

# 1. Introduction: Diana's onlife world

---

## 1.1 NARRATIVE BEGINNINGS: DIANA IN THE ONLIFE WORLD

*Early morning* Diana wakes up to the sound and light of her alarm clock that has been tuned to her mild winter depressions, lifting her mood by an increasing intensity of light and massaging her brains with music that has been shown to invigorate her at that point of the day. The house has woken up slightly earlier (turning on the heating, setting the coffee, and sorting out upcoming assignments and incoming communications). While she goes about her morning routine the house picks up her mood and prepares the roadmap for her smart car, depending on whether she is ready for a high adrenalin ride that may save her time or would prefer a routine trip that will take longer due to traffic jams. The fridge compares notes with her cupboards on this morning's caloric, fibre and nutrient intake to calculate how she could balance her diet during the rest of the day – forwarding the daily diagnosis to her smart phone, which will get in touch with whatever food store or restaurant she may decide to visit for lunch or dinner.

After walking the dog Diana is advised to take public transport as the house finds her nervous and a potential risk for dangerous driving. Diana is free to take the car – since the inferred danger does not cross a certain threshold – but her insurance premium may rise if the car indeed detects fatigue or risky behaviour. Besides, if she takes public transport she will burn more calories, thus allowing an extra serving of her favourite pasta or whatever else she may like to have later that day. So, Diana opts for the light rail that takes her straight to her first appointment.

*What's in a name?* The first appointment has been confirmed by her personal digital assistant (PDA), that is distributed between her smart phone, the system running her smart home, the smart car, her ubiquitous computing office platform, while being on speaking terms with other systems, like those for traffic control and healthcare, commercial and governmental service providers, as well as monitoring systems for private and public safety and security. The close relationship between Diana and

her PDA has caused her to give it a name, a common habit amongst those who have entrusted a variety of tasks to their PDAs. Hers is called Toma. When she thinks of it, Toma is like a friend, a close member of the family, a butler and – sometimes – like a government official or an insurance broker. Whatever the likeness to all these others in her life, there are many differences also, one of which is that no other person has so many details of her private and social life and no other person provides so much calculated advice. Though she is keenly aware that Toma is not a person and though she ‘knows’ that Toma does not ‘care’ about whether Diana follows its advice, for all practical purposes Toma often does resemble a person. Especially since the software has been updated with synthetic emotions, Diana experiences feelings of joy and pride, as well as regret and shame when she is rewarded or rebuked for her behaviours.

*Mobile office life* During the ride in the light rail Diana picks up on the details of her meeting, scanning the automatically composed summary of a report, sent to her office late last night – uploaded into Toma, which has put the doc onscreen on the back of her suitcase (monitors and terminals have been replaced by surfaces capable of displaying text, graphs and images). The report has its own summary, authored by the consultant who wrote the report, but Toma has a personalized algorithm that screens the doc for novel insights or unfamiliar facts. It skips conventional knowledge and highlights what is relevant for Diana’s inferred purpose. The summary works with images, graphs and text, to visualize patterns found within the doc that may be relevant for Diana.

When Diana enters the office she is greeted by the receptionist, with whom she has a friendly chat (Toma has arranged this, knowing that this will relax Diana who still seems nervous). She runs into two colleagues on the way to the working spot that has been allocated for her meeting. They discuss the targets set for the upcoming period, exchanging views on their feasibility and informally testing each other’s competitive advantages. Diana is a sales representative of a large hotel conglomerate, working on the high end of the market: selling classy hotel apartments on a time-sharing basis. Part of her salary is fixed; the other part depends on her actual achievements. Due to the general downfall of the economy – we are talking about the aftermath of the 2020 financial crisis – everyone knows that the least effective sales executives will have to leave. Toma notes that the talk with her colleagues leaves Diana full of energy: she senses that she has been doing very well compared to the others. This triggers an intervention in Diana’s agenda for the day; Toma schedules a lunch meeting with a troublesome client that has been trying to contact

Diana. Because of her nervousness Toma has been slow in responding, but now the PDA sees a chance.

*A call for help* Diana's day continues in a perfunctory manner. Her meetings work out well, including the lunch, and at the end of the day she is both tired and deeply satisfied. Riding back home in the light rail Toma registers a call from her ex-husband about their 6-year-old daughter Lindsay, over whom they have joint custody. Since the call is not urgent but must be answered tonight, Toma does not bother Diana until she reaches home, giving her time to reset after a hectic day. When she returns the call, Tom (her ex) asks her whether she can pick up Lindsay from school the next day, because he had an accident while playing squash with a colleague. Lindsay is staying with Tom this week, but as he will have to be at the hospital he hopes that Diana can take over. When Diana checks with Toma she encounters strong rejection; she has an important meeting with a client who will not appreciate a change of plan. Toma has already checked the regular nannies who might step in, but their PDAs are offline. Diana begins to exhibit signs of a mild panic, being confronted with what she sees as incompatible duties, and Toma comes to the rescue with a convenient solution: Tom will try to reach one of his nannies, while Toma will continue trying to contact those of Diana. Music sounds from the living room, as Toma has turned on the audio, programming some light jazz, known to soothe Diana's anxieties. It is the kind of music that is known to trigger Diana's sense of independence, downplaying her worries about being a good mother. Sensing her exhaustion Toma has ordered a meal that combines a tasty bite with the right balance of calories, fibres and nutrients: a fusion of a yellow Thai vegetable curry and an Italian salad of arugula, balsamic dressing and Parmesan cheese. Diana pours herself a glass of Muscat white wine after having the food and her mind finally drifts off into a pleasant oblivion. Tom has found a nanny for Lindsay, though he would still prefer that Diana take over, knowing that Lindsay is easily upset with a change of routine and would prefer to be in her mother's ambit. Toma decides not respond to the message, thus preventing it from reaching Diana. The PDA infers that it is in Diana's interest not to worry over her daughter, assuming that Lindsay will be in safe hands anyway.

*Of mother and daughter* The next day Diana receives an alarm message from Lindsay's school – requesting her to respond as soon as possible. PDAs have a default setting that allows five persons to override whatever the PDA infers to be a correct response, bypassing the filters of the PDA with an immediate sensory input to its user. Diana gets a small electrical

shock in her left underarm (signalling an alarm from her daughter) and picks up her smart phone. Toma is temporarily set back to a passive mode, registering Diana's behaviours but unable to interfere until Diana switches off the alarm. It turns out that Lindsay has fainted and – according to her PDA – is showing signs of anxiety and confusion since she woke up this morning. To recover and rebalance, Lindsay's PDA urges that her mother comes over and takes charge. Diana instructs Toma to cancel her appointments for the day and sets off to bring Lindsay home from school. Though Toma strongly advises against driving, Diana takes the car because this gives her a feeling of control. Halfway the car begins to slow down, warning Diana that she is crossing the threshold of dangerous driving, meaning that within 5 minutes the car will stop functioning. Diana pulls herself together, focusing on the traffic and calming herself with the certainty that she has made the right decision. The car responds positively by returning to the default mode, allowing Diana to finish her trip to school.

When Diana approaches the school Toma signals her arrival to Lindsay's PDA (called Dina). Dina registers an immediate relief in Lindsay, who has been taken to a small office next to the director's office. Her heartbeat and breathing return to normal, muscle tension is reduced and stress hormone levels diminish. As part of a public-private research programme all children are monitored in terms of their behavioural biometrics, especially the workings of the autonomic nervous system. It is hoped that this will allow prediction of various diseases, ADHD, depression and psychopathology in adult life. Such predictions could eventually justify early intervention to prevent undesirable developments, paving the way for a less conflict-ridden society. The immediate justification for the monitoring, however, is the chance to anticipate behaviours, making it easier for the PDA as well as parents, nannies, teaching staff and doctors to tailor their responses to the child. All significant others and professionals that are in contact with the child have context-specific access to parts of the database that stores and aggregates the child's states and behaviours. From the age of six a child has partial access to her own data, which access gradually extends to full access at the age of 14. This includes access to the group profiles that her data match with (indicating potential health or other problems).

Before Diana reaches Lindsay, the director of the school invites Diana into his office for a brief talk. He expresses serious concern about the mental well-being of Lindsay, based on the type of group profiles she matches. Her behaviours and biometric data match with personality disorders that could seriously interfere with her ability to focus on schoolwork and hamper her social life. In his opinion Diana and Tom

will have to work out a more structured life for Lindsay that would restore her self-confidence. Diana listens to the director and tells him that she will consult with Tom, though they have already made every effort to structure their own lives for the sake of Lindsay. Both have demanding careers, which they cannot give up easily, since this is how they can afford the excellent school that Lindsay attends. Diana goes to her daughter who is very happy to see her mother and glad to come home with her. They spend the afternoon having tea and some healthy snacks, exchanging gossip about school, taking the dog for a long walk and playing with some of Lindsay's favourite non-robotic dolls. They have both switched their PDAs to passive mode for the time being – wanting some undisturbed mother-daughter quality time.

Toma has contacted Tom's PDA to notify it of the changes of plans, such that the nanny who would have taken care of Lindsay can be called off without disturbing Tom (a message awaits him on his cell phone). Toma has also screened the coming week's agenda to assess how today's postponed meetings can be fitted in or replaced by teleconferencing. The PDA assesses the damage that this 'free' afternoon has caused Diana in terms of missed opportunities, delayed responses and loss of reputation.

*Animosity towards PDAs* Diana and Lindsay have had a long talk after their playful and restful afternoon. From what Lindsay tells her Diana gathers that she would rather attend a less reputable school if that were the price of her mother investing more time in her and less time in her career. Lindsay also objects to the fact that Toma often shields Diana from her daughter, as if there is some kind of competition going on for Diana's attention between the PDA and her daughter. When Diana tucks Lindsay in she promises her that she will think about these things and discuss them with her father, ending the day with reading her stories from one of her favourite books.

*Sports life* Later that week Diana goes for her weekly session at the gym. As the reader may guess, Toma has communicated with the gym and figured out which series of exercises would be best. Toma has noticed that Diana has been sitting at her desk for long working hours and has a stiff lower back that is giving her problems, so the exercises are tuned to warming and flexing the muscles of her stomach and lower back. The weights and other settings of the appliances in the gym automatically shift to Diana's preferences and Toma has calculated the duration of each exercise to prevent both under and overly strenuous exercise. All relevant biometrics are recorded, stored and communicated to Toma, as well as matched with relevant predictive profiles. To qualify

for a reduced subscription to the gym Diana can allow the gym to sell her data for marketing purposes, and to qualify for special services from her health insurance she can allow the gym to exchange her data with the insurance company. Also, if Diana consents, she can provide a personal profile that can be used to find matching profiles of other members with whom she could socialize after the workout. Some gyms have even integrated an optional dating service, hoping to increase their competitive advantage.

*Grandfather and robot* Jacob, Diana's 96-year-old grandfather, has a rather close relationship with the PDA that runs his household and monitors his health, but also serves as a social companion. This PDA is embedded; it is a robot. It does not look like a human being, but clearly resembles mammals. Jacob has named his caretaker Henry. It is constructed on the basis of soft robotics, meaning that its morphology helps to produce smooth and efficient movements, and the combination of hard and soft components mean that it will not easily accidentally hurt a human person. Henry can lift Jacob, and wash and feed him if necessary. Next to its soft morphology, its machine learning capacities enable it to sense what kind of pressure is effective in helping Jacob without hurting him. Jacob has developed a trusting relationship with the artefact. Actually they have a lot of fun. The fact that Henry spies on Jacob, to anticipate and prevent health risks, has given rise to a joking relationship because Henry also advises Jacob to cheat a bit on his diets if that improves his moods. Henry has learnt to jest with Jacob, when telling him that a small glass of single malt around 5 pm may interfere with his medication but will surely increase the quality of this life. To win his trust Henry has been known to keep some of Jacob's secrets from family and friends, though perhaps not from the insurance company that pays for his continued service. Jacob understands the deal and appreciates the privacy this affords him, even if it is a contextual privacy that does allow the insurance to remain up to date.

*Henry* Henry runs on proprietary code that keeps the device in continuous contact with proprietary online databases, while also enabling exchange of information with similar devices from the same service provider, and with a number of healthcare service providers (Jacob's family doctor, the medical specialists that treat his various conditions, the insurance that covers the cost, the pharmacies that supply his medications, and the local nursing centre that provides him with hands-on medical care). Henry is an example of what cloud robotics can do for us. Because of the complexity of the various relationships and their mutual

interference, it would obviously not be possible to program Henry in a deterministic way, and in fact it is also undoable to rely on supervised machine learning. Henry operates in part on unsupervised learning algorithms and neural nets that enable improvisation and creative negotiations between the various ends it serves: Jacob's health, the profitability of health insurance, data collection for medical research, Jacob's well-being and the various interests of his family and friends. Though its – largely autonomic – operations make Henry somewhat unpredictable, the overall performance is assumed to be better than it could ever be if human programmers had to foresee every possible scenario that might play out. To some extent the more unpredictable Henry becomes, the more reliable it is – though there are obvious limits to this. Nevertheless, Henry takes its own decisions, compatibilizing the various goals set by its designers. One of these goals is that Henry must sustain its own existence, since Jacob's life may depend on it.

*A robot decides* One day Jacob suffers a mild stroke. In the old days this might have gone unnoticed, as it is a minor infarct that does not immediately impair his health. Based on his connections with large databases, Henry has figured out that more serious harm is to be expected, statistically speaking. The obvious way to proceed would be to do some machine-to-machine talk with the agent systems of the various healthcare services mentioned above, to diagnose the health risks and to plan a possible intervention. On the basis of similar data mining operations, Henry, however, also figures out that Jacob will not appreciate the medical exams this would involve. Jacob may actually become depressed and he might even turn against Henry for telling on him. Henry tries to calculate the best decision and confronts conflicting interests of Jacob, the healthcare institution that 'uses' it to monitor and take care of Jacob, the insurance company that pays for Henry, and friends or family members who may want to guarantee him a long life.

Henry does not inform its patrons and two days later Jacob dies of a sudden and fatal stroke.

## 1.2 SMART ENVIRONMENTS, MODERN LAW AND TECHNOLOGICAL REGULATION

### 1.2.1 Why a Narrative to Introduce the Onlife World?

I hope that the narratives introducing the argument of this book will sensitize the reader to a novel type of anticipation and regulation

engendered by proactive ‘smart’ environments, often referred to as Ambient Intelligence (AmI), the Internet of Things, or ubiquitous, autonomic or pre-emptive computing. In this book the term *onlife* world will be used to highlight the fact that we are not merely talking about technological infrastructures. We are facing a transformative life world, situated beyond the increasingly artificial distinction between online and offline. To some degree, the upcoming *onlife* world thrives on artificial life forms, or at least on ‘things’ that seem to develop a life of their own. These ‘things’ display a form of data-driven agency, a concept that will be further developed in Chapter 2.

The narrative introduction has some likeness to the methodology of scenario studies, which aims to assess future developments that are as yet uncertain but warrant an assessment of potential threats. The idea is that scenario studies do not merely provide a random evocation of the fantasies of one or more Luddite techno-pessimists; nor should they be confused with the pink scenarios presented by business enterprise that often have more similarities with advertorials than a serious evaluation of both threats and potential benefits. Scenario studies are usually prepared by groups of experts from a variety of relevant disciplines to extrapolate existing tendencies on the basis of robust fact finding, while taking into account that black swans and outliers may appear if radically novel technologies are taken up by the market and integrated into everyday life.<sup>5</sup> In part, they are about expecting the unexpected. The storyline I composed builds on a series of scenarios prepared within the European research network on the *Future of Identity in the Information Society*, during a five-year research project of collaborating computer scientists, lawyers, social scientists and philosophers working in the field of cybernetics and information theory.<sup>6</sup> Its function here is, however, not to provide a sound basis for a report with policy advice on how to deal with Ambient Intelligence. I merely hope that by telling the story of Diana and some of her significant others, the reader begins to imagine how everyday life may change if our environment becomes saturated with pre-emptive technologies that are always one step ahead of us. Or so they say.<sup>7</sup> Though consumers may reject some of these technologies, it must be admitted that many of them are already part of our life world: from search engines to location-based services, from behavioural biometric access control for Internet banking to real-time dynamic pricing in smart grids or car insurance. In evoking the everyday effects of pre-emptive and interactive computing I hope to have clarified that the emerging technological infrastructure – like all technologies – will reconfigure our life world and *de facto* regulate our behaviour. Though enabling technologies such as large-scale data mining of online behaviours may be relatively

well known, others are still under the radar. Notably, the onset of radio frequency identification (RFID) tagging and a plethora of sensor technologies will interconnect offline and online data points, leading to what the International Telecommunication Union (ITU) has called the Internet of Things. In the meantime, while Google is working along similar lines towards a Web of Things, advanced robotics is moving into a new phase by tapping into the cloud. If we reach the point that close to everything 'anyware' is translated into machine-readable data points, stored in distributed databases that allow for the application of massive and recurrent pattern recognition techniques, we will indeed have entered an era in which Diana's story is no longer science fiction. The invisible inferences of personalized risks and preference profiles will increasingly afford seamless, unobtrusive and subliminal adaptations of the environment to cater to a person's inferred preferences and to target, include or exclude her on the basis of inferred risks.

The reader may actually find the stories mildly interesting and hardly surprising, thereby testifying to the topical nature of the narrative and the extent to which mobile smart phones, a plethora of Apps, news of self-driving cars, ambient lighting systems and remote control of home appliances have already transformed our expectations. Let's note that though a PEW report shows that a majority of Americans is highly interested in self-driving cars, experts still doubt that they will be capable of safe driving in densely populated urban areas.<sup>8</sup> I have deliberately avoided stories of grand misfortunes or attacks that we do not already meet in our everyday lives; the opening narratives will be used to expound on the subliminal and 'agential' character of smart technologies. In Chapter 4, I will raise a number of questions originating in the narratives, after clarifying the novel dependencies on Big Data Space and the digital unconscious it constitutes in Chapters 2 and 3. This will open the floor for a discussion of the threats of hidden complexity and unbridled artificial intelligence in Chapter 5.

The point of writing this book is to make clear that the extent to which this subliminal regulation takes place will depend on *how* we design these infrastructures and whether we find ways to inscribe legal protection into them. I will argue that the attempt to impose administrative written rules to domesticate these infrastructures is bound to fail, to the extent that written law *by itself* is impotent in the face of the distributed, mobile, polymorphous and real-time character of smart computing environments. As will be clarified in the third part, this does not imply that written law is a relic that is ready for exhibition in the museum of bygone historical artefacts. Quite the contrary, to keep a clear eye on the normative architecture of the onlife world and to enable each of us to

participate in its making, we will need to preserve the affordances of written law.

### **1.2.2 The Nature of Modern Law**

This raises the issue of the nature of law as we know it today. Modern law is an authoritative way to regulate life within a specific jurisdiction (regional, national, international). In a constitutional democracy law is a form of self-regulation: the addressees and the 'addressants' of legal norms coincide. This is the normative assumption of a democracy, even if citizens' participation in law-making takes place via voting, deliberation in the public sphere and stakeholder consultations, and even if not every citizen is addressed at all times by all the legislation that has been enacted. At the same time this assumption is what must be achieved, since it cannot be taken for granted. What counts is that legal norms are in principle made *by* as well as *for* the constituency and to have 'force of law' they must be public in the sense of being visible and legible for every person that is expected to comply with them. This makes it possible to discuss and contest their application, for instance by violating them. The violation of legal norms has consequences, sometimes even automatically. If I do not register my marriage with the civil registry there is no marriage; if I do not register my real estate in the register I cannot own the estate. Other consequences can take the form of a fine or the need to pay compensation. Typical for the Rule of Law is that a person can contest the application of legal consequences in a court of law, and this contestation may even regard the validity of the legal norm that is involved.<sup>9</sup> One can, for instance, claim that the norm violates a higher norm, like a human right or a constitutional liberty. Written legal norms are externalized norms, a feat that makes them amenable to interpretation, extension and change. In as far as legal norms are unwritten they may be less visible, more subliminal and harder to contest. However, the typical combination of written and unwritten law has enabled discussions of the unwritten principles that are implied in the written legal rules as well as the legitimate expectations that often determine their applicability.

Legal norms in a constitutional democracy thus exhibit three aspects that are pertinent: first, legal rules are established by a democratic legislator; second, they can be violated; and third the violation and its legal consequences can be contested in a court of law. These aspects differentiate law from discipline or mere administration. Self-rule, disobedience and contestability are the hallmarks of law in a constitutional democracy.

### 1.2.3 The Nature of Technological Regulation

Technologies regulate our behaviours by making certain behaviours possible and constricting others. The regulation that stems from technological artefacts is less obvious than enacted legal norms, and not initiated by a democratic legislator. Its regulative force depends on how engineers, designers and business enterprise bring these artefacts to the market and eventually on how consumers or end-users engage with them. Its material and social embedding has a way of inducing or inhibiting certain behaviour patterns, such as the sharing of personal data. Depending on their design and uptake, technologies can even enforce or rule out certain types of behaviours. Once a default of usage has settled, artefacts like typewriters, traffic lights, mobile phones, speed bumps, smart fridges and search engines impact the way we interact with each other, often enabling types of interaction previously not possible or ruling out alternate ways of doing things. This does not presume technological determinism. I have a choice not to have a mobile phone and even if I have one, there are many different ways in which I can use it (prepaid or subscribed; having different phones for private and professional calls; with or without Internet access; discussing confidential matters in the train or the details of a shopping list, and so on). But once defaults have settled resistance becomes more difficult and expectations of how things are done consolidate.<sup>10</sup> In that sense socio-technical infrastructures have a normative impact, if normative refers to the mutual expectations that regulate human interaction. As far as the communication and information infrastructures (ICIs) of human society are concerned this regulative impact can hardly be overestimated. The script, the printing press, mass media, the digital computer, the Internet and the world wide web extend the potential of spoken language exponentially. The possibility of addressing another person across ever larger distances in time and space, enlarging the potential audience of a text, has changed the amount of people we must somehow take into account when communicating and has extended the implications and consequences of our actions beyond measure. The latest developments, like email, chat and social networking, seem to conflate time and space into a synchronized environment that allows for 'always on' real-time accessibility. Pre-emptive smart environments begin to transform our dealings with artefacts. At some point we will become aware of the fact that we are being watched and anticipated by machines and we will try to figure out how the infrastructure 'reads' us and with whom it shares its knowledge of our preferences and of the risks we incorporate. One of the issues this book faces is whether we *will* manage to figure this out and what it would mean to live in an online

world that anticipates our behaviour whereas we don't have a clue as to how we are being profiled.

Technological regulation thus differs from legal regulation based on written and unwritten law. It does so on all three accounts. First, its articulation is not controlled by the democratic legislator and there is no legal 'enactment'. Technological regulation is often a side effect of a particular design aimed at a specific functionality. For example, the invention of the cookie by Netscape in the 1990s was meant to enable ecommerce transactions between a web shop and a customer. In the end it facilitated tracking and tracing web users across the web, enabling analytics that are used to personalize search results, websites, pricing strategies and newsfeeds. Cookies in fact regulate our online environment in the sense of creating new affordances and constraints, and despite the far-reaching implications of the subliminal adaptation of our online world, we never got to vote on this. Second, it is quite possible to design technological devices in ways that rule out violating the rule they embody, even if this embodiment is a side-effect not deliberately inscribed. If I cannot access a website unless I accept tracking cookies, I am practically forced to comply with the norm that I should accept them if I wish to access the site. Legal norms do not rule out disobedience. Third, contestation of the technological defaults that regulate our lives may be impossible because they are often invisible and because most of the time there is no jurisdiction and no court. If an online social networking site uses tracking cookies to measure the clickstream behaviours of their visitors, they may use analytics to measure the influence of different settings of their platform. This may even include sending false newsfeeds to their users to measure the impact of either positive or negative feeds. As such measurements are mostly invisible we have no way to contest them, unless the results happens to be published in a scientific journal.<sup>11</sup>

### 1.3 CRIMINAL LIABILITY, SECURITY AND GOVERNMENT SURVEILLANCE

The last part of the narrative raises the issue of criminal liability in the onlife world. It was added to draw attention to the agency characteristics of PDAs, and to underline that the decisions made by our digital companions can easily have far reaching consequences. From a legal perspective this connects to intricate issues around civil and criminal liability, to the legal subjectivity of artificial agents and the disruptions this may engender for foundational legal concepts such as causality, legal

personhood, liability, guilt, wrongfulness, and so on.<sup>12</sup> In this volume I will focus on the potential disruption of the substance of various human rights by the operations of the onlife world. In that context I will come to discuss the presumption of innocence and due process, but the matter of criminal liability is not part of the argument as this would extend the scope of the book and turn it into a hotchpotch.<sup>13</sup>

The same goes for two other topics that are closely related and obviously part of the disruptions generated by an onlife world. The first is the exponential increase in the need for security in the technical sense of resilience against attacks that violate the confidentiality, integrity and availability of digital systems. The onlife world depends on interacting computational systems that are vulnerable to hacking, spying, a manipulation, identity theft, eavesdropping and destruction. This goes for the smart fridge, but also for the smart grid, healthcare and other critical infrastructure. The costs of providing additional security if it is not taken into account from the very start are huge; both in financial terms and in terms of harm, if things go awry. The relationship between security and liberty should not be described as a trade-off, as the one often depends on the other and trade-offs depend on distribution; it may be that some people give up their liberties to provide others with added security.<sup>14</sup> Criminal law and surveillance are meant to secure safety, which is in fact a broader notion that includes absence of physical harm, whereas safety is not restricted to being safe from an attack. An earthquake threatens the safety of inhabitants but does not depend on an attacker. The collaborating distributed computing systems that scaffold the onlife world may be prone to system breakdowns with incalculable effects, threatening our safety irrespective of attacks. All this is highly relevant but hardly integrated in this book's argument. To tackle the issues involved would have taken another volume, which may become my next project.<sup>15</sup>

Finally, surveillance is at stake throughout the volume, but not in a straightforward manner. I am not sure that 'surveillance' captures what this book is after, as the notion suggests a simplified scheme of those who snoop and those who are snooped upon. I rather liked Solove's point when he proposed that the metaphor of Big Brother does not clarify what is at stake in the world of large-scale databases and the detailed personal dossiers they make possible.<sup>16</sup> Solove put forward the metaphor of Kafka's *Trial* as a more apt depiction of the anonymous accusation that looms over the lives of those that keep leaving traces of anything they do. He was one of the first who pointed to the chilling effect of knowing that whatever you do may at some point be used against you. This is part of the argument in the current book, and we should remember that any data anywhere may at some point be accessed by a government. Snowden has

done us the favour of underlining that it is an illusion to think that if the data is available governments will shrink from accessing it, if they believe it will help them in securing policy objectives.<sup>17</sup>

These policy objectives are not restricted to international terrorism or serious crime; they often boil down to more mundane efforts to combat social security fraud or tax evasion. In the context of foreign intelligence we should think of, for instance, industrial espionage, even if this is obviously entirely unlawful under the tenets of international law.<sup>18</sup> This book does not go into details of government surveillance, which should fit a volume on security in the broad sense of resilience against attacks. The analysis and the argument made in this book should, however make clear that the onlife world can be designed in a way that allows for massive spying and subliminal nudging. I believe it is now more important to devote detailed attention to the historical and theoretical underpinnings of the Rule of Law that should protect us from over-inclusive monitoring, than reiterating the fact that governments are overstepping their boundaries. We need to rethink these boundaries and the stuff they are made of.

#### 1.4 THE POLITICAL ECONOMY OF AN ONLIFE WORLD

This book is not about the politics or the economics of privacy.<sup>19</sup> What is usually termed as such tends to reduce the discussion of pre-emptive environments to a discussion of privacy, while framing the debate on privacy as part of a discussion of business models or political influencing. This amounts to taking for granted what should be investigated.

It does make good sense to situate the debate on the design of our onlife world in the larger setting of a political economy that generates an incentive structure that is highly conducive to manipulative environments that treat people as pawns, if not prey. Evgeny Morozov and Julie Cohen,<sup>20</sup> to name but two very different authors who come out with highly original and informative analyses on these issues, have done great work in providing the bigger picture, while refusing to frame issues in terms of existing incentives. They can thus open the discussion of what kind of world we want to fabricate in the era of what I will call data-driven agency. I have chosen to focus on the affordances of data-driven agency and the digital unconscious, as this already presents formidable challenges in terms of comprehension and potential solutions. I am, however, aware of the drawbacks of not addressing the political economy in which our technology developers must operate. The position

taken in Chapters 7 and 8, however, does address the relationship between law, politics and morality. Perhaps I am weary of the prevalent tendency to frame any and all discussion in economic terms, as if the ultimate question is always the one about the business model. I believe that we should not allow ourselves to be distracted when investigating the impact of pre-emptive computing on the life of the law. After determining what normativity we need to survive as reasonably free and reasonably constrained individual persons, we can decide how to distribute the costs as well as the benefits. I am not qualified to do the maths on that, but I am convinced that the issue of distribution is first a political and a legal issue and only then an – important – economic problem.

## 1.5 A BRIEF OUTLINE

### 1.5.1 Part I: Data-driven Agency

The first part deals with data-driven agency as the most prominent and the most transformative aspect of smart technologies. After the narrative introduction in Chapter 1 and the overview of what is at stake, Chapter 2 follows up with a discussion of different levels of ‘smart’. Smartness is analysed in terms of artificial agency. This leads to an analysis of Big Data Space as the distributed heterogeneous timespace on which data-driven agency thrives. Chapter 3 discusses the idea of an *onlife* world, where *things* ‘come alive’ to populate our everyday life world with novel animations. The information and communication infrastructure (ICI) of the *onlife* world is described in terms of pre-emptive computing systems that calculate our inferred future behaviours and engage in pervasive and continuous adaptations of our life world. One of the key terms of this ICI is hidden complexity.

The description of the *onlife* world is coupled with an analysis of human identity as a fragile, relational construct that feeds on a double contingency or a double mutual anticipation, deeply rooted in the *Welt* that springs from the use of spoken and written human language. Double contingency is what makes humans vulnerable to the socio-technical infrastructure of the *onlife* world. Being pre-empted without having the tools to foresee the predictive stance of embedded computing systems, turns double into single contingency, rendering human agents liable to invisible manipulation.

### 1.5.2 Part II: Threats of Border Control

The second part starts off with a discussion of the narrative that introduced the *onlife* world, based on the analyses of Chapters 2 and 3. It does so, in Chapter 4, under the heading of the digital unconscious, another term for the extended mind embodied in Big Data Space. Robots, smart grids, search engines, and the more, all tap into the cloud, to gain access to subsets of the Big Data that hover over and move between the data servers that ground the cloud. The narrative raises a number of questions when taking into account the role played by data-driven agency and pre-emptive computing. These questions basically involve issues of border control in smart environments that infer our future or even current behaviours. In Chapter 5, these questions are translated into a set of threats to the substance of core values of Western democracies, such as privacy, non-discrimination, fairness, the presumption of innocence and due process. Though these values loosely align with fundamental rights, this chapter does not take a legal perspective, saving the legal perspective for the third part of the book.

Part II ends, in Chapter 6, with an exploration of Japanese privacy practices, and Japanese dealings with animated environments. This provides us with a view from the other side of privacy, presenting it as a gift or obligation rather than an individual right. The crucial element in Japanese privacy practices is border control, which depends on the differential settings and rankings that underline the critical importance of what is called the ‘inbetween’ of human society. The chapter ends with an analysis of the difference between privacy as either a gift or an individual subjective right, thus paving the way for the third part that deals with the law.

### 1.5.3 Part III: The End(s) of Law

This part deals with the question of the ends of law, inquiring what aims define the mode of existence of the law. After an initial exploration, in Chapter 7, of different internal perspectives on the law, the chapter argues for an antinomian understanding of the law, defined as *aiming for* justice, legal certainty and purposiveness. These aims should not be reduced to each other and their incompatibilities in concrete situations should be acknowledged without attempting to overcome them, for instance by way of universalist solutions that favour any one of the aims over the others. Chapter 8 confronts law with technology, developing three conceptions of both law and technology to clarify their interrelationships with politics, morality and administration. These conceptions also help flesh out the

relationship between law and its technological embodiment in prevailing information and communication infrastructures (ICIs). The chapter concludes that modern law as well as the Rule of Law have been contingent on the ICI of the printing press. The identifying characteristics of both modern law and the Rule of Law are described as depending on the affordances of proliferating printed text. The challenge facing modern law is to reinvent the law in an environment of pre-emptive computing without giving up on the core achievements of the Rule of Law. This may imply that we build resistance into the architecture of the onlife world, against the lure of indiscriminate processing of personal data and the concomitant subliminal targeting of its inhabitants.

Chapter 9 plunges headlong into the legal framework of data protection, considering the added value of a fundamental right to data protection as distinct from, but contributing to, the protection of privacy, non-discrimination, the presumption of innocence and due process. It plants the flag of data protection firmly in the ground that covers the legality principle, using the myth of Odysseus and the Sirens to explain why data minimization, purpose limitation and profile transparency are critical for our survival in the onlife world. This brings us to Chapter 10, exploring the notion of Legal Protection by Design (LPbD) as a necessary re-articulation of the aims of justice, legal certainty and effectiveness in the emerging onlife world. Finally, two alternative ways of handling an environment infused with various types of artificial agency are introduced: counter-profiling and morphological computation. Law is not the solution to all problems and data protection is not a panacea. Nevertheless, without LPbD inscribed into the onlife world, the Rule of Law will not be sustainable.

