3 Our critique of the CIA definition

Our criticism is two-fold: we aim to show that the CIA definition (as characterized by the previous specification) neither supplies necessary nor sufficient properties for the state of security of information. Thus, the CIA definition fails by being both too wide (characterizing insecure states as secure) and too narrow (characterizing secure states as insecure).

---

17 Of course, it would be possible to argue that security is essentially an epistemic notion. While that could make sense for certain applications, it seems less relevant for information (systems). Also, it still seems that there is a relevant distinction between whether x is secure and whether we think or know that x is secure. However, considering what we propose, it may be reasonable to think that security, on occasion, requires that one knows that x is secure. The problem with Anderson's definition is that it always requires this.
I will give a brief and selective summary of our arguments, starting with the former, i.e., the false negatives. Consider, e.g., availability—the property that information be timely available to authorized users. Contrary to the presumption that availability is necessary, there are security systems that depend on removing the property of availability to increase security. One such example is time locks. The whole idea of a time lock is to make the locked-away content unavailable even to authorized users. This means that availability cannot be a necessary property for a secure system, but according to the CIA definition availability is a necessary property.

That some secure information is defined as insecure shows that the CIA definition has identified various properties as necessary, although they are not necessary. A more serious problem, however, is defining insecure information as secure, i.e., false positives. The CIA definition suffers from false positives because it has conflated serious consequences of a security breach with the state of insecurity, which is a problem since it is not the case that all security breaches have serious consequences.

Consider the following example: a system administrator has all possible forms of access to a system and the information contained within that system. Now, suppose that someone takes the system administrator’s children as hostage. At this moment, it may very well be the case that the properties of confidentiality, integrity, and availability are all retained. However, the system is—of course—not secure, since the hostage taker has influence, and/or, control over the system via the administrator. This is a security breach, but according to the CIA definition, security is only breached if, and when, the hostage taker forces the system administrator to do something such that one of the CIA properties are actually affected.

Our analysis of these kinds of problems boils down—more or less—to the idea that security of some information (system) is relative to the needs of some stakeholder. Because of this analysis, we propose a new kind of definition. To this, we now turn.
3.2.4 Our proposal for a new definition of information security

We argue that what we need—to resolve the problems that the CIA definitions suffered from—is a definition that is contextually sensitive. We, therefore, propose a definition (the ‘Appropriate Access’ definition) of security as follows:

\[
\text{AA (general): The object } O \text{ is secure for stakeholder } H \text{ if, and only if:} \\
\text{For every agent } A, \text{ and every part } P \text{ of } O, \text{ A has just the appropriate access to } P \text{ relative to } H. \quad (p. 129)
\]

If applied to some information/system, we get:

\[
\text{AA (information): The information } I \text{ is secure for stakeholder } H \text{ if, and only if: For every agent } A, \text{ and every part } P \text{ of } I, \text{ A has just the appropriate access to } P \text{ relative to } H.
\]

\[
\text{AA (information system): An information system } S \text{ is secure for stakeholder } H \text{ if, and only if: For every agent } A, \text{ and every part } P \text{ of } S, \text{ A has just the appropriate access to } P \text{ relative to } H. \quad (p. 129f)
\]

In the above definitions ‘agent’ refers to any entity (technical, software, human etc.) that may have some kind of access to some part of the object.

It may seem that the definition is stating only the obvious—i.e. that access relations should be just appropriate. However, the idea of this definition is that it needs to be further applied either to the context (an option we discuss but do not further analyze in the paper) or to the needs of some specific stakeholder (e.g., an organization). The basis of this is that security is relative, by which I mean that, the question ‘is x secure?’ should be replaced by ‘is x secure for H?’ and this, in turn, is a question of what is appropriate for x (given the needs of H), or: what is right for x (given the needs of H). This, however, is evaluated objectively.

Thus, what one needs to do to use the definition is to apply the definition to the specific needs of that stakeholder. In order to do this one needs to determine the appropriate access for any agents and all part of the stakeholder’s information (system). The definition does not only capture that what is appropriate is relative, but also that these
things can change over time. This is also part of the practical benefits of our proposal: that it requires those who apply the definition to think about all the relevant aspects of security and how it is achieved (in relation to the stakeholder’s needs).

That completes the brief over-view and contextualization of Paper II; we now turn to the topic of Paper III and IV.

### 3.3 Privacy

In this section, I focus on the topic of privacy, which is the main topic in Paper III and Paper IV but also partly discussed in Paper II and Paper V.

The discussion on privacy is messy and has been so for a long time. There is vast disagreement both on what we ought to define and on how we ought to define it. There are descriptive and normative conceptions of privacy. Amongst the normative definitions most focus on a supposed right to privacy, while others focus on privacy as an interest, claim, or entitlement (see, e.g., Schoeman 1984 and DeCew 2018 for overviews of some of the options).

I focus on the concept of privacy, as such, and I argue that privacy is a normative concept. Specifically, in Paper IV—when I present my account of privacy—I argue that privacy is a *pro tanto* good, by which I mean “[h]aving less privacy is *prime facie* worse than having more” (p. 172).

However, given that the bulk of the literature focuses on a supposed right to privacy, I will briefly explain why it is not part of my focus and to what extent the discussion in my papers applies to that concept (3.3.1). Next, I will turn to discuss how we ought to define privacy in two subsections. First, I will discuss the issue of picking an appropriate definendum, given that we focus on a normative conception of privacy (3.3.2). Second, I will focus on the definiens in order to discuss some alternatives to the definition that I propose in Paper IV (3.3.3).
Note that my aim here is not to give a full and neutral account of the relevant background and context as it applies to these questions, but the presentation will be selective and critical (motivated in relation to the discussion of Paper III and Paper IV).

3.3.1 Why I ignore the right to privacy

This section will introduce some background relating to the concept of the right to privacy. While I will give a very brief general introduction to the topic, the focus is on explaining it as it is relevant to the papers as such.

The right to privacy can be either a legal or a moral right. A conception of a legal right to privacy relates to a certain extent to theoretical and practical legal issues. Given that, and given that I am interested in a philosophical account of privacy, a legal right to privacy is not of any concern. However, a lot of the debate on the right to privacy takes part in a legal context and, hence, some of the relevant literature is written in that context. Indeed, the serious discussion on privacy is often considered to have started with the seminal law review article “The Right to Privacy” (Warren and Brandeis 1890).

Given that I focus on a normative conception of privacy, one may wonder why I do not focus on the right to privacy. Indeed, Adam D. Moore (2008) has previously argued that “[a] normative account” of privacy “makes reference to moral obligations or claims” (p. 413). Part of the reason why I do not focus on the right to privacy, while I consider privacy to be a normative conception, is that I disagree with Moore on what constitutes a normative concept. Indeed, just because privacy is a normative concept, it does not mean that it needs to refer to any obligations. Happiness is a normative concept, but the concept of happiness does not necessarily refer to any obligations. Indeed, all I mean when I say that privacy is a normative concept it “is a value that we can have less or more of” (p. 175). Given that it is a pro tanto good it also follows that “having less/more of it is prima facie bad/good” (ibid).

Whether any obligation follows from such a value depends on what kind of normative theory we apply. The aim of my account of
privacy—as it is explicated in Paper IV—is to conceptualize an account of privacy—as a value, or good—that is compatible with any type of normative theory.\(^{18}\)

Furthermore, as I stress in both Paper III and IV, if there indeed is a right to privacy, then the concept of privacy should give some guidance as to how the concept of the right to privacy can and should be defined. It seems to me that the literature is full of confusion relating to this issue. First, many that focus on the right to privacy do not even say so (cf. Parent 1983: 273, fn. 11 for a similar complaint). Second, and more importantly, a sound and complete account of the right to privacy reasonably ought to require that one give some account of what privacy as such is. Indeed, given that it is reasonable to presume that the right to privacy is a right to privacy, both concept must be presented in a coherent account even if one is only interested in the former (i.e. the plausibility of a conception of the right to privacy partly depends on the plausibility of a conception of privacy). This is something that many seemingly fail to recognize. For example, Andrei Marmor (2015)—amongst many others—defends a right to privacy without concerning himself with whether the implied account of privacy is plausible. In Paper III, I use a modification of Marmor’s account of the right to privacy to defend a control-conception of privacy against a potential dilemma, only to ultimately show that privacy cannot be defined in terms of control without also taking the context into consideration (as part of the defining criteria). However, if privacy cannot be defined in terms of only control, then it is reasonable to ask how the right to privacy can be defined as such. Indeed if privacy is \(x\), then the right to privacy have to correspond in a relevant sense to that \(x\), for otherwise, it is not a right to

\(^{18}\) I am using “type of normative theory” to indicate that it aims to be compatible with any broader category of a normative theory such as deontology, consequentialism, virtue ethics, etcetera (supposing a right-based theory would require that the proposed analysis of privacy is adapted to the concept of our right to privacy, which it is compatible with). Nevertheless, that my proposal aims to be compatible with any type of normative theory does not imply that it is compatible with all normative theories. For example, adapting it to purely hedonistic theories—such as classical utilitarianism—would arguably require further revisions.
privacy, but a right to something else. If privacy cannot be defined in terms of \( x \), then that yields a problem for defining the right to privacy in terms of \( x \) (which is what I argue, as a side-note, in Paper III).

This argument hangs on the relation between the concept of privacy and the concept of the right to privacy. An illustrative example to the point I aim to make the following. Consider the following account of the right to privacy:

Definition: A right to privacy is a right to control access to and uses of—places, bodies, and personal information. (Moore 2008: 421)

According to Moore, the above account is a normative account of privacy (i.e., according to Moore, it “makes reference to moral obligations or claims”, p. 413), while “[a] descriptive account or non-normative account of privacy describes a state or condition where privacy obtains” (ibid), which Moore defines as follows:

the condition of privacy obtains when an individual, place, or personal information is inaccessible. (p. 421)

While there may be various relevant arguments against Moore’s analysis—e.g., I previously noted my disagreement with his characterization of the distinction between normative and descriptive concepts—what I want to focus on now is how the example illustrates the problem of extreme asymmetrical relations between a definition of privacy and a definition of the right to privacy.

Indeed, if privacy is “the condition which obtains when an individual, place, or personal information is inaccessible”, then why is the right to privacy not a right to that condition, but “a right to control access to and uses of—places, bodies, and personal information” (p. 421)? It seems to me that every proponent of any account of the right

---

19 Note that Moore writes ‘the condition’ (2008: 421), something, which is obviously problematic, given that there reasonably is more than one condition of privacy.
20 Of course, Moore may argue that there is an asymmetry between his definition of the right to privacy and his definition of privacy because the latter is defined descriptively. Alternatively, he may argue that the right to privacy is not a right to privacy. Or, which is more sensible, he may argue that a condition of privacy does not
to privacy needs to address these questions, questions which are standardly ignored. However, it is fair to say that many would not agree with me.

This takes us to the issue of how we ought to define privacy, or specifically: what is the appropriate definiendum for the concept of privacy. I will turn to this in the next subsection.

3.3.2 Defining privacy: Qualifying the definiendum
In the above-discussed definition, part of the conception of privacy is given by the definiendum that Moore had chosen. While I disagree with Moore’s assertion—that privacy is a state or condition—there is nothing wrong with attempting to qualify a concept by qualifying the definiendum. Indeed, this is an important aspect of defining a concept (cf. Appendix Part A, p. 57f).

However, while the assertion that privacy is a state or condition is a common tradition in the literature (see, e.g., Parent 1983: 269, Schoeman 1984:3), I think there are several good reasons to hold that this assertion is problematic. Indeed, contrary to this assertion I hold that privacy is a good (or value), which we can have less and more of. Now, it may be that many who define a state or condition of privacy do not do so because they equate privacy with a state or condition. Rather, they may think that a state or condition of privacy is what is most important to define. As I will explain, I disagree with this claim as well. In my view, it is more pressing to give an account of an agent’s degree of privacy. There are several reasons for this. It gives us an account of what constitutes privacy in any situation, rather than one of several accounts under which a state of condition of privacy obtains. Part of the problem is that it is perfectly plausible to hold that competing accounts of privacy properly define a state or condition of privacy, but that it does not give necessary conditions for any state or condition. It is, of course, possible to give necessary and jointly sufficient conditions for define privacy nor what is essential about it—by if he thinks so, why would he focus on presenting such a definition?
any state or conditions of privacy. However, in comparison to defining when an agent is in a state or condition of privacy, defining the degree of an agent’s privacy is preferable since it is easier to evaluate the proposed analysis of privacy against possible counter-examples. Indeed, an account of the conditions that determine someone’s degree of privacy covers all states or conditions of privacy and all other states in which privacy can be affected. Furthermore, we can also define a state or condition of privacy in terms of the degree of privacy (e.g., “a state or condition of privacy for agent A obtains if, and only if, access relations to A’s private matters are not” of the wrong kind, p. 185).

The above discussion relates to how we qualify the definiendum to make the account more sensitive to counter-examples and better adapted to the purpose of making sure that we define privacy properly. This can be illustrated by my own position on these issues: I hold the position that both complete limited access and complete control (in the negative sense)\(^{21}\) can achieve a state or condition of privacy, but I do not think that either is necessary. Conversely, when it comes to the question of what can diminish someone’s privacy I hold that the accounts of limited access and control are neither necessary nor sufficient. I think that defining privacy as a state or condition may be one of several important reasons for some of the confusion in the debate. However, since this discussion directly relates to the issue of the definitional criteria (i.e. spelling out the definiens) of privacy, we will now turn to this issue.

### 3.3.3 Defining privacy: Necessary and jointly sufficient criteria

In this subsection, I will critically present some classical accounts of privacy. The basis of this criticism will connect to the supposition that privacy is a normative concept, and specifically that privacy is a *pro tanto* good.

---

\(^{21}\) By ‘complete control in the negative sense’ I mean that others do not have control over the relevant object (in this case that would be the content of privacy for both limited access and control definitions).
Two classical accounts of privacy are—the previously mentioned accounts of—limited access and control respectively. These accounts can be spelled out in various ways. As previously noted, privacy is often defined in terms of a condition or state. Limited access accounts of privacy are often conceptualized as a state or condition that obtains when others have limited access to your private matters, whatever those are (cf. Schoeman 1984:3). However, as previously noted, such a state or condition tells us nothing about whether privacy is indeed constituted by limited access. It is perfectly possible to grant that limited access is sufficient for a state or condition of privacy, but deny that it is necessary. While we can strengthen this way of defining privacy, e.g., by expressing what is the necessary and jointly sufficient conditions for obtaining any state or condition of privacy it is (for reasons already given) preferable to make a stronger claim and present conditions of an agent’s degree of privacy. Limited access views would then imply that “A person has privacy to the degree that other people do not have access to her private matters” (Paper IV: 5). There are two mutually exclusive options for further specifying this account. First, suppose that the degree of privacy is affected equally irrespective of whom one shares one’s private matters with, then this would imply the counter-intuitive idea that being nude in front of a work colleague and in front of your intimate partner affects your privacy equally, ceteris paribus. Supposing that privacy is a pro tanto good, this seems implausible. So it cannot be that privacy is diminished equally irrespective of whom one shares one’s private matters with. Second, suppose alternatively, that the degree of privacy is affected unequally depending on whom one shares one’s private matters with, then that would resolve the previous counter-example. However, the account would also require further specification to clarify how this unequal diminishment works. The problem is that such a specification must go beyond a pure limited access account since the difference between the two above-discussed examples of nudity has nothing to do

22 By ‘private matters’ I mean those kinds of things relating to a person, P, that if accessed by someone else, can lead to P’s privacy being diminished (cf. p. 176).
with the limits of access, but with who the accessor is. Thus, presuming
that privacy is a pro tanto good, it cannot be defined only in terms of
limited access. In Paper IV, I explicate an account of privacy that can
explain these kinds of examples. I will introduce this account shortly.

Another classical account of privacy is that of control. As I
explain in Paper III, the concept of control have been used in different
ways in various control-based accounts. I believe it is fair to say that the
debate on control-accounts is confused and that it suffers from the fact
that its proponents and opponents alike have failed to properly qualify
what control is and what it requires. I believe the best defense of
control-based definitions of privacy (in terms of the right to privacy) is a
recent article by Andrei Marmor (2015). While Marmor does not define
control, he does attempt to give a detailed account of how someone’s
control can be affected. I discuss some of the details of his account in
Paper III.

The problem that limited access accounts suffer from arguably
holds mutatis mutandis for control-based accounts as well. Indeed, as I
argue in Paper III, proponents of control-based accounts have to go
beyond the concept of control to explain examples such as the one
considered above.

Many accounts of privacy can be considered as variants or
combinations of the above accounts. For example, the right to be let
alone is reasonably understood as a right to delimited others access to
one’s private matters (which, of course, is an account of the right to
privacy). However, in the last twenty years or so a competing alternative
has emerged. The alternative has been promoted by legal scholars such
as Daniel J. Solove and Helen Nissenbaum. Its popularity, however, is
not limited to the legal domain. Broadly speaking they promote
contextual accounts of privacy (although both focus on the right to
privacy), according to which the context is everything. Indeed, both
refuse definitions and according to Solove privacy is an umbrella
concept similar to that of Wittgenstein’s notion of family resemblance
(Solove 2008: 47, cf. Wittgenstein 1953). According to Nissenbaum, we
must analyze a broad set of aspects to determine whether a violation or infringement of the right to privacy has occurred (see, e.g., Nissenbaum 2010).

In agreement with these scholars, I argue in Paper III that control-based accounts of privacy must take the context into consideration. However, in Paper IV I argue that we can limit these contextual accounts. What matters are our social relations. Indeed, I argue that privacy is constituted by our social relations. That there is a strong connection between privacy and social relations is a common idea (see, e.g., Rachels 1975). However, contrary to Rachels I argue that privacy is constituted by our social relations, not only that privacy is important for our social relations. In the end I propose and argue for the following definition of an agent’s degree of privacy:

Agent A has privacy for the private matter(s) P, relative to B, to the degree that B’s access to P is not inappropriate in virtue of A’s and B’s social relation. (p. 185)

The details of the definition require further explanation. Briefly, access is not merely a bivalent property but includes what I call ‘access-sharing’ (i.e. how the private matter is or was shared), and the social relations are not type-based, but token-based (i.e. the degree of privacy depends on the social relation between the tokens A and B). Furthermore, appropriateness should be evaluated in virtue of all aspects of the social relations, not all-things-considered, which means that while of B’s access to A’s p can be appropriate in virtue of some aspects of their social relation, it can also be inappropriate in virtue of some other aspects. It follows that A’s privacy is affected, relative to B, by the access that is—and to the degree that the access is—inappropriate. Appropriateness as such is not defined intensionally in the text; rather it is explained by various examples. I presume a common sense understanding of the concept, in line with how we would use it in normative analysis.

3.4 Anonymity

The topic of the final paper is anonymity. As I note in the paper, little has been said about the issue of anonymity amongst philosophers.
While there is a vast technical literature relating to deanonymization technologies and the question of how we protect conversations against eavesdropping, etcetera, this is not the place for such accounts. Although the technologies have developed since, Paul Ohm (2010) offers a good introduction to some of the elementary technical issues, adapted in a form suitable for a non-technical reader.

The question I address in my final paper is what concept we need to properly analyze and make sense of the possible harms from these deanonymization technologies. Normative analysis requires good conceptions of relevant concepts. What I question in Paper V is whether anonymity is what is really at stake or whether the possible harm from these techniques goes beyond anonymity. I argue that they do.

In this section, I will briefly summate the final paper. I will start by briefly presenting three previous accounts of anonymity (3.4.1). Next, I aim to briefly explain some of the relevant facts about the deanonymization technologies, and related information aggregation technologies (3.4.2). Last, I will briefly explain why I take this to be a threat that goes beyond anonymity. Specifically, a threat that potentially will harm our ability to be anonymous, which is what is really at stake.

3.4.1 Previous accounts of anonymity
Previous philosophical accounts of anonymity argue that anonymity is non-reachability (Nissenbaum 1999), non-identifiability (Wallace 1999), or non-trackability (Matthews 2010).

Kathleen A. Wallace thinks of anonymity in terms of a definitive description, as long as one is not singled out (identified) one is anonymous. Specifically, she argues that:

“[a]nonymity is noncoordinability of traits in a given respect(s) [---] making it difficult or impossible for the known trait to pick out the person in other respects and vice versa” (1999: 250).

Before Wallace, Helen Nissenbaum argued that “the value of anonymity lies in the possibility of acting or participating while remaining out of
reach, remaining unreachable” (1999: 142). Furthermore, while Wallace aims for a “metaphysical” account of what anonymity is, which ought to be useful in ethical analysis, Nissenbaum specifically thinks that her account is an account of “precisely what is at stake in anonymity” (ibid).

Finally, Steven Matthews (2010) argues that what is at stake is avoidance of trackability over different contexts. Matthew’s uses an example from Laud Humphrey about male-to-male encounters in public restrooms. What Matthews argues is that these males are, to some extent, identified and reachable by each other. However, this is not what matters, what matters is not be trackable from this social context to another.

I will not go into the details of these different accounts rather I focus on some aspects that they all share (what I call the ‘common view’):

The common view: a person is anonymous relative to some information only if that person cannot be singled out as the one linked to the information. (p. 202)

My aim is not to question the common view as a fair conception of anonymity. Indeed, it is reasonable to hold that the common view gives a fair account of a common sense, or lexical, conception of anonymity. What I question in the paper is whether the concept of anonymity is what is really at stake given possible harm from deanonymization technologies. To this we now turn.

3.4.2 Deanonymization and information aggregation technology

Deanonymization, relative to the common view, can be understood as follows:

a person that was previously anonymous relative to some information is deanonymized if that person can be singled out as the one linked to that information. (p. 204)

The standard means of achieving deanonymization is by information aggregation. For example, a combination of ZIP code, sex, and date of
birth can be used to identify at least 61 percentage of the US population (see Ohm 2010: 1705, fn. 4, for a few relevant studies). There are two things that I want to note about these kinds of techniques.

First, contrary to Wallace, deanonymization does not merely require coordination (or linking) of what would constitute ‘traits’. No piece of information, or data, is too insignificant to be useful. For example, Johansson et al (2015) shows how they can deanonymize online users by analyzing the times when users post information.

Second, anonymity cannot be analyzed in isolation. The power of deanonymization is due to the availability of information (already noted by Nissenbaum [1999: 141]). Whether someone can remain anonymous depends on what kind of information that is previously available. In relation to this issue, Ohm discusses what he calls the ‘accretion problem’. By linking ‘anonymous’ information with other ‘anonymous’ information, further linkages are possible; “[s]uccess breeds further success” (2010: 1746). As Ohm notes, this is worrisome, since it increases the likelihood of further deanonymization and future harm. More importantly, it shows that seemingly insignificant information can be harmful because it can be used to deanonymize more significant question.

The question is to what extent this is merely future harm from future deanonymization or if we can be harmed without being deanonymized. Thus, the question is whether anonymity is what is really at stake—or if it goes beyond anonymity. In paper V, I argue for the latter.

This question can be expressed as follows. According to the common view, what is at stake is whether the information is linked to a person (what we may call ‘information-to-person’ linkage), not only whether information-about-a-person is linked to information-about-a-person without being linked to that person (what we may call ‘information-to-information’ linkage). According to the common view, the latter only matters as far as it actually affects the former. On my
view, the latter can be harmful beyond the former and although information-to-person linkage remains unaffected.

3.4.3 What is really at stake?

It is not *prima facie* implausible to think that what is really at stake is the actualization of the risk to our anonymity. However, it is reasonable to think that the possible harm goes beyond this.

One of the examples I consider in Paper V is about Joe. Joe is in a situation such that a lot of sensitive information about him is linked to a lot of other information about him and if he says or does certain things, enough information will be available to deanonymize him. Suppose further that Joe knows this.

In this scenario, Joe can be harmed without being deanonymized. The harm comes in the form of a dilemma choice between being deanonymized (and freely being able to express himself and do what he wants) and self-censorship (and retaining anonymity).

I analyze this in terms of an *ability to be anonymous*, which goes beyond mere anonymity. It is decreased by information-to-information linkage, which can harm our ability to be anonymous now and in the future, but information-to-information linkage can also harm us without deanonymization, which the above example illustrates. However, the harm goes beyond the example of Joe, since in the modern information society we often have to choose between participation and exclusion. Part of the problem is that this choice (especially, what we give up) is rarely transparent. Furthermore, it is also hard to foresee the actual effects the choices have, since it is practically impossible to foresee what information that will be linked to which information in the future.

Last, in the paper I, explicate our ability to be anonymous in terms of *a reasonable control over what we communicate*. I further explain that by control over what we communicate I mean the absence of others control over what kind of information we disseminate and to whom. Furthermore, I show how this concept differs from the concepts of privacy and the right to privacy, but I need not go into that here—given
that any reader by now would know that I am skeptical about the idea of defining (the right to) privacy in terms of control.

That concludes the thematic chapter, as it relates to the content of the five papers. We now turn to another side of the themes, possible future research.
4. Future research

In this chapter, I turn to address possible future research relating to the four themes and the five papers. While there are vast possibilities for applied normative analyses given the available normative frameworks, such applications are fairly obvious and less interesting to discuss in this brief concluding section. Thus, I will focus on questions relating to the definitions and accounts as such, which—of course—are motivated by more applied issues. I will discuss the four themes below, topic-by-topic (in section 4.2-4.4) and end by giving an example of how the analyses of the articles can be extended to a joint framework (section 4.5).

4.1 Information

While Paper I contributes to a key topic in the debate on information, and on semantic information in particular, several questions remain. Indeed, as previously noted the question of how we should define semantic information remains. For example, in Lundgren (2015c) I argued that semantic information is only meaningful data. Furthermore, I proposed a sense of meaning that merely requires that it is possible to make sense of the data. There are reasons to be skeptical of this idea and an obvious alternative—for a proponent of an alethically neutral conception of semantic information—is to require a stronger sense of meaning, specifically a propositional sense of meaning, such that semantic information is the kind of information which has truth-values (i.e. what we may call propositional information). I note this in Paper I (p. 78, fn. 2).

It is also important to discuss whether semantic information is, or should be, distinguished from information as such; and if so, how do we define information? And what other kinds of information are there? For example, Floridi considers environmental information as an alternative (see, e.g., Floridi 2016). More importantly, what is the relation between semantic information and the main alternatives (see Adriaans over-view quoted in 3.1.1)? Many of these alternatives can reasonably be
interpreted as an alternative to a semantic conceptions of information—but what is their relation?

A central question is also the definition of informativity and whether it is relative to different possible kinds of information. This is further related to the epistemic state of being informed and misinformed. The relevance of this issue should be obvious in the age of fake news and so-called ‘fake news’ (i.e. news that is called fake, but really is not).

4.2 Security

Given that the focus in Paper II is on the security of two related objects (information and information systems), the most interesting research question is whether the AA-definition can be expanded beyond those objects (see, e.g., Herrington 2012: 14 for an overview of some previous definitions of security). While it is reasonable to think that AA applies to ordinary objects (i.e. if objects are interpreted as non-living physical entities), it is questionable whether it applies to entities such as humans or nations. For example, it may be reasonable to think that a human or nation needs access to drinking water to be secure. Thus, security of certain entities is reasonably not only a matter of agents’ access to them but also of the entities access to fundamental necessities.

This is an interesting challenge to the AA-definition, since it indicates the possibility of defining security, as applied to some objects, in terms of access to a specific list of fundamental needs. This is contrary to our conclusion concerning information security, which indicates that the best candidates for which properties that constitute necessary needs for any information (system) all have counter-examples. However, all humans do need water. Thus, on the one hand, the potential for a list of properties that holds for each human may be possible. On the other hand, it is questionable whether a complete list, without actual or possible counter-examples, can be compiled. More importantly, it may still be preferable to show that security can be encompassed under a modified version of the AA-definition (i.e. one
that recognizes that living objects, such as humans, or abstract entities, such as nations, require appropriate access to other entities, rather than only requiring that others have the appropriate access to them).

There are other interesting questions as well. Given the aim of the AA-definition—which is not merely to contribute with a philosophical analysis of information security but a definition that can also be used and applied in practice—an interesting follow-up would be to analyze the usage of the definition *in situ*\(^23\). For example, how would practical usage of the AA-definition differ from practical usage of the CIA definition? This would require empirical studies, and it would be interesting to parallel such studies with a more theoretical discussion of the role of empirical studies—and, e.g., experimental philosophy—as it relates to the normative work of providing the best definition of the most relevant concepts.

### 4.3 Privacy

Privacy, in conjunction with the next topic, is one of those topics that would benefit greatly from a more applied normative analysis.

However, in the two papers, several more theoretical questions remain that would also benefit from being developed. First, one could dedicate a paper to merely defending the idea that privacy is *a pro tanto* good. Second, debunking more alternatives could contribute to the discussion. Third, the account in Paper IV left most issues relating to a *right to privacy* untouched. Is there a right to privacy? If so, how would it be related to what is proposed within Paper IV? For example, what are the normative constraints to such a right? Does it protect against risks? Under which conditions can it be overridden? Etcetera.

---

\(^23\) *In situ* is Latin for on site. The term is used in various senses. Above I use it to stress testing the definition in practice, used by practitioners, rather than the theoretical analyses that we normally see in philosophy or a systematized theoretical evaluation by practitioners.
4.4 Anonymity

The most prevalent questions concerning Paper V are of an applied nature. How should we in practice balance the benefits of big data and information aggregation against the individual’s needs, which in part relate to the ability to protect her privacy. It is important to point out that there are many benefits of big data, so the answer is not obvious. However, there is also a risk that big data will change society for the worse, because of the ways it can be abused. Here we need practical guidance on every level, which the paper’s conceptual analysis provides a fundamental tool for.

4.5 Combined analysis: the example of security and privacy

While the accounts that I give in each of the papers are individual accounts, relating to their separate themes, there are many thematic overlaps, which could easily be expanded to a joint framework. I will use the example of security and privacy, which is also—albeit briefly—mentioned in Paper II.

Privacy and security are often considered dichotomous, in the sense that increased security require diminished privacy and vice versa. This is, of course, strictly speaking not a necessity, but there is often a value-conflict and/or trade-off between these values.

A benefit of the way these concepts are defined in Paper II and IV—, which goes beyond their individual motivations—is that the separate accounts allow for a simple joint-analysis. A key-function in both definitions is appropriate access, but the appropriate access is relativized to different factors; the needs of a stakeholder (in the case of security) and the social relation (in the case of privacy). Although both definitions require some analysis to be applicable in an applied context (as normative ethics standardly does), the joint usage of appropriate access allows for an easy illustration of the involved value conflicts once that is achieved. Indeed, once we know what kind of access that security and privacy respectively require, in a given situation, it is clear in what way there is a conflict between these values, in the given situation.
Another virtue of the joint framework—formed by both definitions—is that we can apply someone’s privacy as a security object.24 Furthermore, the AA-definition can be applied relative to several stakeholders. In a situation where stakeholders have diametrical needs, the definition would correctly reveal the conflicts as contradictions. The contradictions can then be analyzed further (e.g., is it possible to re-analyze the needs in relation to the restrictions needed to resolve the conflicts?).

These analyses can be applied and extended to various practical challenges. A simple example would be the security-privacy conflict of public usage of surveillance cameras (e.g., CCTV-systems). The problem is that those accessing the CCTV-system, standardly, would not have the appropriate social relation with all people passing by the cameras. At the same time, CCTV-system can allow for tracking of criminals (e.g., terrorists), so it can be argued that such access is precisely appropriate, given that we focus on the security of some relevant stakeholder(s). A possible way to remedy this conflict is to configure the system so that it does not allow for crisp images (i.e. that people are not identifiable), e.g., without a court order. This would minimize people’s privacy less (because the access would be less inappropriate), while still allowing for functions that may be needed for security purposes, such as tracking of people and identification of mischievous activities. The example of CCTV-systems can also illustrate that security and privacy are not necessarily in conflict since hacking of CCTV-systems would affect both.25 These are all very obvious and superficial considerations, but it

24 Although it is discussable to what extent the AA-definition can be used beyond information, someone’s privacy should be applicable within the definition given that privacy is defined in terms of appropriate access as well (or at least someone’s informational privacy). Of course, when put within the AA-definition what we have is the conditions for securing someone’s privacy, which is possibly stronger than merely retaining it.

illustrates that the definitions easily allow for joint analysis and how it can be used for applied ethical analysis (something that would require a more extensive analysis).

That ends the main chapters of the introduction, but the appendix remains.
Appendix: Definitions

Despite the prominent role of definitions in philosophy, surprisingly little has been written on definitions (and even less on distinctions). The only main textbook on definitions, Richard Robinson’s Definitions (1950), has, despite its virtues, serious drawbacks. Few attempts at writing a new textbook have been made, Roy Harris’ and Christopher Hutton’s Definition in Theory and Practice: Language, Lexicography and the Law (2007) is one example.

The subject is curiously underdeveloped. Raziel Abelson (1967) claimed in The Encyclopedia of Philosophy that “no subject is more in need of a fresh approach” (p. 314). According to Harris and Hutton (2007), this was still valid at the time of their writing (p. ix). In Belnap (1993), we find the disclaimer that “There is, alas, hardly any literature on this topic” (p. 115). Although things have happened in the last 50, 20, or 10 years, there is still more to do.

Below the appendix is divided into two parts. First, Part A deals with formalism and basic criteria of definitions. It also addresses the issue of quality (i.e. what is a good definition). Second, Part B gives an over-view of some of the major kinds of definitions.

Appendix. Part A. Formalism and basic criteria of definitions

The standard formula for a definition is a complex which consists of three things: a definiendum (that which is to be defined), a definiens (that which defines), and a definitional connective. The standard formula may be characterized as below:

\[
\text{DEFINIENCE} \Omega \text{DEFINIENCE}
\]

in which \(\Omega\) is a placeholder for a definitional connective, commonly an equivalence relation (I will return to the definitional connective after discussing a few other points).

However, Gupta makes an important point that:
Many definitions—stipulative, descriptive, and explicative—can be analyzed into three elements: the term that is defined (X), an expression containing the defined term (...X...), and another expression (---------) that is equated by the definition with this expression. Such definitions can be represented thus:

(1) X: …X… =df --------- (2015)

While we may debate whether the first occurrence of ‘X:’ is necessary I am in full agreement with Gupta on the important thing, i.e. that X, as part of the definiendum, must be properly contextualized. This means that one must clarify what kind of thing one is defining. This is not always prima facie clear. For example, in Paper II it is argued that information security can be many things: information security praxis, information security as an academic field, and information security as something you do, etcetera. We argue that what is most interesting and pressing to define is the state when information is secure. This is an example of what I mean by contextualizing the definiendum. We must clarify what kind of entity we are defining. The discussion on the definiendum of privacy (3.3.2) illustrates this issue on an even more detailed level. Thus, while definiens supplies “the definition” (in a common sense way of expressing it), the definiendum directs the scope and context of the term to be defined (cf. Belnap 1993).

So much for the basic formalism. Nuel Belnap (1993) argues that there are two necessary and jointly sufficient criteria for a good definition:

- Eliminability: when we replace a word or concept by a definition the definition should cover all the meaning of the word/concept that we replaced. (p. 119)
- Conservativeness: when we replace a word or concept by a definition it should not add any new meanings beyond the word/concept that we replaced (i.e. it should cover only the meaning of the word/concept). (ibid)
As Belnap notes, these criteria are context-sensitive. No definition allows elimination in every context (p. 121), which is part of the reason why contextualization is so important.

Now, there is one thing about conservativeness that needs be noted to avoid confusion. It is not uncommon that we introduce definitions of concepts, or entities, partly because of previous misconceptions and/or misunderstandings. The definition, as such, is supposed to bring clarity to a situation where there was confusion. However, given that such definitions actually add something to what is previously known or thought, it may seem as if the criterion of conservatism cannot be satisfied. This is, of course, the reason why a new definition—as previously mentioned—ought to (i.e. need to) be supplied by arguments that makes it sensible, and conservativeness can then be retained relative to those arguments. In such cases what one does—and what I hope I have done in my papers—is to show that there is confusion that can be resolved by adapting a definition that is true to the clarity of how we should understand some particular concept or conception. Technically, Belnap defines conservativeness as relative to the definition as such (see, e.g., p. 135-138).

Belnap’s criteria can certainly be questioned. Indeed, it is possible to construct definitions that satisfy the criteria, but should be considered bad (e.g., because they add redundant content). However, I will not expand on this issue here. Other quality criteria that have commonly been considered are:

1. A definition must give the essence of that which is to be defined.
2. A definition must not be circular.
3. A definition must not be in the negative when it can be in the positive.
4. A definition must not be expressed in figurative or obscure language. (Suppes 1957: 151)

These criteria can also be questioned (see, e.g., Gupta 1989 for a discussion on circular concepts and Burgess 2008 for discussions on benign circularity).
Finally, the connective (Ω) can vary with different applications. Standardly, we seek a definition that supplies necessary and jointly sufficient conditions, requiring an equivalence relation, but for certain purposes it may be appropriate to define only necessary or sufficient conditions. For example, in Paper V, I introduce what I call the ‘common view’, which shares a few necessary qualities of previous definitions of anonymity. The common view, hence, defines only necessary conditions. However, for most common applications, neither sufficient nor necessary conditions alone are considered sufficient for a proper definition (i.e. the necessary and jointly sufficient conditions for a proper definition are necessary and jointly sufficient conditions).

That ends the brief overview of basics formalisms for definitions. We now turn to an overview of a selection of some of the different possible kinds of definitions (most of which are relevant for this thesis).

**Appendix. Part B. Different kinds of definitions**

A standard way of distinguishing between definitions is to distinguish between nominal and real definitions.

A nominal definition is concerned with meaning(s) of words, while a real definition is concerned with objects or concepts. The specific terminology seems to originate from Locke’s distinction between real and nominal essence (cf. Gupta 2015), although similar conceptual ideas were prominent already with Plato.

Robinson (1950) distinguished between word-word, word-thing, and thing-thing definitions, in which the two former are nominal, and the latter is real. However, we often use words to qualify which thing that is defined as that thing. That we use words does not imply that the definition is nominal, the question hinges on whether it is about the words or not.

Gupta suggests the following:

Perhaps it is helpful to indicate the distinction between real and nominal definitions thus: to discover the real definition of a term X one needs to investigate the thing or things denoted by X; to discover
the nominal definition, one needs to investigate the meaning and use of X. Whether the search for an answer to the Socratic question “What is virtue?” is a search for real definition or one for nominal definition depends upon one's conception of this particular philosophical activity. When we pursue the Socratic question, are we trying to gain a clearer view of our uses of the word 'virtue', or are we trying to give an account of an ideal that is to some extent independent of these uses? Under the former conception, we are aiming at a nominal definition; under the latter, at a real definition. (Gupta 2015)

While everyone agrees that there are nominal definitions, there have been, as previously noted, some controversies surrounding real definitions.

Another relevant distinction is that between the extension and the intension of a concept, C. The extension of C is all those objects that fall within the scope of C. In set-theoretical terms, the extension is all of the members of a certain set, C. The intension of C is a combination of essential, or jointly necessary and sufficient, criteria that each instantiation of the concept must have in order to qualify as C (cf. fn. 4, p. 19 for a, hopefully, simple explanation).

While the distinction between extensional and intensional definitions is useful, it is not, for various reasons, suitable for the classification of different kinds of definitions. I will list two reasons below.

First, these concepts are not completely mutually exclusive. A definition that is intensional can also be partly extensional (e.g., by defining part of the criteria extensionally). For example, many definitions of privacy identify privacy as having something to do with control and/or limited access, but the thing which one should have control of, and/or limited access to, is sometimes defined extensionally (see, e.g., Moore 2008).

Second, the concepts of extension and intension can also be used in another sense viz., as part of the evaluation of various kinds of definitions. As such, the distinction between intensional and extensional
definitions is orthogonal to the way various kinds of definitions can be qualified relative to the basic distinction between nominal and real definitions. For example, according to Gupta, there are three grades of descriptive adequacy of a (descriptive) definition:

- extensional, intensional, and sense. A definition is **extensionally adequate** iff there are no actual counterexamples to it; it is **intensionally adequate** iff there are no possible counterexamples to it; and it is **sense adequate** (or analytic) iff it endows the defined term with the right sense. (Gupta 2015)

Of course, on Gupta’s usages of ‘extension’, it is the actual, rather than the possible, extension of a concept that is indicated. This usage of the terms extension and intension differ slightly from the terminology I previously introduced (see, e.g., fn. 4, p. 19).

Relatedly, one problem with the subdivision of extensional and intensional definitions is that one may fail to appreciate the interaction between the extension and intension in a definitional process. Extensional examples often serve the role of counter-examples. Thus, when performing conceptual analysis, it is often presumed that we know it when we see it, at least in the sense that we know a sufficient part of the extension of a concept so that it allows us to evaluate a proposed definition without adhering to circular reasoning. For example, in Paper II it is presumed that the extension of the concept of security (as it applies to information [systems]) is not contested, or at least not contested beyond a point that makes counter-examples futile. This also holds for definitions that are purely stipulative, since the relevant extension is often given by the purpose of the stipulation.

In philosophy, we do—on occasion—disagree about certain examples. Despite this, we often agree about a large part of the extension of the concept. It is by comparing a proposal for necessary and jointly sufficient criteria with such agreed-upon examples (and more contested ones) that we are able to see if the proposal has any “indisputable” (or disputable) counter-examples. (This is the process I discussed earlier, see, e.g., p. 19f)
Furthermore, it is often the case that disagreement stems from conceptual inaccuracy, imprecision, or obscurity. For example, despite the popularity of conceptualizing privacy in terms of ‘control’, proponents of control-based accounts of privacy often lack anything close to a substantial account of the concept of control (cf. Paper III, p. 155-169).

For the above reasons I will stick to the standard classification of nominal and real definitions. Amongst the nominal and real definitions, we can identify a few different definitional types. I will explicate the major ones briefly below.

**Lexical or dictionary definitions.** Lexical or dictionary definitions are nominal. A lexical definition reports the meaning of a word as it is commonly used. It is common to classify dictionary definitions as lexical definitions, although dictionary definitions do not always precisely, nor exclusively, report the common usage; rather they are sometimes prescriptive to some degree, e.g., by (more or less) correcting mistakes which have become common usage (cf. Robinson 1950, Gupta 2015).26

**Stipulative definitions.** Stipulative definitions are standardly nominal. They are simply, and strictly, pure stipulations. They are often used to introduce terminology that will be used in a particular context, such as by ‘x’ I will mean ‘…’. Stipulative definitions are sometimes prescriptive (i.e. it is often the case that by saying by ‘x’ I will mean ‘…’ you also prescribe to the readers that they should use your stipulation, at least in the given context). It is an interesting philosophical question—that I, however, will ignore—whether real definitions can have a prescriptive element (cf. Gupta 2015, Robinson 1950, Harris and Hutton 2007).

**Descriptive definitions.** According to Gupta:

> Descriptive definitions, like stipulative ones, spell out meaning, but they also aim to be adequate to existing usage. When philosophers

---

26 Note that I do not treat ‘prescriptive definitions’ as a separate kind. While a definition may certainly be prescriptive in itself (because it defines a rule or a norm), it is, however, debatable whether prescription such as you ought to use definition x can be seen as part of a definition as such, or if it is a separate proposition about the definition. Given the potential controversy, I avoid the issue here.
offer definitions of, e.g., ‘know’ and ‘free’, they are not being stipulative: a lack of fit with existing usage is an objection to them. (Gupta 2015)

That descriptive definitions “aim to be adequate to existing usage” (ibid) does not mean that they are lexical, the exact relation here is a debatable question. But it is minimally necessary that we aim at the same entity, e.g., water, as the colloquial use of the word ‘water’, does.

As previously noted (and quoted above), Gupta distinguishes between three kinds of descriptive adequacy: extensional, intensional, and sense. Gupta uses the classical example of water as H2O, which supposedly has no actual counterexamples. Further supposing, as some philosophers do (e.g., Kripke/Putnam) that if water is actually H2O then it is so necessarily, i.e. it follows that it has no possible counterexamples. However, although a definition of water as H2O is thus both extensionally and intensionally adequate (using Gupta’s terminology), it is not sense-adequate, because it does not give use the sense of ‘water’. This is not what people mean by ‘water’. These criteria can reasonably be applied to both words and concepts, nominal or real.27

27 There is a complication here in the way that Gupta presents these criteria. I have moved this to a footnote not because it provides further explanation, but in order to avoid this complication in the appendix. Gupta claims that the definition “is not sense-adequate, for the sense of ‘water’ is not at all the same as that of ‘H2O’” (ibid). It is important to note how this conclusion relates to Gupta’s classification of descriptive definitions. He criticizes the sense-adequacy of defining ‘water’ as ‘H2O’ because the latter lacks the sense of the word, i.e. ‘water’. But focusing only on the sense of the words ‘water’ and ‘H2O’ betrays a relevant difference. Clearly, no-one would claim that ‘water’ (i.e. the string of symbols that make up the word) is ‘H2O’; although many may claim that ‘water’ is a name for H2O, while others would claim that water is H2O. Supposedly Putnam/Kripke held/holds the latter view (see, e.g., Kripke 1980). The difference here is whether or not we focus on a descriptive definition that is nominal or real. It seems that Gupta’s criteria are, as formulated, nominal. The usage of quotation marks certainly seems to indicate that, but it may depend on whether we could interpret Gupta’s notion as indicating concepts and whether concepts are nominal and/or/or only real. However, if there are real definitions, then there should certainly be real definitions which are also descriptive (i.e. real descriptive definitions). Supposing concepts are real, rather than nominal. It then follows that a real definition describes (if successful), e.g., a concept or a kind, while nominal descriptive definitions would describe a word (mutatis mutandis depending on alternating views on concepts). Real descriptive definitions are, arguably, the kind of definitions that, e.g., chemists are.
However, while philosophers often do think that there is an important relation between common sense usage, or intuitions, of a word and the best possible conception of its related concept, it is not always the case that such usage, or intuitions, supply relevant counter-examples to a conceptions of the concept which a word supposedly expresses, because the conception is often meant to improve upon common usage or previous conceptions. This brings us to Carnap’s explicative definitions.

Explicative definitions. In the words of their inventor/discoverer:

explication consists in transforming a given more or less inexact concept into an exact one or, rather, in replacing the first by the second. We call the given concept (or the term used for it) the explicandum, and the exact concept proposed to take the place of the first (or the term proposed for it) the explicatum. The explicandum may belong to everyday language or to a previous stage in the development of scientific language. The explicatum must be given by explicit rules for its use, for example, by a definition which incorporates it into a well-constructed system of scientific either logicomathematical or empirical concepts. (Carnap 1962: 3)

Arguably, it is often the case when philosophers are doing descriptive definitions that they are also partly explicating a previous conception, or correcting the common understanding of a word/concept/entity. In Paper II, one could say that we aim for a descriptive definition, but that we are also doing an explication (since we improve on previous conceptualization of security).

Explicative definitions can, arguably, be both real and nominal, depending on what we explicate (e.g., a word, a concept, or an entity respectively).

interested in. The definition of gold—in chemistry—is not a definition of the word (‘gold’), but of the actual thing (gold). However, it is debatable whether Gupta’s concept of sense-adequacy applies to real definitions. If applicable, the idea would be that while Gupta’s example focuses on the sense-adequacy of nominal descriptive definitions, the sense adequacy of a real descriptive definition would focus on the sense of the concept or entity, not the word.
Ostensive definitions. Ostensive definitions are the kind of definition we use when the answer we give to questions like “Who is x?” is an action such as *pointing to x*. Ostensive definitions can arguably be both real and nominal, depending on whether it is a response to a question about what a word refers to, or about what thing some entity is. An ostensive definition is arguably often a special case of an extensional definition, since it (most commonly) points to a particular extension of a word/concept/entity, rather than to the whole extension. Sometimes, of course, with an addendum, e.g., red is *that* (*pointing*) kind of color. While philosophically interesting, ostensive definitions will not be dealt with in this thesis.

Finally, given what I have said so far, it is reasonable to ask what kinds of definitions that are used in thesis’ five papers. For example, what kind of definitions am I proposing? In all of the papers, you will see different kinds of definition. For example, various concepts that I use in the analysis are stipulated (and adapted for the given purpose). However, if we turn to the actual main definitions (i.e. what the papers are about, the result of the analysis), then all of the definitions are compatible with various presumptions about definitions. All of the proposed main definitions can be read as, e.g., descriptive, explicative, or stipulative. The definitions can be viewed either as nominal or as real. However, the definitions are obviously not ostensive and the aim is not to provide purely lexical accounts either.

The main definitions are descriptive in the sense that they aim to describe the defined concepts. They are explicative in the sense that they aim to improve on previous conceptions or concepts. Supposing that the definitions are nominal (rather than real), they could be viewed as stipulative if we suppose that a nominal definition is either lexical or stipulative (see, e.g., Hansson 2006: 6). However, given what has been said above this choice is not necessarily binary. While I would not call my definitions purely stipulative (nor lexical), if one does consider the definitions stipulative it is important to keep in mind the normative
assumption (i.e., supposing that they are stipulative, the aim is to supply the best possible stipulations).

On my view, the best way of describing what I do it is that I aim to explicate and describe the best possible conceptions of the most relevant concepts.³⁸

This ends the appendix and, hence, the whole introduction. I hope that you are now eager to turn to the five papers.

³⁸ Note that the descriptive nature of the definitions apply even in the case when I define normative concepts, for the aim is to describe those concepts.
References


