Resolving stakeholder tussles in healthcare systems: ethical challenges to data protection

Brian Pickering (✉)[0000-0002-6815-2938]1, Giuliana Faiella[0000-0002-1782-030X]2 and Fabrizio Clemente[2,3]

[1] University of Southampton, Southampton, SO16 7NS, UK
[2] Fondazione Santobono Pausilipon Onlus, Naples, Italy
[3] Institute of Cristallography CNR, Roma, Italy
j.b.pickering@soton.ac.uk, guiliana.faiella@gmail.com, fabrizio.clemente@ic.cnr.it

Abstract. For cross-border collaborative healthcare delivery, data protection legislation seems to be increasingly obstructive. In extreme cases, this may compromise the quality of care a patient receives and at the same time prevent clinicians practicing and developing their medical skills to their full potential. A dilemma develops whereby the fundamental rights of patient and clinician are constrained by the very legal instruments designed to make delivery of healthcare easier. The contention between patient and clinician expectations, or *tussles*, may pose a threat to future healthcare delivery. Compromising healthcare delivery in this way has wider complications for community trust. The concept of tussles in technology infrastructures suggests an actor-network approach involving the patient and clinician relationship within the context of community response to their interactions to offer an innovative perspective on the problem of tussles in healthcare. In this paper, we develop such an approach and discuss an initial validation based on cross-border healthcare scenarios illustrating the contention between fundamental ethical rights and actor-network compliance.

Keywords: Ethics, Privacy, Regulation, Trust, Proportionality, Healthcare, Actor Networks.

1 Introduction

To discipline the digital economy and facilitate the easy movement of people between member states, the European Commission introduced the General Data Protection Regulation [1]. Harmonizing the treatment of personal data across states, it was hoped, would benefit private citizens not only commercially but also for their care. A tourist could therefore expect appropriate treatment regardless of host country, with clinicians able to access their health records wherever needed. But in complex networks, like the infrastructures required for the secure transfer of personal and special category data between member states [2], the needs and expectations of different stakeholders may well conflict [3]. This is particularly important within healthcare since failure to gain access to health data could put the data subject (the patient) at risk. Innovative health

services tend to focus on privacy and security. In consequence, they often introduce many additional challenges regarding legal and ethical concerns that need to be addressed to provide healthcare professionals and developers with regulations and guidance [4,5]. What is more, unless the patient is unconscious and unable to give explicit consent where vital interests might be used as a lawful basis for processing, the clinician may be prevented from accessing the information they need to treat the patient effectively and in accordance with the ethical principles of their profession. In this paper, we explore the ethical and legal tussles which different stakeholders face who depend on healthcare socio-technical systems. With the GDPR in place, it is assumed that all technology developers need to do is handle data such as health records securely, including appropriate access control. But earlier work by [6] provides a multi-disciplinary perspective of how the information society affects individuals as well as society as a whole, concluding that human choice is paramount. Yet the drive for digitalization, not least of patient health records, is increasingly difficult to resist [7]. Li [8], by contrast, and the failure of the ICT-enabled healthcare system described by Dyb and Halford [9] illustrate a complicated interaction between human choice, policy and the socio-technical context where technology is deployed. It is hardly surprising, therefore, that the adoption of ICT into healthcare environments is known to depend on multiple factors beyond the technical functionality of the technology itself [10,11]. There is clearly a need to revisit factors beyond regulation and consider 'human choice' as it relates to different agents within a complex network. Based on work by Liyanage, Faiella and their colleagues [12-14], we present an ethical framework designed to identify potential tussles within cross-border, coordinated healthcare. Extending the initial attempt to balance societal and individual interests in making health data available [13] to explore contention between the rights and concerns of multiple stakeholders, the framework presents ways in which the ethical and regulatory tussles of those stakeholders around the network may be evaluated.

1.1 Tussles

The concept of tussles for cyber-physical networks was originally coined in regard to resource contention [3]. For example, net neutrality dictates that all information is treated equally when transmitted across the network. We think that fair. Yet in emergencies, priority should be given to the most significant information packets, such as from emergency services. Contention arises between treating everyone with equanimity and contextual demands. Further, unless the emergency services use specific routing, all packets must be inspected compromising privacy to identify which are a priority. But even here the monetization of personal data suggests multiple standards [15]. So, tussles represent conflicts between stakeholder interests. Therefore, this paper explores the contention between the ethical expectations of actors within a healthcare actor network and professional or regulatory requirements for operational security.

1.2 Tussles in Healthcare

Consent is a common lawful basis whereby the data subject agrees their data may be collected and used for specific purposes such as healthcare (Art. 6 & Art. 9) [1]. Consent must be explicit (it must be auditable) and informed (the data subject must understand why and how their data are to be used). Other legal bases are possible, though may conflict with a data subject's expectation of privacy.

Taking cross-border travel to illustrate the problem, consider several different scenarios as listed in **Table 1**. Each brings to light different potential contention.

Table 1. Sample scenarios to validate the proposed approach

Scenario	Description
1	A businessman travelling abroad who has a known medical condition travels for work to another EU country. Because of the pre-existing condition he has provided *explicit and informed consent* for access to his medical records as it relates to this specific problem. While away, he feels unwell and is taken to a local hospital for treatment.
2	An Italian lawyer has gone to Brussels to attend a workshop on e-Privacy. She has no known medical condition. She is taken ill at the workshop and has to be taken to hospital urgently.
3	While on vacation from home in Hamburg to Spain, a mother and son are involved in a serious accident. They are rushed to a hospital emergency department unconscious.
4	A young student is on an exchange study tour. He is a member of a religious community which is subject to violent opposition. During clashes in the street, he is injured and needs hospital treatment.

In the first scenario, since the patient (the data subject) has provided explicit consent for a specific condition, the clinician in the host country may access the personal / special category data. However, there may be contention if the current episode is not directly or solely related to the pre-existing condition. If the patient has been specific and explicit about the data which can be shared, then there may be other factors which the host clinician is not allowed to see. This may include religious belief (see below) or a relevant comorbid condition. The clinician may not therefore be able to treat the patient appropriately: they cannot necessarily avoid harm or exercise their own professional autonomy.

Provided the lawyer in the second scenario is conscious, local clinicians can attempt a diagnosis by discussing symptoms with her. The problem might arise if they feel they need additional information which she is unable or refuses to provide. As above, the clinician is prevented treating her to the best of their ability. But for the data subject (the patient) herself, she may have legitimate reason not to want to disclose certain information: she is legally not medically trained and may not, therefore, be competent to make a fully informed decision. As with the previous example, it may not be possible to request only relevant data to be transferred.

In the third example, vital interests may be used if both mother and child are unconscious. Even if conscious, the child cannot give consent in most member states. Further, if the father is present or easily contactable, he can provide consent for the child. But only *in extremis* can he do the same for his partner. The clinician may be delayed in accessing relevant data which may compromise appropriate treatment. This could also undermine the patients' chances of complete recovery depending on their condition.

In the final scenario, the patient needs to give consent, of course, but may be reluctant to disclose their religious beliefs for fear of discrimination. In so doing, however, they may be treated using medication or some other procedure which is against their religious conviction. The clinician may therefore inadvertently contradict the wishes of their patient; they will do emotional if not physical harm.

All four scenarios present issues not only for the clinician being able to practice to their best ability and satisfaction, but also for the patient in that they may not receive the most appropriate treatment and may be obliged to disclose more than they would like. Trying to resolve contention between patient and client might, for instance, use a different lawful basis for processing. But if the home medical institution uses consent, it is unclear how a different lawful basis might override the original basis. There is clearly a need to think of healthcare from a different perspective.

1.3 The Socio-technical Context of Healthcare

Healthcare is not only about the treatment of patients. Sitting & Singh [16] describe a complex layered socio-technical system, including the clinical context as well as operational workflows. For our purposes, this may be simplified to a broader socio-technical dimension: patients are treated by clinicians within a community. The agents form a simple actor network [17,18], with the community bystanders who alternately benefit from the successful treatment of patients through increased medical knowledge and expertise (clinicians *inform*), but also monitor the overall acceptability of what is being done in terms of patient care and medical research (the community sees what happens and so patient and community *protect* one another). A schematic is shown in **Fig. 1**.

The actors rely on a socio-technical system with multiple technology and infrastructure components as Sitting & Singh describe [16] but also broadcast and social media supporting information exchange and community building [19,20]. So, *community* are not directly involved in the treatment of patients as previously explained and yet play an important moderating role in the actor network. The most significant feature of the network though is the focus on activity – interaction between patient and clinician, and observation by the community – as well as structure. Contention between the rights both of patient and of clinician would have a directly negative effect for the community in reducing trust, but also perhaps indirectly in constraining the medical experience and information which might add to and improve future knowledge. The clinicians may find themselves criticized for being unwilling to take the risk to try and access the information they require. Over time, trust in the operation of the network would decline.

1.4 Ethical and regulatory context for health data

With that in mind, we next consider actor behavior and how it relates to structure. De Lusignan, Liyange and their colleagues undertook a systematic literature review on the use of healthcare data [12]. This led to the identification of fourteen ethical principles and the same number of privacy principles [12]. They extended the approach to identify a further set of seven ethical and eight privacy guidelines [13]. The principles and guidelines were then validated in a 3-round Delphi study by a cohort of healthcare and informatics professionals, finding unambiguous agreement on nine each of the ethical and privacy principles, three ethical guidelines, and all nine privacy guidelines. Notwithstanding reported difficulties in interpretation of the principles, interestingly they found no agreement on the ethical principles that clinical judgement should be respected, whether the lawfulness bases might be ignored, and on the privacy principles that data subject (patient) consent should be respected and the purpose of processing limited [13]. Important for establishing agreement on a set of principles, perhaps, are failures to reach consensus. Although their aim was to look at the use of healthcare data in research, the results might inform perceptions of ethical treatment around health data for actual patient engagement.

Based on De Lusignan et al.'s work [12], Faiella et al. [14] sought to use the ethical and privacy principles in order to identify a set of design principles for developing technology to support the secure curation of healthcare data in real life healthcare contexts. They identified six basic principles: trust, privacy & security, related alternately to consent and data subject rights on the one hand and to data management methods; ownership & control; equity; and dignity. Extending this provides the starting point for the present study. We suggest a modified approach as their original, technology-focused framework is extended to the socio-technical, actor network.

2 Approach

In each of the four scenarios described above, ethical principles such as autonomy and the expectation to be able to give and receive effective treatment conflict with legal considerations around data protection. In this section, we develop an approach to validate fundamental ethical principles in the context of trust and proportionality to handle tussles in healthcare.

2.1 Ethical principles

Lacking consensus from domain experts [13], our initial approach is based on one regulatory principle and three fundamental ethical values. One difference between the GDPR (2016) and the previous Directive [31] was the more formal definition of data subject rights. This gives the onus back to the data subject, to some degree, even though they may be unsure of how to exploit or the consequences of asserting those rights [32].

As a high priority item [12,14] and as part of the concept of data ownership and control [14], we will consider *autonomy* as a fundamental right and therefore as an ethical consideration. Autonomy, in the sense of personal control over data, was part of the

motivation for the data subject rights encoded in the GDPR. Beyond that, the European Convention on Human Rights [30] includes articles on life itself (Article 2), privacy (Article 8), and to have individual beliefs respected (Article 9). These are summarized in **Table 2** along with an explanation of how they apply to patient and clinician.

Table 2. Basic ethical principles based on rights as they relate to patients and clinicians in the network

Ethical Principle	**Actor**	
	Patient	Clinician
Autonomy	The right to determine what should happen	The right to use their skills to the best of their ability
Privacy	The right for personal information not to be disclosed	The right to act as a professional rather than pursued as an individual
Beliefs / Values	The right to have convictions respected	The right to follow their own beliefs and convictions in doing their job
Life / Benefit	The right to be given whatever treatment is necessary to preserve life	The right to provide treatment to their patients to preserve lives

2.2 Trust and Proportionality

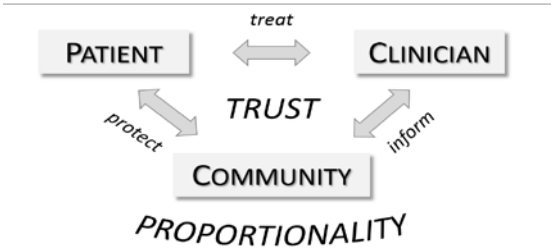

Fig. 1. Schematic view of a healthcare actor network

Trust in a socio-psychological sense is the willingness to expose oneself to vulnerability [21-23]. In an actor network therefore, trust is less about reliance on regulatory control but rather on how the trustor interacts with the trustee. Where technology is involved, trust may be mediated by self-efficacy and agency [24-26]. Trust becomes an "organizing principle" [27] which underlies both the activity across a socio-technical network (between patient and clinician) as well as how it is perceived (by the community) [28-29]. So in the present discussion, we extend our concept of trust from what Faiella and her colleagues mean [14] to the socio-psychological construct based on these trustworthiness indicators [21]: *Benevolence* or the belief that the trustee (the clinician) is motivated to do the best they can for the trustor (the patient); *Competence* or the belief that

the clinician has the necessary skill to treat the patient; and *Integrity* or the belief that the clinician will use their skill appropriately.

Faiella et al [14] also introduced the concept of proportionality. As they define it, this refers to the balance between excessive security and pragmatic data governance. Since this is a socio-technical system, we take proportionality to refer to the actions of the clinicians as well as structural elements in delivering treatment as part of the network. So here, we take proportionality for our healthcare actor network to refer both to physical measures (*security* and reduction of inadvertent *disclosure risk*) and behaviors (the clinician operates to the best of their ability to *avoid harm*).*Proportionality* in this sense refers to the physical infrastructure *and* the measures taken to maintain its security whilst the clinician attempts to execute their duties to ensure the best possible outcome for the patient.

As shown in **Fig. 1**. *trust* facilitates the mutually beneficial operation of the network: the willingness of the patient to expose themselves to vulnerability as the original definition suggests [21-23] provides some leeway for the clinician to achieve their aims. In so doing, the community at large appreciates (and thereby trusts) that the network functions well. The appropriate balance of skill, human activity and physical security measures – *proportionality* – allows this trusting stance to develop and be maintained.

3 Validation

The ethical principles selected (see Section 2.1) may now be used to gauge the effectiveness of the healthcare actor network. The assumed benefit of respecting ethical principles can be used as an indication of how this contributes to *trust* while respecting the challenges associated with *proportionality*.

Table 3. Ethical principles versus *Trust* and *Proportionality* from the Patient's perspective

Ethical Principle	**Trust**			**Proportionality**		
	Benevolence	Competence	Integrity	Security	Risk Reduction	Avoid Harm
Autonomy	+			+	+	
Privacy	+		+	+	+	
Beliefs / Values	+			+		+
Life / Benefit	+	+	+			+

Table 3 shows an example from the perspective of a patient. Each plus sign (+) indicates a positive contribution to trust or to maintaining appropriate balance in the system. For example, respecting the patient's *autonomy* – their ability to decide for themselves what information is and is not disclosed (see Scenario 1 above, for instance) – may lead to the patient's perception of benevolence but nothing else. If the clinician fails to treat them appropriately, they will not recover satisfactorily and therefore competence and integrity would be undermined.

Similarly, when their privacy is respected, the patient will assume clinician benevolence and integrity, as well as a secure network and reduced risk of disclosure. If the clinician is unable to access a complete medical record, then this may compromise their ability to carry out their professional duties (their *competence*) and to avoid harm. Respecting beliefs would again lead to a perception of benevolence, in not using treatment which might contravene those beliefs this would allow the clinician to avoid emotional harm (though not necessarily physical harm). This may also lead to perceptions that network security is good. Finally, focusing only on a patient's right to life (getting the best possible treatment) would optimize trust across the clinician's benevolence, competence and integrity, as well as allow the clinician to avoid harm. However, there may be concerns about security and the avoidance of risk of data disclosure.

Table 4. Ethical principles versus *Trust* and *Proportionality* from the Clinician's perspective

Ethical Principle	**Trust**			**Proportionality**		
	Benevo-lence	Compe-tence	Integrity	Security	Risk Reduction	Avoid Harm
Autonomy	+	+	+			+
Privacy			+	+	+	
Beliefs / Values			+	+		+
Life / Benefit	+	+	+			+

Following similar reasoning for the clinician would lead to a different perspective on trust and proportionality in **Table 4**. To encourage trustworthiness in their skill and experience, clinicians want to project *benevolence* (they have the patient's best interests at heart), their *competence* (they have the ability to treat correctly) and their *integrity* (they act appropriately). They are less interested in operational issues such as infrastructure security and possible data breaches, but they do want to avoid harm with their treatment. All these indicators relate to their autonomy – their right to determine how they treat their patients. Remembering that the rights in the far-left column (*privacy, beliefs/values* and *benefit*) are from the clinician's perspective allows the table to be completed. For instance, the beliefs/values right for the clinician may refer to their religious or philosophical beliefs but equally to their professionalism.

Comparing patient and clinician matrices of rights related to trust and proportionality in the actor network results in the summary shown in **Table 5**. Here, a plus sign (+) shows where there is agreement between the two actors (each from their own perspective), a minus sign (-) indicates a disagreement (one but not both of the actors), and a blank that neither agrees nor disagrees.

Of the twenty-four cells in the table, where individual rights can be supported by the construct of trust and the operational characteristics of the network, there are ten cases of agreement (+) and eight cases of disagreement (-); and six cases (blank) where neither shows a possible relationship between their rights and trust or proportionality. Across all possible relationships in the network, therefore, there are 8/24 (a third of cases) where the perspective of patient and the clinician treating them are at odds.

Excluding the 6 cases where neither is affected, the level of contention increases to 8/18 discrepancies. Tussles between patient and clinician perspectives occur for almost half of the cases, therefore.

Table 5. Differences between expectations of Patients and Clinicians

Ethical Principle	**Trust**			**Proportionality**		
	Benevo-lence	Compe-tence	Integrity	Security	Risk Reduction	Avoid Harm
Autonomy	+	-	-	-	-	-
Privacy	-		+	+	+	
Beliefs / Values	-		-	+		+
Life / Benefit	+	+	+			+

Since little consensus on respect for clinical judgement, consent, legal compliance and the use of personal data [13] found, **Table 6** attempts to summarize a community perspective of the effectiveness of the healthcare actor network. For example, *autonomy* applied both to patient and clinician assumes that treatment would be effective (avoiding harm) and therefore trust would be maintained (i.e., the perception of benevolence, competence and integrity); privacy, by contrast, relates only to physical security and awareness of it ("integrity"). To respect beliefs and values, and preserving life and maximizing benefit, would reflect a perfectly operational actor network in which trust is developed and continued. Interestingly, the privacy line seems to reflect only the robustness of the infrastructure and its perceived security that are appreciated. Trust is only developed in conjunction with treatment outcomes (avoiding harm).

Table 6. Ethical principles versus *Trust* and *Proportionality* from a Community perspective

Ethical Principle	**Trust**			**Proportionality**		
	Benevo-lence	Compe-tence	Integrity	Security	Risk Reduction	Avoid Harm
Autonomy	+	+	+			+
Privacy			+	+	+	
Beliefs / Values	+	+	+	+	+	+
Life / Benefit	+	+	+	+	+	+

4 Discussion

In seeing the healthcare delivery socio-technical system in terms of an actor network introduces the perspective of interactional relationships. Deadlock around the

contention between patient and clinician is not so much a reflection of inconsistencies between data protection legislation and the ethical rights and expectations of the data subject, but rather what the community at large regards as best for the whole community. The ethical design principles which apply to the technology elements [14] of an actor network are relevant for individual actors to perceive the effective delivery of care. However, human-to-human interactions also rely on interpersonal and organizational trust [21,22,27]. Developing and maintaining trust is a continual negotiation [28] which may be hampered by expectations around privacy and technical security. Whilst patient and clinician develop this trust, it may well be that independent bystander perceptions from the broader community need to shape the implementation of privacy.

If this community perspective could be separately validated, then this would offer a solution to the contention between patient and clinician expectations. In a healthcare actor network, the expectations of the generic community of bystanders in the network may override those of individual actors. Trust as an "organizing principle" [27] develops and is maintained only when compromise occurs: data subject consent, as evidenced by Liyanage et al [13], is not the final arbiter. For healthcare delivery to be seen to be effective and thereby trusted, there must be cooperation between patient and clinician. The former must be prepared to accept vulnerability [21,23], whilst the latter should perhaps be guided by other factors such as data subject beliefs and convictions. The clinician's judgement may not unequivocally determine the course of action [13] but be subject to community scrutiny. This in turn would allow for culturally divergent perspectives [33].

This exploratory study focuses on healthcare as a socio-technical actor network. Specifically, we have considered not only the physical security of the infrastructure, but also its trustworthy operation. We have looked from the different actors' perspectives to identify the possible source of contention between the expectations of those actors (i.e., stakeholder tussles). This contention is exacerbated in cross-broader collaborative healthcare where different legal bases at different cross-border locations may be incompatible. To resolve these tussles, looking at the effectiveness of the healthcare actor network in terms of the relationship between ethical principles and the maintenance of trust and proportionality, introduces a third actor: the community at large.

5 Future research

The panel of experts in the Liyanage et al [13] studies failed to reach consensus on all the ethical and privacy principles or guidelines they identified from their original systematic literature review. Our proposed re-examination of healthcare socio-technical systems suggests that the community at large – those who benefit from advances in healthcare as well as monitor how it is delivered – may be able to resolve the patient-clinician tussle. Using the design principles which Faiella et al [14] propose we have attempted to review the different actor perspectives within the context of features of patient-clinician interactions (trust) and of the operation of the socio-technical healthcare delivery system (proportionality). To validate this, we now intend to develop

quantitative instruments to investigate the attitudes of private citizens to the resolution of tussles that the analytical tables above suggest.

Acknowledgements. The research reported in this paper was supported with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement 727528 (the KONFIDO project) and 727301 (the SHiELD project).

References

1. European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016," 2016.
2. M. Nalin, et al., "The European cross-border health data exchange roadmap: Case study in the Italian setting," *Journal of biomedical informatics*, vol. 94, 2019, pp. 103183; doi 10.1016/j.jbi.2019.103183.
3. D.D. Clark, et al., "Tussle in cyberspace: defining tomorrow's internet," *IEEE/ACM Transactions on Networking (ToN)*, vol. 13, no. 3, 2005, pp. 462-475; doi 10.1109/TNET.2005.850224.
4. P. Natsiavas, et al., "Comprehensive user requirements engineering methodology for secure and interoperable health data exchange," *BMC medical informatics and decision making*, vol. 18, no. 1, 2018, pp. 85; doi 10.1186/s12911-018-0664-0.
5. X. Larrucea, et al., "Assessing source code vulnerabilities in a cloud-based system for health systems: OpenNCP," *IET Software*, vol. 13, no. 3, 2019, pp. 195-202; doi 10.1049/iet-sen.2018.5294
6. G. Collste, et al., "ICT in Medicine and Health Care: Assessing Social, Ethical and Legal Issues," Springer US, 2006, pp. 297-308.
7. S. Halford, et al., "Beyond implementation and resistance: how the delivery of ICT policy is reshaping healthcare," *Policy & Politics*, vol. 37, no. 1, 2009, pp. 113-128.
8. J. Li, "A Sociotechnical Approach to Evaluating the Impact of ICT on Clinical Care Environments," *Open Med Inform J*, vol. 4, 2010, pp. 202-205; doi 10.2174/1874431101004010202.
9. K. Dyb and S. Halford, "Placing Globalizing Technologies: Telemedicine and the Making of Difference," *Sociology*, vol. 43, no. 2, 2009, pp. 232-249; doi 10.1177/0038038508101163.
10. R.W. Sanson-Fisher, "Diffusion of innovation theory for clinical change," *Medical journal of Australia*, vol. 180, 2004, pp. S55-S56.
11. A.K. Yarbrough and T.B. Smith, "Technology acceptance among physicians: a new take on TAM," *Medical Care Research and Review*, vol. 64, no. 6, 2007, pp. 650-672; doi 10.1177/1077558707305942.
12. S. De Lusignan, et al., "Using routinely collected health data for surveillance, quality improvement and research: Framework and key questions to assess ethics, privacy and data access," *Journal of Innovation in Health Informatics*, vol. 22, no. 4, 2016, pp. 426-432; doi 10.14236/jhi.v22i4.845.
13. H. Liyanage, et al., "Building a Privacy, Ethics, and Data Access Framework for Real World Computerised Medical Record System Data: A Delphi Study," *Yearbook of medical informatics*, vol. 25, no. 01, 2016, pp. 138-145; doi 10.15265/IY-2016-035.
14. G. Faiella, et al., "Building an Ethical Framework for Cross-border applications: the KONFIDO project," *Proc. International ISCIS Security Workshop*, Springer, 2018, pp. 38-45.

15. V. Erramilli, “The tussle around online privacy,” *IEEE internet computing*, vol. 16, no. 4, 2012, pp. 69-71; doi 10.1109/MIC.2012.92
16. D.F. Sittig and H. Singh, “A new socio-technical model for studying health information technology in complex adaptive healthcare systems,” *Cognitive Informatics for Biomedicine: Human Computer Interaction in Healthcare*, V. L. Patel, et al., eds., Springer, 2015, pp. 59-80
17. W.N. Kaghan and G.C. Bowker, “Out of machine age?: complexity, sociotechnical systems and actor network theory,” *Journal of Engineering and Technology Management*, vol. 18, 2001, pp. 253-269; doi 0.1016/S0923-4748(01)00037-6.
18. J. Law, “Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity,” *Systems practice*, vol. 5, no. 4, 1992, pp. 379-393; doi 10.1007/BF01059830.
19. N. Newman, “The rise of social media and its impact on mainstream journalism,” 2009.
20. L. Gunton and K. Davis, “Beyond broadcasting: Customer service, community and information experience in the Twittersphere,” *Reference Services Review*, vol. 40, no. 2, 2012, pp. 224-227; doi 10.1108/00907321211228282.
21. R.C. Mayer, et al., “An Integrative Model of Organizational Trust,” *The Academy of Management Review*, vol. 20, no. 3, 1995, pp. 709-734; doi 10.5465/AMR.1995.9508080335.
22. F.D. Schoorman, et al., “An integrative model of organizational trust: Past, present, and future,” *Academy of Management review*, vol. 32, no. 2, 2007, pp. 344-354; doi 10.5465/AMR.2007.24348410.
23. D.M. Rousseau, et al., “Not so different after all: A cross-discipline view of trust,” *Academy of management review*, vol. 23, no. 3, 1998, pp. 393-404; doi 10.5465/AMR.1998.926617.
24. J.B. Thatcher, et al., “The role of trust in postadoption IT exploration: An empirical examination of knowledge management systems,” *Engineering Management, IEEE Transactions on*, vol. 58, no. 1, 2011, pp. 56-70; doi 10.1109/TEM.2009.2028320.
25. D.H. McKnight, et al., “Trust in a specific technology: An investigation of its components and measures,” *ACM Transactions on Management Information Systems (TMIS)*, vol. 2, no. 2, 2011, pp. 12; doi 10.1145/1985347.1985353.
26. B. Pickering, et al., “The Interplay between Human and Machine Agency,” *HCII 2017*, Toronto, Canada.
27. B. McEvily, et al., “Trust as an Organizing Principle,” *Organization Science*, vol. 14, no. 1, 2003, pp. 91-103.
28. R.J. Lewicki and C. Wiethoff, “Trust, trust development, and trust repair,” *The handbook of conflict resolution: Theory and practice*, vol. 1, no. 1, 2000, pp. 86-107.
29. B.A. Sparks and V. Browning, “The impact of online reviews on hotel booking intentions and perception of trust,” *Tourism management*, vol. 32, no. 6, 2011, pp. 1310-1323.
30. Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, *E. C. o. H. Rights*.
31. European Commission, “DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,” 1995.
32. A. Acquisti, et al., “Privacy and human behavior in the age of information,” *Science*, vol. 347, no. 6221, 2015, pp. 509-514; doi 10.1126/science.aaa1465.
33. G. Hofstede, et al., *Cultures and Organizations: Software of the Mind*, McGraw-Hill, 2010