Vision: Enabling secure collaboration is the overarching theme of my research. I understand *privacy* and *security* as ethical values, and I envision ethics-aware social computing techniques and infrastructure that facilitate natural interactions among autonomous social entities (people and organizations). To develop foundations for such social computing techniques, I adopt a sociotechnical stance in which agents (as technical entities) help autonomous social entities or principals (people and organizations). This multiagent conception of a sociotechnical system (STS) captures how cybersecurity and privacy concerns arise in the mutual interactions of multiple stakeholders. In pursuit of developing the foundations which would enable us to realize secure STSs, I intend to make fundamental contributions in cybersecurity and social computing.

Objective: The challenge in realizing a secure STS is — how to understand social reality, i.e., understanding social norms and regulations, social context, and values including security and privacy. To address this challenge, I have been developing computing techniques and infrastructure to (1) support humans in secure decision-making, (2) ensure prosocial outcomes, and (3) yield robust and resilient systems. I emphasize empirical evaluation of research contributions. I have conducted a variety of empirical studies including developer, end-user, and simulation studies to evaluate my contributions.

Social Intelligence and Secure Decision-Making

Our actions and interactions in a society are not driven solely by individual needs. Instead, we adapt our behavior considering the needs of others, e.g., by being courteous and lending a helping hand. Such acts, even if inconvenient at times, deliver a privacy-respecting experience. In a society where an agent acts and interacts on behalf of a stakeholder (a human user), it is important that the agent understands these nuances in social interactions.

To address the challenge of modeling social intelligence, I develop Arnor [5], a method which facilitates modeling stakeholders' actions and expectations, and how these influence each other. Arnor employs Singh's [9] conception of social norms to capture social expectations, and incorporates argumentation constructs for sharing decision rationale. Social norms in Arnor enables capturing *accountability* in decision-making.

I am also interested in developing formal approaches to capture decision-rationale and verifying and reasoning about that. I develop Aragorn [3], a general purpose argumentation-based method to capture decision-rationale for firewall policies. Revani [6] and Coco [4] address secure decision-making formally in healthcare domain.

Understanding Social Context for Privacy-Respecting Outcomes

Norms describe the social architecture of a society and govern the interactions of its member agents. It may be appropriate for an agent to deviate from a norm; the deviation being indicative of a specialized norm applying under a specific context. To address the challenge of understanding social context, I develop Poros [1], an approach for building intelligent agents that carry out enriched interactions where deviating agents share selected elements of their context as explanations, and other agents respond appropriately to the deviations in light of the received information. Revealing and reasoning about social contexts to infer contextually relevant norms yields both *transparency* and *accountability*, but at the cost of *privacy*.

I am interested in understanding the abstractions of shared context. When agents share context, it is important for them to know *what to share* and *what not to share*. If agents can understand abstractions of the context being shared, they can better ensure *privacy* of their users while maintaining transparency. I also have interest in incorporating natural language techniques to understand context. In an ongoing effort (work not published), we are analyzing app reviews to identify and flag mobile apps that promote intimate partner surveillance.

Robust and Resilient Systems

Privacy, values, and ethics are closely intertwined. Preserving privacy presumes understanding of human values and acting ethically. If norms require agents to perform or not perform certain actions, values provide a reason to or not to pursue those actions. Each action a Poros agent executes potentially promotes or demotes one or more values such as privacy and security. Being aware of the trade-offs in these values helps developing robust and resilient systems. To address the challenge of reasoning about values, I develop Elessar [2], a framework to design ethical and secure STSs. Elessar incorporates a multicriteria decision-making method to aggregate value preferences of stakeholders and select robust actions.

I also have an interest in formal verification and reasoning of policies. Future directions in verification and reasoning are two-fold. First direction is adopting argumentation to model and to infer preferences among values [3]. Second direction is to generate optimal normative specification trading-off security and liveness of systems. Whereas Poros and Elessar yield privacy-respecting experience, these approaches do not formally verify if the systems are robust and resilient. I intend to develop formal approaches on lines of my other recent works [7, 8] to compare normative specifications that emerge by computing tradeoffs and generating optimal normative specification for STSs.

Collaborations

As part of the Cybersecurity hub, I will contribute toward developing new social computing technologies and infrastructure that will enable realizing secure STSs.

In the cybersecurity group at King's College, I will seek collaborations with (1) Dr. Jose Such on developing privacy-enhancing computing techniques, and conducting user studies to evaluate those, (2) Professors Luc Moreau and Luca Viganò on formal approaches for secure STSs, and (3) Professor Lorenzo Cavallaro on machine learning and vulnerability prediction in software applications, which follows my ongoing (unpublished) work on software security.

Internationally, I will continue to collaborate with (1) Professor Munindar Singh at NCSU on the broad theme on secure collaboration, (2) Professor Laurie Williams at NCSU on secure software engineering, (3) Dr. Özgür Kafalı at University of Kent on developing formal reasoning and verification, and (4) Dr. Pradeep Murukannaiah at Delft University of Technology on privacy. Outside of academia, I will seek industry collaborations with (1) Dr. Jessica Staddon at Google on cybersecurity, (2) Dr. Raghvendran Balu at HERE Technologies, Eindhoven on location privacy.

Expected Outcomes

Pertaining to interdisciplinary nature of my work, I expect to publish my research findings in prestigious journals and conferences in Security and Privacy (e.g., IEEE S&P, USENIX Security, CCS, SOUPS), Artificial Intelligence (e.g., JAIR, AIJ, JAAMAS, AAAI, IJCAI, AAMAS), and in Software Engineering (e.g., TSE, TOSEM, ICSE, FSE, RE). I will make the software I build and data I collect (modulo IRB and university restrictions) publicly available.

I will seek research funding from (1) EPSRC (New Investigator Award) and (2) UKRI Future Research Fellowship.

References

[1] Nirav Ajmeri, Hui Guo, Pradeep K. Murukannaiah, and Munindar P. Singh. Robust norm emergence by revealing and reasoning about context: Socially intelligent agents for enhancing privacy. In *Proceedings of the 27th International Joint Conference on Artificial Intelligence (IJCAI)*, pages 28–34, Stockholm, July 2018. IJCAI.

[2] Nirav Ajmeri, Hui Guo, Pradeep K. Murukannaiah, and Munindar P. Singh. Elessar: Ethics in norm-aware agents. In *Proceedings of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 1–9, Auckland, May 2020. IFAAMAS.

[3] Nirav Ajmeri, Chung-Wei Hang, Simon D. Parsons, and Munindar P. Singh. Aragorn: Eliciting and maintaining secure service policies. *IEEE Computer*, 50(12):50–58, December 2017.

[4] Nirav Ajmeri, Jiaming Jiang, Rada Chirkova, Jon Doyle, and Munindar P. Singh. Coco: Runtime reasoning about conflicting commitments. In *Proceedings of the 25th International Joint Conference on Artificial Intelligence (IJCAI)*, pages 17–23, New York, 2016. AAAI Press.

[5] Nirav Ajmeri, Pradeep K. Murukannaiah, Hui Guo, and Munindar P. Singh. Arnor: Modeling social intelligence via norms to engineer privacy-aware personal agents. In *Proceedings of the 16th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 230–238, São Paulo, May 2017. IFAAMAS.

[6] Özgür Kafalı, Nirav Ajmeri, and Munindar P. Singh. Revani: Revising and verifying normative specifications for privacy. *IEEE Intelligent Systems (IS)*, 31(5):8–15, September 2016.

[7] Özgür Kafalı, Nirav Ajmeri, and Munindar P. Singh. Kont: Computing tradeoffs in normative multiagent systems. In *Proceedings of the 31st Conference on Artificial Intelligence (AAAI)*, pages 3006–3012, San Francisco, February 2017. AAAI.

[8] Özgür Kafalı, Nirav Ajmeri, and Munindar P. Singh. Specification of sociotechnical systems via patterns of regulation and control. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 29(1):7:1–7:50, December 2019.

[9] Munindar P. Singh. Norms as a basis for governing sociotechnical systems. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 5(1):21:1–21:23, December 2013.