SIX

Lessons Learned

Introduction

We now bring the book to its substantive conclusion by considering what the previous chapters tell us about digital responsibilities and draw lessons that can be learned relevant to future digital policy making when our framework is applied. Applying the framework, the case studies can be understood as digital policy challenges in different ways:

- Chapter 3, Digital Safety, is a principal challenge of *realising responsibility* and specifically when responsibility is not realised, the state falls back on ascription of blame through the establishment of legal obligation and technological enforcement to achieve responsibility actions.
- Chapter 4, Digital Migration, is a challenge of *establishing responsibility* which does not create sufficient impetus for positive responsibility actions which then leaves vulnerable refugee communities looking to non-state for protection and digital support.
- Chapter 5, Digital Census, is a challenge of *actioning responsibility* to absorb the limited discharge of realised and established responsibilities by central and local government that created a lacuna which required civil society institutions and organisers to step in.

Five lessons can be adduced. First, even though all three case studies highlight responsibility actions, we argue that actions do not tell the full story about digital responsibilities. The actions are fragmented and must be understood in the context of realising and establishing responsibility. It is that context which helps to better situate and explain the actioning strategies across all case studies. Second, all case studies highlight the distributed nature of digital responsibilities including the distribution of responsibilities across infrastructural networks of digital technology that are governed by different legal and regulatory requirements. Responsibility distribution, then, is a key facet of each case study but also a key determinant factor in our focus on realising, establishing and actioning.

Third, the distributive nature of digital responsibilities also leads to lacunas across realising, establishing and actioning processes. Lacunas are absent spaces, devoid of responsibility allocation, which require actions to be taken by parties for digital technology implementation to take place. The lacunas that arise in the case studies are mostly at the actioning level where the positive actions of some parties obviate the attempts to avoid or refuse responsibilities by others. Responsibility lacunas are consequently important because they highlight the limits of both legal obligation and security technologies. Fourth, as the case studies show, the tried and tested response to legal and technical lacunas is force, either through legitimate state action in the establishment of legislative obligation or the use of security controls in digital technology. The case studies highlight the limits of legal and security forcing functions that essentially seek to bypass collaboration and consensus to achieve a responsibilisation outcome. Finally, we then consider the role that resource allocation by government and revenue generation by the private sector played in the case studies.

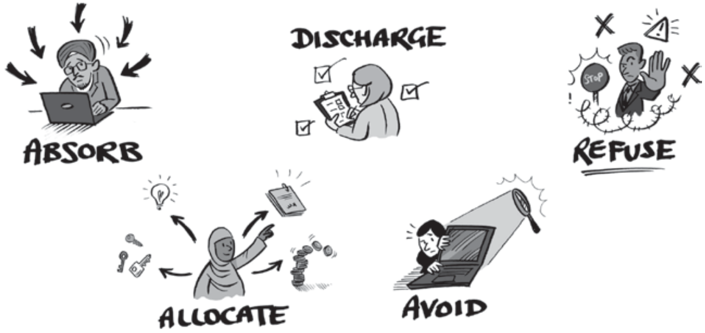
All of this leads to where we started our book with an overview of different responsibility frameworks. We contend that responsibility frameworks need to be understood differently, regardless of disciplinary orientation. Largely speaking, the traditional frameworks of responsibility are grounded in an older model of individuality that does not fully account for the multiplicities that arise from the digital context. As we show in our lessons learned discussion, ascription of legal rules and security controls will only go so far and therefore responsibility frameworks must be broader in their thinking about the need for consensus and collaboration. With that in mind, let's consider in more depth what lessons can be learned, beginning with what the case studies tell us about responsibility actioning and why it is important to understand actions in the context of realising and establishing responsibility.

Actions tell us a lot about responsibility (but not everything)

Chapter 2 highlighted different responsibility frameworks from different literature. It outlined that responsibility is an amorphous concept with tendrils that run deep into moral philosophy, social and political science, technology development and law. The tendrils run so deep that responsibility considerations tend to surface through actions. It is unsurprising then that responsibility frameworks are action-based, whether they be the blameworthy ascriptions of traditional legal approaches or their contemporary applications in responsibility gap analyses. Even contemporary frameworks, such as RRI, are grounded in the broader governance of responsible acts around technology development. Actions are thus an important way to conceptualise and understand responsibility. The actioning of responsibility also has the advantage for scholars of being visible which means it can be determined and measured to ascertain whether an individual or party is responsible for their acts or accountable with their obligations.

Actioning has an important role in our framework and we agree that a starting focus on responsibility actions is informative. Take, for example, the application of the case studies to the non-exhaustive list of responsibility actions that we proposed in Chapter 2. Doing so enables the seeing of

Figure 6.1: Responsibility actions



responsibility in a clearer way that specifically acknowledges the possibility of both positive and negative acts.

1. *Absorb* – the highest positive act as it seeks to fulfil the agreed consensus of the environment at potentially the expense of the individual party's own benefit. Several acts of absorption are identifiable from the case studies, particularly relating to the Digital Migration and Digital Census chapters. Civil society organisations in both cases voluntarily absorbed the established responsibility of other parties to provide extra support for vulnerable communities. Chapter 4 highlighted the actions of underfunded refugee-serving organisations and their attempts to extend the use of their own technologies to individuals and refugee communities. COVID-19 lockdowns exacerbated digital disparities and further marginalised refugees who were already struggling with the costs of internet access, device ownership and English language digital literacy requirements. In many ways, as highlighted in the chapter, the need for digital inclusion strategies for refugees was realised and established in international governance. Yet it had to be absorbed by community groups even in a broader society that was increasingly presented by government as 'digital-by-default'.

Chapter 5 also highlighted the extraordinary acts of care enacted through the support and outreach work of Kurdish community groups. The absorption of responsibility by those groups extended from the training required to successfully operate a rather simple digital solution to creating a shared cultural experience that assisted to allay the security fears of the Kurdish community. Absorption then is double fronted. First, there is the willingness to be responsible for the implementation of a digital measure that is essentially beyond the party's remit, but still within its capabilities. Second, and more importantly, there is the creation of a culturally safe environment to generate support and interest on the basis that it will carry longer-term benefits for the community. Both absorbing acts are way beyond the implementation strategies envisaged by the state.

2. *Allocate* – in this situation, parties take on responsibilities designated to them, and to others, to identify and share those responsibilities across environments. In many ways, responsibility allocation is a classic act of government and a key method for allocating responsibility actions is by the implementation of law. Digital Safety's coverage of the pre-legislative debates leading up to the OSA is a clear example. The allocation of new duty-based responsibilities to online service providers outlines the allocative role that traditionally government has played. Allocation, in this sense, was not based on the consensus requirements we called for in Chapter 2 and was ultimately forced upon perceived recalcitrant parties who were unlikely to bear responsibility for actions but were nonetheless best placed to implement. Equally, the co-ordination of community response, and the sharing of resources in relation to positive responses, was a key similarity in the Kurdish and civil society actions outlined in Chapters 4 and 5.
3. *Discharge* – refers to the baseline act of fulfilling or discharging a responsibility. The act of discharge sits in the middle of the spectrum because it can represent both positive and

negative acts. A discharge is thus contextual. An example of discharging behaviours arising from the case studies involves minimum level implementation strategies for refugee and asylum seeker digital services provided by local authorities. At times, these were bare minimum requirements in which it is questionable whether the established responsibilities were actually discharged. The same perhaps could be said about the provision of additional language capabilities in the census. The provision of a digital solution without the necessary support, training and community assurance required for implementation by the Kurdish community, could be viewed as a baseline discharge by the ONS.

4. *Avoid* – refers to the negative act of avoiding a responsibility that has been realised and established as relevant to a party. Digital Safety highlighted that many of the contentions arising from the OSA's fractious debates regarded online service provider attempts to avoid responsibility for the broader protection of digital environments. Consistent attempts to reframe problem construction as a matter of content moderation, in which individuals were better placed to respond, can be seen as an avoidance of engagement with the problems highlighted by all the other parties within the broader digital environment. Similarly, the actions of local authorities, and especially of central government, could be considered avoidance of responsibility in relation to the provision of digital services for refugees in Digital Migration.
5. *Refuse* – a definitively negative act of refusing to take on a responsibility that has been realised, established and actioned by other parties flowing from collaboration and consensus. The case studies show that the impact of avoidance and refusal acts means that realised and established responsibilities eventually emanate on individuals through responsibilisation strategies. As such, even though none of the case studies specifically involved a refusal action, the extent that different parties tried to avoid responsibility had the same sort of impact upon individual citizens, namely, to

> try to make them responsible for someone else's established actions. The attempts to make users responsible for content moderation by online service providers and the inaction of local authorities in both the Digital Migration and Digital Census case studies, led to the need for absorption and reallocation of responsibility actions.

Our focus on the actions arising from the case studies helps to better understand the dynamic nature of responsibility. An action in one context can give rise to the need for a different type of action in another. An avoidance of responsibility by one party gives rise to a corresponding need for absorption or reallocation by another. Responsibility then is diffuse, shifting and amorphous. It changes as the actors and parties in given environments respond differently over time. It is not surprising therefore that the varied academic attempts to understand responsibility begin with actions. However, as alluded to already, we contend that it is equally important to understand that responsibility does not end with actions. Focusing on responsibility as actioning does not conceptualise the true complexity of responsibility, especially in the digital realm. Actions alone do not tell the full story. They are fragments of realising and establishing responsibility and so it is important to take a step back and consider digital responsibilities beyond actions. Actions are a sensible and useful starting point but they do not explain the complete picture.

That is why our framework also gives weight and prominence to realising and establishing responsibilities. As the case studies show, how responsibility is realised and established, or not as in some case studies, can impact upon how responsibilities are actioned. Understanding responsibility as purely a process of ascriptive output does not encapsulate the broader collaboration and consensus requirements that realising and establishing processes speak to. Without those processes, responsibility allocation merely returns to the ascription of individual blameworthiness and the historicised projection of future obligation. All of which encourages an understanding of responsibility that is predicated on the use of forceful authority to ascribe obligation upon individuals whose ultimate role is to tacitly accept. We now contend that traditional model is made more challenging because of the distributive nature of responsibility in digital environments.

Distribution of responsibilities is inescapable

Our framework's focus on realising, establishing and actioning also outlines the distributed nature of digital responsibility formation. The case studies highlight that the formation of responsibility does not take place at one specific site and is formed through different processes. There is a clear relationship between the top-down focus of established policy positions and ground-up actions across all three cases. For example, in the Digital Census case study, the originating act of realisation began when the ONS employed a drop-down list for different languages in the first digitally focused census. The use of the drop-down list would have been based on an established legal justification and actions were taken on the ground by Kurdish community groups to ensure its successful implementation across the diaspora. Similarly, the Digital Migration case study highlights that responsibilities were realised and established internationally which required actioning by central government and local authorities. As noted in the chapter, the actual actioning of responsibility, like the Digital Census chapter, was undertaken by civil society organisations. Equally, the Digital Safety case study highlighted the shifting movements of responsibility imposition through legislative development.

Traditional legal models of responsibility are based on a rather unitary understanding of how responsibility is formed. Law is created, obligations are formed and individuals accept responsibility for legally bounded actions as a recognised social good for all. In one sense, this traditional model is still

Figure 6.2: Distributed responsibilities

partly relevant to understanding the case studies through our framework. There are clear acts of forcible ascription, most notably in the Digital Safety case study. However, ascription alone does not tell the full responsibility story. The state's ability to ascribe responsibility through legislative obligation is still, of course, a prime source of institutional authority. That has not changed, and we are not contending that it has. However, what has changed are the distributive capabilities of digital technology which now enable responsibilities to emerge through technological infrastructure. It is the infrastructure that allows responsibility to be formed and actioned across many different environments.

As we consider further, the pathways of digital responsibility formation are consequently pluralistic. Take the Digital Safety case study as an example. The formation of the OSA highlights the difficulties involved in establishing digital responsibilities. In one sense, it could also be argued that the realisation of responsibility was never fully accomplished because of the shifting nature of legal establishment. There is already a movement, or distribution of responsibility realisation, that shifts across different parties at contrasting times. The Bill's life germinated from the Online Harms

White Paper which had a multitude of harms that reached from national security to individual harms. The harms were so broad that necessary responsibility conversations were never fully realised, which helps to explain some of the difficulties arising for the Bill's establishment. Moreover, the Bill also entailed a confusing mix of command and hybrid governance that obliged online service providers to act but also allowed providers significant leeway to implement enforced duties. There was both an imposition of control through ascription and forms of delegation deemed necessary for a digitally distributed environment.

The different regulatory strategies at play highlight another factor pertinent to distribution considerations. The legal models of ascription, propounded by Hart and others, have traditionally guided how responsibility in a legal sense should be understood. As noted already, it was understood in a unitary sense which was representative of the forms of centralised institutional authority that characterised public policy and service delivery in the last century. We noted in Chapter 2 the effect that privatisation strategies had on understandings of responsibility formation in the context of responsibilisation, namely, by making citizens responsible for their choices and part-operation of services. The effect of privatisation, which Hart could not have contemplated, ranged from the decaying of the dominant public institutions that form responsibilities (Parliament, agencies, regulators, etc.) to the process of shifting responsibilities to the private sector and individuals. All these developments were silently predicated on a functional distribution model that now attached a range of responsibilities to different parties through digital infrastructure. New digital opportunities – digital census, monitored regulation of digital spaces, meeting the digital needs of the most vulnerable – equally came with a set of responsibilities for implementation that were now dispersed over location and mediated through infrastructure.

Contemporary responsibility frameworks, such as RRI, better contemplate the possibilities of distribution but they nonetheless do so from a confined perspective, namely, the responsible implementation of a given technology innovation, by a given set of actors. Even digital civics, with its much broader critique of public service delivery, does not consider the full consequences of responsibility distribution. We contend that our framework starts to capture these complexities. The case studies highlight how responsibility is distributed across different sites and realms through the interaction of the market as a government service delivery mechanism, including the absence of that mechanism and the impact on users, both as consumers and citizens.

The case studies also highlight the distribution of responsibility through the different processes of realisation, establishment and action. Movement of responsibility formation is fluid between these processes and is distributed dynamically. Finally, the case studies also show how responsibility is distributed across time, as the collaborative and consensus building elements of realising, establishing and actioning play out across different temporal frames. When all these aspects are combined, they demonstrate that responsibility formation is distributed, which requires a much stronger focus on collaboration and consensus processes.

The importance of lacunas

Chapter 2 highlighted a contested academic discussion about the existence and utility of responsibility gaps. To recap, there are two broad positions. The first, as espoused by Matthias and others, is that there is the potential for gaps of responsibility ascription in autonomous systems because there is no human decision maker that machine-based decisions can be ascribed to. In other words, the system has become so sophisticated that decisions are constructed in such a complex manner that they cannot be parsed to identify the causal relationship between output and human data inputs. It therefore becomes impossible

Figure 6.3: Responsibility lacunas

to ascribe responsibility to an individual in these circumstances. The ‘responsibility gap’ argument is not universally supported. Critics outline that even in complex automated systems it is still possible to ensure that a human is always made responsible for the outcomes of a machine-based output. The responsibility gap can be filled and responsibility can always be attributed. Responsibility is therefore constructed to meet circumstances rather than an accepted consequence of machine intelligence.

There are clearly some distinctions between the book’s case studies and the type of digital infrastructure envisaged as part of the responsibility gap analysis. The case studies do not cover or examine the prospect of autonomous machines. In that sense, the digital component to our case studies is relatively low level, such as the use of online drop-down forms or basic digital support needs. The contentions involving digital safety do, however, speak to the socio-techno visions of autonomous machines. However, the focus of contention is not about the prospect of autonomous machine activity; rather, it is about the business models of online service providers and the appropriate role of the state in regulating those models. The business models are, of course, built to combat scale and are largely automated in their data collection and analysis processes. Nevertheless, they are not of the complexity contemplated in the gap analyses. We therefore do not use our book to contribute to the ongoing and broader debate about whether responsibility gaps do exist, and if so, what they tell us about responsibility in a digital context. However, that does not mean to say that the concept of gaps has no relevance to our overall argument.

We believe our case studies highlight responsibility lacunas rather than gaps. A lacuna is preferred because it speaks to the idea of an absent part that thus draws attention to something, rather than a gap that is required to be filled. It is the drawing of attention that becomes the important aspect of our analysis. We do not believe that responsibility lacunas are bugs of the system caused by the inability to assign responsibility to a given machine output. To follow the well-trodden logic, lacunas are a feature, rather than a bug, in the formation of digital responsibilities.

Disruptions caused by digital technology and infrastructural implementation will always cause lacunas. In part, this is due to the disruptive nature of novel technological application which will give rise to unexpected uses and unforeseen consequences. It is also due to the distributive nature of digital responsibility allocation as already outlined. Put simply, distributed responsibilities advance the prospects of lacunas emerging because there are going to be points of digital technology implementation where it is unclear how the technology will apply and who will be responsible for actioning. We consequently believe that a digital responsibilities framework must operate within this reality and accept that the dynamic nature of responsibility as realised, established and actioned means that formation will not always be readily visible. As noted in the previous section, actions can be seen as fragments of realisation and establishment and are thus, by nature, incomplete.

Lacunas are important because they highlight responsibility contentions that need collaborative processes to form consensus. Lacunas, in this regard, are a positive aspect of responsibility discourse that help to realise and establish responsibility. Take, for example, the lacunas arising from the case studies. Digital Census details the absence of an educational support process to augment the positive implementation of language drop-down lists. Seeing this absence purely as a responsibility gap does not fully encapsulate the uptick of positive actioning that flows from the Kurdish community. The absence of appropriate support mechanisms was not considered by that community as a space where no responsibilities exist. Instead, it was viewed as an opportunity to extend existing community bonds and to contribute to broader policy goals through census data provision that would lead to greater recognition both locally and nationally. Much like the types of non-exhaustive responsibility actions that we highlight in our framework, lacunas can have both positive and negative effects. In the Digital Census, and indeed the Digital Migration case study, the recognition of a lacuna led to positive actions. Even in the Digital Safety case study, the lacuna arising from the attempted avoidance of responsibility by online service providers also gave impetus to legislators to act positively.

We believe the identification and analysis of lacunas is important in understanding the formation of digital responsibilities. These are not spaces that should be feared by policy makers seeking to implement policy or service delivery outcomes through digital means, particularly involving third parties. In fact, we believe lacunas have the opposite effect. They highlight spaces of potential contention, spaces of unwanted responsibility by some parties that do not by default have to be filled by responsibilisation strategies that automatically bestow responsibility on individuals. Digital Census clearly shows the willingness of community activists to absorb responsibility for educational support where little to none was provided alongside the implementation of digital innovation, albeit straightforward. The case study also shows the distributed nature of digital responsibility formation which takes place across different physical and digital spaces. Formation took place in the code behind a website and the various public and private sites in North London.

Lacunas are an important part of understanding the digital landscape, and in particular, the connection points between the digital and physical in which responsibilities are actioned. These are also the places that show the limits of digital technology reach. Lacunas can provide valuable insights for policy implementers about how responsibilities are formed across potentially diffuse parties with diverse needs and goals. We contend then that lacunas give rise to the possibility of dialogue that promotes consensus and may therefore reduce the need for forceful actions, whether through technology or legal means. We now consider that point further in the context of forcing functions.

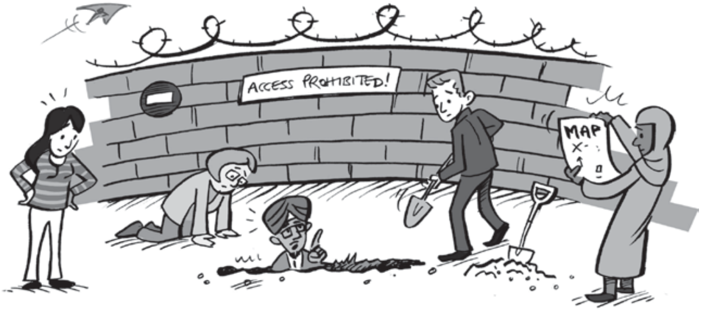
The limits of forcing functions

An under-discussed and under-researched area is the interaction between digital responsibilities and security technologies. In digital-first or digital-by-default societies, there is a reliance on security technologies to not only protect data, services and technology but to also implement or operationalise public and organisational policies. For example, consider welfare delivered as digital by default. Setting up an account on the digital welfare platform and using that account to access digital welfare services, make welfare claims and provide evidence of employment seeking, rely on technological security mechanisms. They can include: identification and authentication processes to verify that the claimant is who they claim to be; behavioural pattern monitoring that checks the verification of the claimant and validity checks against financial and open-source data to assess the likelihood of additional income. Traditional security mechanisms include identification and authentication, to ensure that authorised individuals can access services, data protection mechanisms to ensure confidentiality of data, and data integrity mechanisms, to ensure that data is not subject to unauthorised modifications. Even though these security functions can be extensive, as in the case of welfare monitoring, we nonetheless believe they are still limited in the context of digital responsibilities formation.

In addition to these traditional mechanisms, we have seen the growth of behavioural security mechanisms that use a combination of machine learning and AI to assess the authenticity of service user actions, to verify the assertions and claims that an individual makes about their circumstances and to assess the risk that the individual user is a threat to the system or service. Cloud computing and the development of sensor technology has also meant that these security mechanisms can draw on geographical, motion and biometric data to augment security control decisions. This contemporary paradigm of technological security controls has encroached on many aspects of our lives that were once thought of as separate and private and therefore require a greater degree of both trust and consent to work. Without trust and consent, such security technologies become a type of forcing function to push through the goals of public and organisational policy. When security technologies are used as a forcing function, the likelihood of workarounds, control subversion and non-engagement increases and with it the effectiveness of the security technology decreases.

Realising, establishing and actioning digital responsibilities in a way that is transparent and that creates consensus is an important means of increasing trust in state actors and

Figure 6.4: The limits of forcing functions



strengthening the effectiveness of security technologies. Reviewing our case studies, we can see that for security technologies to be used effectively to protect digital activity, and to enable individuals to safely access services, there needs to be consensus about where responsibilities lie and with whom. If consensus is not achieved, security technologies become less powerful because the duties and obligations necessary for them to be successfully deployed are absent. For example, in the case of age verification technology in Digital Safety, if no party recognises an obligation to ensure that such technologies are usable and accessible by all, individuals will be locked out of services and the technology will not be able to support the access control goal. Equally, if no party acknowledges that it has an obligation to respond to queries and potential errors in age verification, then the technology will not be able to support the access control. If no party ensures that age verification technology is deployed in a meaningful way, people will move to other, less controlled and potentially less visible, platforms leaving children more, rather than less, vulnerable to harmful content. Therefore, where there are lacunas, ambiguities and tensions in digital responsibility these should be proactively examined because such tensions can constrain the effectiveness of security controls and could thus inhibit successful digital policy implementation.

In some ways, the same could be said for the legal considerations outlined in the case studies. The pre-legislative development of the OSA highlights the difficulties involved in establishing digital responsibilities. In one sense, it could also be argued that the realisation of responsibility was never fully accomplished because of the shifting nature of legal establishment. The Bill's life germinated from the Online Harms White Paper which had a multitude of harms. From there, several tensions were perhaps never fully realised which helps to explain some of the difficulties arising for the Bill's establishment of responsibilities – for example, the transition of content harm to digital environmental protection that would have imposed new system-based positive duties on online service provider business models.

The development of the OSA, and indeed the other case studies, shows that even a strongly established piece of law does not necessarily lead to the successful implementation of the desired legislative outcome. This, of course, is well trodden ground in the public policy literature but we highlight it again now to outline the complex relationship between the attribution of state authority through the commanding of legislative obligation and the distributed nature of digital technology implementation. It is the uncertain combination of command and hybrid governance that can give rise to the type of responsibility lacuna we have already noted. In Digital Safety, it is the state that governs the shape and resolution of the absent part – to our mind the lack of consensus across all parties – with forceful authority. We acknowledge that this type of action is a constituent part of state authority. We are not defenders of the significant power that online service providers have amassed for themselves. Rather, we highlight this issue to acknowledge that use of law as a forcing function of legitimate state authority has limits due to the distributed nature of digital policy implementation. A better way of understanding the multifaceted contours of digital responsibilities is therefore required.

We believe that mapping digital responsibilities to show where there is discord as to where and how digital responsibilities should be ascribed and carried out is fundamental to the security analysis of a digital product and its use. Our case studies indicate that digital responsibility is defined at the intersection of: (i) the site where digital responsibilities are placed and (ii) the realm of activities that is underpinned by these responsibilities. The sites of digital responsibility (the state, the regulator, the market or the individual) are where obligations and duties are assigned. The environment's digital responsibility – information; content production and management; and design, management and implementation of technology – are where digital responsibilities are carried out. Our case studies show that there is a tension between the state, the regulator and the technology companies (represented by the markets) as to where responsibilities for the deployment and use of digital technologies should lie. Responsibility is pushed away from these competing actors and towards the individual technology user who has the least power to push back on the obligations and duties they are ascribed. We suggest that much could be done to better map where digital responsibilities are sited and for what realm of environmental activity. Such mapping could be an extension to existing security practices already included in technology design processes, user walkthroughs and technology testing.

Resource allocation and revenue generation

Our final consideration is the one that is most contentious, but one that we believe is visible from the case studies. It regards the role of resource allocation and revenue generation and the impact they have on responsibility formation. Needless to say, this is deeply political territory and one that we take care in walking through. That said, we believe it is necessary to walk this path as it highlights the need to consider digital responsibility formation as a collaborative and consensual process that involves realising, establishing and actioning responsibility. It is this broader framework that better explains digital responsibilities and assists policy makers involved in digital policy implementation to better understand the complex contours of digital and physical environments, including the actors that govern those spaces and reside in them. Let's start first with governmental resource allocation.

Digital Migration is the clearest example of the impact of limited resource allocation across the three case studies. Even though the importance of digital support for refugees is clearly realised at the supra-jurisdictional level, it remained to be established and actioned through the state at national and local

Figure 6.5: Resources and business models

levels. Formalised resource allocation strategies were lacking and were exacerbated further by the COVID-19 pandemic. The lockdowns strained every facet of UK society, particularly the most vulnerable, who were suddenly required to negotiate complex bureaucracies through purely online services. Much like Digital Census, the responsibility for providing online access and the skills necessary to complete online forms were absorbed by on-the-ground civil society organisations. Resource stretched charities were essentially forced to further take on the practical role of the 'surrogate state' due to the lack of actioning by local authorities and the lack of resource allocation by central government.

Digital Census does not describe the same degree of resource abandonment. There is no doubt that the inclusion of extended language possibilities in the online census was a positive active of resource allocation. It clearly generated excitement among the Kurdish community about the possibilities of being recognised as a part of UK society. We pointed out the limits of educational support which were willingly absorbed by community groups. The limits of resource allocation, in this sense, are more contested especially in the context of the Digital Migration case study. Base resources were allocated, unlike in Digital Migration, and it was the willing ground-up community response that provided the impetus for additional educational services.

Nevertheless, both case studies show the clear relationship between governmental resource allocation and responsibility realisation, establishment and actions. Even if a responsibility is realised and established it does not guarantee that sufficient resources will be allocated for responsibility actions. Going back to our framework, we can say that the discharge of baseline responsibilities through resource allocation required other parties to absorb responsibilities to provide more effective educational and support resources.

As we have noted elsewhere in the book, there is a strong connection between the implementation of digital technology with its distance from physical space and the need for physical, human connection to take responsibility for its use within that space. We do not see these absorption actions as the outcome of responsibilisation strategies, especially in relation to the Digital Census study. Rather, they are response-able outcomes that are guided by a deep understanding of the physical and social environments in which the technology is used, and indeed, from the deep sense of an individual's ability to positively respond to a given situation. Again, we think this re-emphasises the need to better identify and understand lacunas because they are environments in which positive responsibility acts can be realised and actioned. Lacunas may then point to places of positive and beneficial resource allocation for all parties, including government.

Similar considerations appear to arise in the context of revenue generation by private sector actors. Our book has significantly covered the distributed nature of digital responsibility, not least through governance structures involving public and private sector actors. The clearest case study example is, of course, the online safety debates. The fractious nature of the debates can be read in several ways, most notably as the online service provider response to core business model construction and the revenue threats that it could impose.

Chapter 3 highlighted the responsibilisation issues that arose with the attempts by online service providers to make users more responsible for actions related to content moderation. Content moderation thus became a debate about a potential source of consumer harm pitted against the design, management and implementation of digitally safe spaces. The development of the latter, as Chapter 3 noted, would have a direct impact on the root cause of harms engendered as a core part of business models based on supposed free-of-charge services that enable on target advertising related to finely monitored user behaviour. It is at this point that online service provider attempts to avoid responsibility and re-allocate content moderation actions to users become more visible. Key is online service provider attempts to shift the realising of responsibility to discussions about content moderation as a user generated harm rather than a profit motive, business model consideration. It is this attempt to re-shape the pathway of law reform establishment that starts in earnest with the attempted responsibilisation of users as the appropriate point of content moderation. In doing so, the debate started to shift away from the broader structural implication of what online safety reforms were trying to achieve.

Our framework then allows a better understanding of the role of resource allocation and revenue generation in relation to responsibility formation. It is unsurprising that traditional frameworks for understanding legal responsibility, and to a lesser extent, even contemporary frameworks, largely fail to connect resource allocation with responsibility formation. The reason for this, which we note elsewhere in the book, is that ascribed responsibility through law is seen as a closed and unitary process. It is hopefully apparent by now that the interdisciplinary nature of our framework offers a unique perspective to digital responsibility that can consider the role of law in a broader setting than previously envisaged.

The same, we think, can be said for understanding the relationship between revenue generation by private sector parties and responsibility. The case studies show that marketisation of public services and obligations do not entail the eradication or reduction of responsibilities on policy makers or private sector service deliverers. Lacunas cannot simply be avoided by attempting to make users responsible for digital policy outcomes. Avoiding or refusing responsibility actions does not make responsibilities go away. Instead, it shifts them to other parties that may or may not be better placed or resourced to absorb or reallocate responsibilities. These lacunas will keep appearing as they are an unavoidable consequence of the pluralised nature of digital policy implementation. As such, we need a framework that allows conversation to openly develop, including the surfacing of profit motive discussions which are often tacitly baked into business model construction.

Our focus on sites and realms of responsibility realisation and establishment are important to understanding the formation of digital responsibilities. These are the spaces, whether formed or in lacuna state, in which negotiations take place. Realms determine the active stakeholders involved in consensus building and sites surface the many interests and values foregrounded by parties. Our key focus on expanding responsibility analysis to this breadth is to highlight the possibility of negotiated consensus. Non-resolution loops – for example, the situation where a lacuna is not resolved and thus responsibility actions remain unallocated – are expensive for all parties. Understanding responsibility in a broader sense could lead to the reduction of non-resolution loops and provide better implementation strategies for all parties by having clearer and more targeted discussions about realising, establishing and actioning responsibilities. Doing so reduces the need for technical, and indeed, legal, forcing functions as a means of ending non-resolution loops which become harder to impose on users as time moves on.

Conclusion

Chapter 6 outlines the lessons we think can be learned when our digital responsibility framework is considered against the book's case studies. The framework is by necessity broad and we hope this analysis helps to explain why. It provides a necessarily encompassing picture of how responsibilities are realised, established and actioned that better explains the broader implications of digital policy implementation. Other responsibility frameworks tend to focus on actions alone, whereas we believe actions must be understood as attempts to realise responsibility and how those realisations are established. Our different responsibility processes also highlight the distributed nature of responsibility formation across technical, legal and social domains. Lacunas are an important way to understand responsibility distributions because they highlight points of absence in collaboration and consensus. These points of absence are often considered as gaps that need to be filled by forcing functions technical, legal or otherwise. We show that need not be the case.

All these considerations highlight the intrinsic link between resource allocation, revenue generation and responsibility formation, which again is central to understanding the breadth of our framework. Having outlined the lessons learned, we now conclude the book with five understandings to take away.