FPF serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

Big Data: FPF has pursued a combination of practical strategies and high-level thought leadership to address new opportunities and privacy risks presented by novel uses of personal information. FPF has centered its big data work on de-identification and ethics, examining both research and applications of analysis using novel or previously unmanageable datasets.

De-Identification: FPF has proposed a practical framework for applying privacy protections based on the nature of data that is collected, the risks of re-identification, and the legal and administrative protections that may be applied. FPF's framework, described in Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification, was published in the Santa Clara Law Review.

Ethics: FPF is calling for new frameworks and standards to promote valuable research and to ensure the ethical use of data for research. Sponsored by the National Science Foundation and the Alfred P. Sloan Foundation, FPF held a day-long workshop regarding ethical review mechanisms for data collected in corporate, non-profit, and other non-academic settings. The program resulted in the publication of a law review, Beyond IRBs: Ethical Review Processes for Big Data Research. FPF is also pursuing cutting edge work regarding the risks of algorithmic discrimination, potential solutions that can address those risks, and the benefits and privacy implications of artificial intelligence.

Brussels Privacy Symposium: FPF and the Vrije Universiteit Brussel co-founded a program to develop and promote research, scholarship and best practices to support beneficial uses of data while respecting individuals' fundamental rights. The annual Brussels Privacy Symposium draws on the expertise of leading EU and US academics, industry practitioners, and policymakers to highlight innovative research on emerging privacy issues.

Internet of Things (IoT): FPF convenes and enriches dialogue between business and consumer advocates about the privacy and security concerns surrounding networks of smart devices. FPF published Always On: Privacy Implications of Microphone-Enabled Devices and Kids and the Connected Home, white papers that highlight privacy issues regarding key IoT technologies. FPF has argued that IoT data needs to be used in ways that will benefit disadvantaged populations and promote inclusion in filings and op-eds.

Location and Ad Practices: FPF analyzes new location based technologies and educates companies and regulators about their use. In conjunction with the Local Search Association, FPF published Understanding Beacons: A Guide to Bluetooth Technologies. FPF explores evolving advertising technologies and identifies potential privacy issues and appropriate consumer controls. FPF developed a website for opting out of Mobile Location Analytics and is creating a comprehensive Ad Tech Due Diligence Guide.

Smart Communities: FPF appreciates the value in technologies that inform and streamline municipal services while respecting individuals' privacy. FPF published an interactive visual guide to smart city technologies and data flows, Shedding Light on Smart City Privacy, as well as a central repository for privacy-related guidance documents, best practices, reports, codes of conduct, and other resources relevant to smart communities. FPF is developing a *Privacy and Security Readiness Guide* for municipal technology and privacy leaders. FPF convened a roundtable, Privacy in the Smart City: Finding the Middle Ground, to discuss how we can secure social benefits while protecting autonomy. FPF is working with the City of Seattle to perform a privacy risk assessment of the city's Open Data program.

Connected Cars: FPF advances privacy practices and understanding of new in-car technologies. Responsible data practices help ensure the benefits of technologies are well-received by consumers. In conjunction with the National Automobile Dealers Association, FPF launched a consumer guide to educate drivers about data collection and use. FPF published The Connected Car and Privacy: Navigating New Data Issues. FPF files comments with regulators, including the FTC and NHTSA, and is developing a taxonomy to analyze how personal data is used in connected cars.

K-12 Education: FPF maintains a comprehensive education privacy website, FERPA|SHERPA, and launched the Student Privacy Pledge, now with over 300 signatories, to ensure the responsible handling of student data. FPF published A Parent's Guide to Student Data Privacy Rights *and* The Educator's Guide to Student Data Privacy. FPF administers an annual survey examining parental support for technology and beneficial data use in schools and hosts privacy boot camps for ed tech vendors.

Higher Education: FPF believes that critical improvements to learning that are enabled by data and technology, and that the use of technology is not antithetical to protecting student privacy. In order to facilitate this balance, FPF equips and connects advocates, industry, policymakers, and practitioners with substantive practices, policies, and other solutions to address education privacy challenges.