

Why Discrete Science?
Why the DHS Institute for Discrete Science (IDS)?
Why University-affiliated Centers (UACs) with the IDS?

- Why Discrete Science?
 - **We live in an information age and those who are best able to capture and utilize information are at a clear advantage.** To deny this basic premise could be self-defeating. IDS is dedicated to developing tools and techniques for representing, capturing and safeguarding information.
 - The intelligence community was roundly criticized in the wake of 9/11 for its **failure to “connect the dots.”** Though billed as a failure in communications, it was also a failure to fully utilize the information we had. The technologies that IDS is developing will play a role in preventing future failures, by intensifying the “signal” within available data and making it visible to more people, more rapidly. Our work is vital to help ensure our security against terrorism and natural disasters by **overcoming core technical obstacles in large-scale, efficient intelligence data analysis.**
 - **Discrete science is crucial for a wide variety of DHS missions.** For instance: The DHS Office of Intelligence and Analysis uses it to understand the terrorist threat to the U.S.; Immigration and Customs Enforcement uses it to guard against terrorist infiltration; Customs and Border Protection uses it in container inspection; the Coast Guard uses it to protect against incursion from invasive species; the Domestic Nuclear Detection Office uses it to search for nuclear threats; the BioWatch program uses it to detect both bioterrorist and naturally-occurring disease threats; and FEMA uses it to prepare for and predict natural disasters.
- **IDS/UAC research will serve to protect our nation while also serving to protect our nation’s data from invasion of privacy.**
 - UAC research **will not involve data collection and will only use open-source data.** There is a vast amount of open-source data that has the potential to help eliminate threats. Analysts consider it imperative to develop cutting-edge methods that analyze vast amounts of open-source data that could help us detect threats. Work on analysis of open-source data is being carried out widely already. We need world-class experts to do it better.
 - Our adversaries have the skill and ability to extract information from open-source data and are surely doing it. **We need to keep ahead of our adversaries, both known and unknown,** and also understand what they might learn. We must, for our own defense, know what can be gleaned from our open source data. Research on privacy-preserving data analysis is crucial in helping us protect our data from our adversaries by helping us understand the extent to which privacy can be compromised in data analysis. **We cannot respect privacy if we don’t know what we are revealing.** The IDS/UACs can become

a trusted advisor on such issues, identifying potential areas for misuse and designing appropriate safeguards.

- **Privacy protection can and must be a design constraint in data analysis.** Privacy preserving data analysis is already a subject of academic study, and is part of the UAC work. DHS can become a national leader in developing principles that ensure privacy protection in data analysis methods. Privacy protection methods include technical, administrative, and legal approaches, such as anonymization, use of cryptography, sophisticated restrictions on access to data sets, and development of Institutional Review Board (IRB) processes for the protection of citizen privacy.
- Research on privacy protection in data analysis can **both help us protect our citizens' privacy and also help us develop techniques that will protect the privacy of our data from our adversaries.**
- **Technological advances in any field open the door to both opportunity and misuse.** In all such cases, we need to weigh the benefits against the risks. In the case of discrete science, **the benefits far outweigh the risks.**
 - Nuclear science provides energy capabilities but with it a nuclear threat. Space exploration is inextricably linked with missile systems. Modern telecommunications, if not properly managed, could also threaten privacy. **In each case, we develop the science and technology for its potential to enhance our goals and with built-in technical protection mechanisms, and then enact regulation and law to preclude its misapplication.** Information science is no different. The IDS/UACs, by understanding both potential benefits and opportunities for exploitation, can develop new capabilities and be a partner in preventing their misuse, providing safeguards through algorithmic instrumentation and technical guidance to lawmakers.
 - Discrete science in general and the aggregation of multiple data sources in particular certainly has the potential for misuse. In particular, since this research deals with information about people (among other things), there is a clear issue regarding personal privacy. However, **by choosing not to develop discrete science methods, we in no way prevent the threat to privacy,** we simply leave this to someone else.
- Information science, and specifically **the research program of the IDS/UACs, has great potential benefits to many critical areas of national importance.** This potential lies not only in national security applications, but also in applications from other fields that must reconcile large amounts of data from a variety of sources. These fields include medical informatics/health care, environmental protection, and natural hazard prediction.