For this one-pager I've chosen two topics that both excite me and worry me. One*, migration of data and services to the cloud*, is well underway, and we can expect it to come to dominate the user experience over the next ten years; the second, *imposition of computer-mediated reality*, is in its early days, and the rate of adoption by 2025 is a little hard to predict. Inevitably it will become widespread, if only for certain applications. These trends raise alarms because of the new trust relationships into which they force the user to enter, but their architecture also can enable new assurance mechanisms if properly exploited for that purpose.

Migration of data and services to the cloud: The cloud offers users unprecedented *convenience*—data is accessible from anywhere, private stores do not need to be maintained, back-ups are seamless, and *functionality*—access to a dynamic and diverse set of applications, computational power beyond the reach of the user's choice of platform—but as implemented today, these benefits come at the cost of confidentiality and control. With so much data gathered in just a few places, users should have serious concerns both about how well cloud hosts can protect data from adversaries, and about the appropriateness of the uses to which data is put. It is not that hard, however, to envision a future where the cloud can give the user vastly better protection than he can manage on his own. A centrally-managed virtually-hosted infrastructure, given the right tools and methodologies, seems rife with opportunities for sensing, detecting anomalies, prophylactically refreshing, and possibly even fighting back. At the same time, further development of cryptographically-based techniques such as functional encryption and secure multi-party computation hold promise for handing back some control to the user, or at least requiring some sort of contract between data miner and data user. Stakeholders for these improvements run the gamut of commercial and critical infrastructure service providers and private through institutional users.

Imposition of computer-mediated reality: Wearable and embeddable appliances with the ability to sense, interpret, and perhaps distort reality literally require users to put their lives on the line. Motivators for this technology come from diverse perspectives: gaming, concierge services, health and fitness, and biomedical , just to name a few. It is not hard to imagine a future in which people come to depend upon these devices to guide them through everyday life, and in which the appliances, probably in conjunction with a network connection back to a knowledge base, provide actionable advice. In what is sure to be a real-time environment trust decisions will be instantaneous. There will be no time to decide whether to accept a certificate or not, so authentication had better be fail-proof. Identifying the user could become much easier than today with devices existing in such close proximity to or in symbiosis with the human body. Authenticating the entities with whom the user interacts does not necessarily get easier. With the stakes so high, new approaches are needed that greatly decrease the likelihood that the user will misplace his trust.