국가차원에서의 프라이버시 연구 전략

1. 요약

현대인들의 삶은 사이버 공간, 정보 시스템과 밀접한 관련이 있다. 컴퓨터 발전은 다양한 경제발전에 기여했고, 인터넷과 모바일 커뮤니케이션은 사회의 상호작용에 큰 영향을 미쳤다. 교통, 교육, 보건 등 다양한 분야에서 데이터 수집과 컴퓨터화가 가능해지면서 디지털 트렌드는 급속도로 성장할 전망이다. 하지만, 데이터가 대량으로 수집, 처리, 저장되면서 개인의 온라인 사생활 보호에 대한 논란이 불거지고 있다. 대량의 데이터를 분석하는 것은 과학, 공학, 의학 분야에서는 필수적이지만, 사전동의를 받지 않고 대량의 개인정보들을 다른 데이터와 결합하거나 재사용하는 것은 범죄와 차별, 의도하지 않은 정보공개, 오명, 또는 곤란한 사태를 초래할 수 있기 때문이다. 개인정보와 관련된 다양한 리스크는 이용자들로 하여금 온라인 이용을 감소시키는 효과 (chilling effect)를 불러일으킬 수 있다.

미국 연방정부는 개인정보침해사고 대응과 처리방법을 위해 연구개발의 중요성을 인지하고 있다. 최근 발표한 "빅 데이터: 기회 포착과 가치 보호 (Big Data: Seizing Opportunities, Preserving Values)" 보고서에 따르면 연구개발을 위한 투자를 강화하고 컴퓨터 공학과 수학 외에도 사회과학, 커뮤니케이션, 법적 규율 등을 통합한 대규모 융.복합 연구가 필요하다고 주장했다.

국가 프라이버시 연구전략 (The National Privacy Research Strategy)은 정부 지원을 받아 내외부적으로 진행될 연구에 대한 목표를 선정하고, 프라이버시 강화 기술에 대한 연구 체계를 구축하고, 정부와 사회의 역할에 대해 통합적인 연구를 장려하고자 기획되었다. 국가 프라이버시 연구전략의 주요 목표는 개인과 기업, 정부가 새로운 지식과 기술을 통해 기술 발전으로부터 오는 혜택을 누리고, 기술혁신의 기회를 늘리고, 개인정보와 프라이버시를 위한 의미 있는 보호정책을 만드는 것이다.

국가 프라이버시 보호를 위한 연구전략의 핵심 주제들을 아래와 같다.

- 프라이버시 연구와 해결방안에 대한 다각적인 접근방법 모색
- 프라이버시에 대한 이용자들의 욕구 이해와 효과 측정
- 프라이버시에 대한 이용자들의 욕구, 필요조건, 규제를 포함한 시스템 디자인 개발
- 데이터 수집, 공유, 이용, 보관에 대한 투명성 향상
- 정보의 흐름과 사용이 프라이버시 규제를 따를 것이라는 보장성 강화
- 프라이버시 침해 시 해결방안과 복구 방법

- 분석적 알고리즘의 프라이버시 위험 감소

2. 소개

2.1 프라이버시 연구 목적

네트워킹과 정보기술은 사람과 기업, 정부간의 소통방법을 개선함으로써 21세기 현대인들의 삶에 변화를 주고 있다. 컴퓨팅, 커뮤니케이션, 데이터 보관의 혁신적 발전은 사회복지 (social well-being)를 향상시키고, 건강과 의료환경을 개선하고, 교육과 취업에 대한 진입장벽을 제거했다. 또, 제조업, 교통, 농업과 같이 다양한 부문에서의 발전에 기여하고 있다.

새로운 애플리케이션이 약속하는 "변화"는 대량으로 정보를 생산 및 수집하고 전송.처리.보관을 할 수 있는 능력에서 비롯된다. 하지만, 수집된 많은 양의 개인정보가 다른 데이터와 결합되거나 재분석되는 경우도 늘어나면서 데이터를 어떻게 관리 할지에 대한 논의가 심화되고 있다. 개인정보가 다양한 목적으로 사용될 수 있게 됨으로써 범죄와 차별, 사전동의 없는 공개, 부적절한 결정 등 불리한 결과를 가져올 수 있다. 데이터 수집에 대한 프라이버시 위험은 새로운 기술 사용에 대한 이용자들의 의욕을 저하시키고 (chilling effect) 더 나아가 기술 발전에도 해가 될 수 있다. 따라서 이 시대 가장 큰 도전은 대량의 정보가 생산, 수집, 보관, 처리되어도 국가의 핵심 가치들은 변하지 않는다는 믿음을 심어주는 것이다.

한 세기 넘게 시민들, 입법자들, 학계 내에서는 기술발전이 개인정보에 어떤 영향을 줄지에 대해 고민해왔다. 미국 입법도 오래동안 소비자들의 프라이버시 보호를 위해 다양한 분야에서 구체적인 법률을 마련해왔지만, 급격히 발전하는 데이터 수집, 처리, 보관 능력을 따라가는 것이 벅찬 상황이다.

오늘날의 정보는 복잡하고 다이나믹한 생태계에 다양한 주체들과 공존하고 있다. 개인과 관련이 없을 수도 있는 수집자 (collector), 데이터를 구입 판매하는 데이터 브로커 (data broker), 정보처리 시스템을 만드는 분석 기술자 (analytics provider), 분석결과를 통해 데이터를 사용하는 데이터 유저 (data user)들이 정보 생태계를 구성하고 있다. 데이터 보관료의 급락, 인터넷에 상시 연결되어있는 스마트 기기, 환경감지기, 추적시스템등은 기업들이 대량의 데이터를 수집하고 장기간 보관할 수 있는 기회를 제공했다. 하지만, 어떤 데이터가 얼만큼 수집 및 활용되는지 정확하게 공개되지 않고, 기업의 목적에 맞춰 각기 다른 데이터를 모아 사용하는 모자이크 효과 (mosaic effect)"가 가능해지면서 개인정보 유출과 잘못된 추론에 대한 위험이 증가하고 있다. 독립적인 데이터일 때는 문제 되지 않다가 데이터를 결합 및 가공하게 되면서 문제가 제기되고 있다.

이러한 기술 발전에 맞춰 오바마 행정부는 프라이버시 관련 폭넓은 이슈들을 해결하기 위해 적극적으로 리더십을 발휘하고 있다. 사이버 보안을 구현하기 위해서 2011년에는 NSTIC (National Strategy for Trusted Identities in Cyberspace)를 발표했다. NSTIC는 공공ID와 개인ID등 다중ID를 제공함으로써 보다 신뢰성 있는 신원 확인을 가능하게 한다. 온라인 거래의 안전성을 높이기 위한 NSTIC제도는 공공과 개인의 사업영역이 협력할 수 있는 로드맵을 수립했다. 소비자의 정보보호와 관련해서 오바마 정부는 2012년 소비자 정보보호 권리장전 (Consumer Privacy Bill of Rights)을 도입해 기업들이 이용자로부터 수집한 개인정보를 어떻게 사용하고 보호해야하는지 전반적으로 규정했다. 최근 발표한 "Big Data: A Report on Algorithmic Systems Opportunity, Civil Rights (빅데이터: 알고리즘 시스템, 기회, 그리고 시민권리)"보고서는 빅데이터와 알고리즘 사용이 다양한 영역에서 차별이 이루어질 수 있다는 것을 지적했다.

2014년 미국정부는 네트워킹 및 정보기술 연구개발 (Networking and Information Technology Research and Development, NITRD)에 총 3억9천만 달러를 지원했다. 이 중 프라이버시 관련 연구에는 8천만 달러가 투자됐으며, 투자금은 다시 의료, 프라이버시 준법, 종합적인 정보보호, 컴퓨터 보안상에서의 정보보호 연구로 세분화되었다. 각 분야의 개인정보보호 연구도 중요하지만, 프라이버시에 대한 종합적인 연구전략이나 목표로 이어지지 않음으로써 프라이버시 연구는 아직도 잠재성이 많다고 판단된다.

미국 오바마 정부의 과학기술자문위원회 (The President's Council of Advisors on Science and Technology, PCSAT)는 빅데이터와 프라이버시에 대한 협동 연구를 해야한다고 주장하고 있다.

> "네트워킹 및 정보기술 연구개발 (Networking and Information Technology Research and Development, NITRD) 부서는 미국 과학기술 정책국 (Office of Science and Technology Policy, OSTP)과 협력해 프라이버시 관련 기술개발과 새로운 기술을 어떻게 사회에 도입할 수 있을지에 대한 연구를 강화해야 한다. 개인정보보호를 위한 제어 기술은 이미 존재한다. 이제는 프라이버시를 보호해줄 수 있는 기술개발, 개인정보보호를 위한 사회적 메커니즘 구축, 급속한 기술발전에도 유효한 법률을 만들어야 한다. 국가 보조의 연구를 통해 기술이 프라이버시와 경제발전, 국가 주요 정책과 공존할 수 있도록 도와야 할 것이다."

PCSAT의 제안에 따라 국가 프라이버시 연구전략 (The National Privacy Research Strategy)은 전략적인 목표를 설정하고 정부기관들이 프라이버시 관련 연구개발을 어떻게 도울 수 있을지에 대한 가이드라인을 제시한다. 국가보조연구를 통해 새로운 지식을 창출하고 프라이버시와 관련된 위험요소들을 파악 및 완화할 수 있는 기술을 개발할 계획이다. 이번 연구전략의 목적은 정보기술이 줄 수 있는 혜택을 깨닫고 부정적인 인식을 최소화하는데 있다. 잠재적인 위험을 줄이기 위해서는 데이터 수집과정부터 데이터가 사용되는 과정을 세심하게 관찰하는 등 다양한

방법을 모색해야할 것이다.

연구목적을 이루기 위해서 NPRS는 프라이버시가 직면하고 있는 다양한 도전들의 연장선에서 문제를 제시한다. 어떻게 사용자들이 프라이버시를 이해하고 있는지, 어떤 프라이버시 니즈가 있는지, 사용자들의 욕구는 어떻게 존중될 수 있는지, 개인정보가 침해 됐을 경우 어떻게 해결해야하고 방지할 수 있는지 등 다양한 상황에서 접근할 것이다. 끝으로, NPRS는 연구 결과를 정부와 사업자들에게 공유하여 이용자들이 안전하게 정보기술의 혜택을 누릴 수 있는 사회를 만들 계획이다. (Appendix A에 연구전략 발전 과정요약 참고)

2.2 프라이버시의 특징

프라이버시의 특징을 정의하는 것은 생각보다 쉽지 않다. 프라이버시를 포괄적으로 이해하기 위해서는 도덕, 철학, 사회학, 심리학, 법과 정부정책, 경제학, 기술과 같이 폭넓은 분야에서의 의미를 고려해야하기 때문이다. 미국 연방정부는 Fair Information Practice Principles (FIPPs)에서 제시하는 프레임워크를 따라 정보의 안전성, 적법절차, 공정성을 프라이버시의 주요 특성으로 바라본다. 2012년 소비자 정보보호 권리장전 (Consumer Privacy Bill of Rights)도 맥락의 중요성과 FIPPs의 프레임워크를 적용해 프라이버시를 정의했다.

정보시스템의 원칙들이 효율적으로 실행되기 위해서는 적절한 연구가 필요하다. 2014년 미국정부에서 발표한 빅데이터 관련 논문에서도 프라이버시는 "다양한 방법으로 이용자들의 사생활에 침입하므로 각 상황마다 적절한 보호가 필요하다"고 주장했다. 프라이버시는 개인의 사생활, 정보의 기밀성, 개인정보의 처리 제한, 정보주체의 권리 등 어느 부분에 초점을 두는지에 따라 여러 가지 방법으로 정의될 수 있다. 프라이버시의 특징과 정의는 지속적으로 변하고 있어 많은 연구 가능성이 있는 분야다. 프라이버시에 대한 연구개발은 특정한 시각이나 정의에 의해 제한되면 안된다. 다양한 방법으로 접근하고 일반적이거나 특수한 상황에서의 프라이버시 관련 사례들을 연구하여 연구의 폭을 넓혀야 할 것이다.

국가 프라이버시 연구전략 (The National Privacy Research Strategy)은 프라이버시의 주요 4가지 특징에 초점을 둔다 – 주체 (subjects), 데이터 (data), 행동 (action), 맥락 (context)

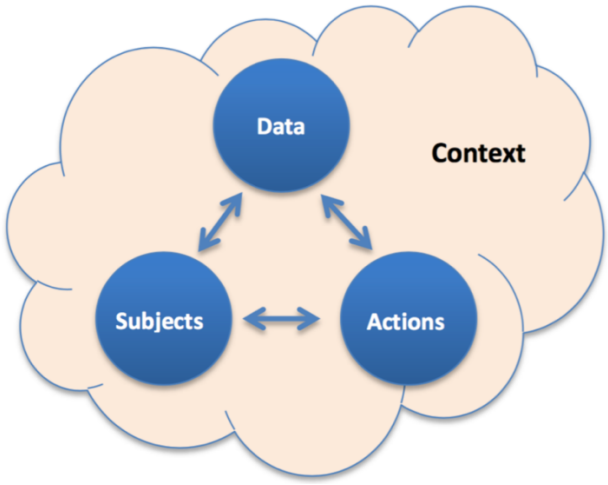

그림 1 NPRS 프라이버시 특징

주체 (subjects)는 정보의 주체인 개인 또는 단체를 의미한다. 허위 또는 익명의 신분으로 활동하는 주체들의 권리, 자율성, 개인정보보호 관련 욕구들을 포함한다. 데이터 (data)는 정보주체들의 모든 정보를 의미하고, 활동 (action)은 다양한 데이터를 수집, 처리, 분석, 저장하는 것 외에도 개인정보 이용을 규제하거나 데이터 수집으로 생기는 다양한 효과들을 뜻한다. 주체, 데이터, 활동의 상호작용의 영향과 생길 수 있는 위험 등은 각 맥락 (context) 안에서 해석될 수 있다.

이러한 특징 안에서 "프라이버시"는 적절하고 책임감 있게 정보를 수집, 생산, 활용, 처리, 공유, 전송, 저장, 보관, 보호, 삭제되야한다. 여기에는 이용자들의 개인정보를 합법적으로 보호하기 위해 데이터를 사용하지 않는 것도 포함한다.

2.3 프라이버시의 주요 문제점

아래의 문제점들은 이번 프라이버시 관련 연구 전략의 우선순위 선정에 영향을 준다.

2.3.1 맥락(context)의 영향

이용자들은 개인의 정보를 구체적인 목적을 가지고 커뮤니티안에 있는 다른 사람 또는 기관과 공유한다. 예를 들어, 이용자들은 자신들의 건강상태를 의료전문가들과 나눌 수 있고, 소매업자들과 선호하는 제품을, 로펌과 관심있는 규제방안을, 종교단체와 종교적인 질문들을, 여행사와 여행계획을 나누는 활동 등이 있다. 커뮤니티는 이용자들이 데이터를 나눌 수 있는

맥락을 제공하는 것이다. 만약 이용자들이 특정 커뮤니티에서 공유했던 정보가 의도하지 않은 곳과 맥락에서 발견된다면 이용자들은 개인정보가 침해됐다는 기분이 들것이다. 또 특정 맥락에서 주고받았던 정보의 가치도 훼손될 것이다. 프라이버시의 맥락적 특성은 프라이버시와 관련된 구체적인 질문들과 연관이 있다. 따라서 프라이버시가 누구에게 영향을 주는지, 콘텐츠는 무엇인지, 어떤 동기와 조건으로 이루어진 것인지, 어떤 역할과 관계를 위한 것인지 등을 자세하게 언급할 필요가 있다.

프라이버시의 맥락적 특징은 개인정보보호 시스템을 설계하는데 어려움을 준다. 맥락적 상황에 따라 바라보는 관점과 해석, 개선방향과 요구사항 등이 이용자들마다 다르기 때문이다. 또, 시스템 설계자들은 프라이버시 특성에 최적화된 기술을 제공하는데 어려움을 겪고 있다. 현재 기술과 컴퓨터 모델은 프라이버시 관련 IT시스템을 파악하거나 "의도된 목적", "예상 사용" 등 프라이버시가 적용되는 맥락을 이해하는데 한계가 있다.

2.3.2 데이터 수집, 사용, 보관의 투명성

데이터 수집과 사용의 투명성을 제공하는 데는 어려움이 있다. 현재 이용자들에게 제공되는 개인정보동의서와 같은 전통적인 프레임워크에는 한계가 있다. 개인정보 동의서 중 상세하게 쓰여진 것은 너무 길고 어려워 이용자들이 충분히 읽고 동의했을 것이라는 추측이 어렵고, 반대로 개인정보관련 폭넓게 서술하다 보면 향후 일어날 수 있는 다양한 상황에 대해 세밀한 동의가 부족할 수도 있다. 다양한 기관들이 이용자들의 데이터를 수집하고 활용하길 원하면서 이용자들은 자신들의 개인정보사용을 통제하고 관리하기 어려운 상황이다. 또 기술발전으로 인해 다양한 기기의 센서들이 교통, 환경 조절, 공공안전등에 사용되면서 개인정보관리는 더 어려워지고 있다. 투명성 확보와 이용자들의 선택과 동의, 규제기관의 효율적인 감시를 위해서는 더 나은 해결방안이 필요하다.

데이터 보관과 잠재적인 효과에 대한 대중의 이해도 매우 부족한 상황이다. 이용자들은 개인의 온라인 활동 기록에 대한 이해가 부족하다. 기록의 유효성과 개인정보 사용에 대한 통제를 요구하는 방법이 불분명하다. 기업들은 데이터 사용에 대한 변화가 있을 경우, 이용자들에게 효과적으로 알리는 방법이 없어 어려움을 겪고 있다.

2.3.3 데이터 집적, 분석, 공개

데이터 수집, 집적, 분석 등 기계 학습 (machine learning)의 능력이 증가함에 따라 세상에 대해 새로운 상관관계, 지식, 패턴을 발견하고 알고리즘을 분류 및 예측할 수 있게 되었다. 이용자들이 모르는 사이 보관되는 개인정보 데이터는 다양한 목적에 맞춰 기록 및 평가되어 기업 결정에 중요한 영향을 미치고 있다. 기업들은 이러한 알고리즘 기술에 의지해 다양한 결정을 내리고 있다. 하지만, 알고리즘에 의지한 의사결정은 차별과 편견 등을 초래할 수 있고, 아직 규모나

파문에 대한 피해가 알려지지는 않았지만, 예측하지 못한 결과들도 낳을 수 있다.

통계, 분석, 원자료 (raw data)를 개제하고 싶어하는 연방정부의 지속적인 관심과 노력도 프라이버시보호에 대한 우려를 낳고 있다. 미국정부는 개인정보보호를 위해 개인 식별 정보(personally identifiable information, PII)가 폐지된다고 밝혔다. 하지만, 이용자들의 데이터보호를 위해 예민하거나 기밀한 정보는 다시 이용자들에게 돌려주겠다는 방침은 데이터를 익명으로 보관하겠다는 본래 취지에서 어긋난다. 데이터수집은 데이터 남용에 대한 위험도 있다. 현재 사용하고 있는 k-anonymity[1]와 differential activity[2]는 프라이버시보호를 고려한 대표적인 모델이지만, 이 모델들도 데이터침해로부터 안전하다고 보장할 수는 없다

2.4. 희망사항

이번 NPRS의 목표는 새로운 지식과 기술을 창출해서 개인과 사업자, 정부가 기술발전과 데이터사용의 혜택을 누리는 동시에 적극적으로 프라이버시 관련 위험을 인지하고 완화시키는 것이다. 또, 이용자들이 자신의 사생활에 대한 영역을 쉽게 결정짓고 합의할 수 있는 방안들도 마련하는 것이다.

프라이버시는 정치적 표현의 자유와 선택의 기회를 제공해야하며, 소비자들과 기업들이 데이터 사용과 관련해 합의할 수 있는 공간도 제공해야 한다. 개인정보가 보호되지 않을 경우, 개인과 사회는 표현의 자유, 차별, 기관에 대한 신뢰성 감소, 제한된 혁신 등의 피해를 볼 수 있다.

지속 가능한 프라이버시 실현을 위해서는 특정한 맥락에 따라 적용될 수 있는 기술과 프라이버시 침해를 감지 및 완화할 수 있는 과학적 공학적 기반의 기술이 필요하다. 지금까지 프라이버시 기술과 애플리케이션에 대해 세부적으로 접근했다면, 이번 연구 전략은 프라이버시를 과학적으로 접근하여 문제점, 위험, 손해, 잠재적 혜택, 처리, 분석 시스템 등을 철저히 분석하는 것이다. 또, 프라이버시를 더 안전하게 보호하고 개인정보보호에 대한 이용자들의 기대를 충족시킬 수 있는 기술을 개발하는 것이 목표이다.

NPRS는 이번 전략을 통해 프라이버시에 대한 기준이나 규율을 세우려는 것이 아니다. *Cyberspace Policy Review*, *U.S. International Strategy for Cyberspace*, *Consumer Data Privacy in a*

---

[1] K-anonymity는 프라이버시 보호를 위한 공식적인 모델이다. K-anonymity보호를 제공한다는 것은 데이터세트에 포함된 모든 사람들의 정보가 잘 구분될 수 없다는 것이다.

[2] Differential privacy는 통계 데이터베이스에서 프라이버시를 다룰 때 사용하는 공식적인 모델이다. 이 모델은 개인이 전체의 성질을 알 수 있지만, 개인의 프라이버시는 알 수 없도록 보호해준다. 적당한 양의 인조적인 "noisy"데이터를 데이터베이스에 추가하여 한 개인의 정보가 추가되어도 정보의 통계적 성질이 데이터베이스에서 잘 구분될 수 없도록 만드는 원리이다.

Networked World, and *Big Data: Seizing Opportunities, Preserving Values*에서 기술한 것처럼 이용자들과 미국 연방정부가 개인정보보호를 위해 힘쓰고 지속 가능한 사회적 가치를 창출해낼 수 있도록 돕는 것이다. 이번 연구전략은 국가안보 또는 프라이버시 법률 집행과 관련되어 다루고 있지 않다 (하지만 연구 전략을 통해 관련된 이슈들을 이해하는데 도움을 얻을 것이다). Appendix B에서 프라이버시를 법률적이고 정책적인 맥락에서 논한다.

또, 이번 연구전략은 개인정보침해에 영향을 줄 수 있는 컴퓨터 보안 상태나 정보보안 실천에 대한 해결방안을 제시하지 않는다. 해당 내용은 2016 Federal cybersecurity R&D security plan을 참고하면 될 것이다.

마지막으로, 이번 연구전략의 우선순위들은 NITRD프로그램 안에서 계획되었으며, 각 정부기관에 구체적인 연구 의제를 제시하지 않았다. 대신, 행정부에게 전략목표를 제시하고, 각 부서들이 각처의 능력과 예산에 맞춰 유연하게 연구 의제를 설정할 수 있도록 했다. 부서들 간의 연구전략과 목표를 공유하고, 각 부서에게 자율성을 제공함으로써 공통된 주제 안에 다채로운 포트폴리오를 만들 수 있게 했다.

3. 국가차원에서의 개인정보보호 연구 우선순위

Information technology research-funding 부서와 함께 선정한 연구우선순위들은 프라이버시영역의 중요한 공백들을 메우는데 주력했다. 우선순위선정은 전략 수립에 중요하다. 미국 정부기관은 각처의 미션과 능력에 맞춰 전체 전략에 맞는 포트폴리오를 만들어야 한다. 이번 연구전략을 통해 각 부서들이 프라이버시 영역에서 평행한 노력을 할 수 있도록 계획되었다.

3.1 프라이버시 연구와 해결방안에 대한 다각적인 접근방법 모색

이 전략의 목표는 미국 정부가 주어진 미션과 책임을 수행하는 동시에 프라이버시 보호 능력을 향상시키는 것이다. 정부 각처의 연구 노력을 통해 시민들의 정보를 보호하고, 공정성을 보장하며, 차별을 방지하는 시스템을 구축하는 것이다. 프라이버시 연구는 컴퓨터 공학, 사회/행동과학, 생물과학, 심리학, 경제학, 법과 정책, 윤리 등 다양한 분야에서의 연구 접근이 필요하다. 다문학적인 접근은 통합적으로 프라이버시의 목표와 위험을 파악하고, 개인정보 관련 사례 (프라이버시침해 관련 타협을 맺는 활동)들을 이해하며, 기술자들을 위한 개인정보보호시스템 연구와 개인정보침해 해결방안 등을 찾는데 효과적이다.

프라이버시 관련 연구결과를 활용하는데 장애물이 있을 수 있다. 개인정보보호에 대한 새로운 접근은 기존의 기술시스템, 회사 경영, 규제와 법률에 영향을 미친다. 새로운 기술에 투자할 때는 초기 비용과 장기적인 혜택을 언급해야한다. 다각적인 방법으로 개인정보보호에 접근하면서 개인정보보호 기술 도입이 정책과 규율에 어떤 제한을 받는지, 회사는 어떤 태도로 바라보고 있으며 시장경쟁에는 어떠한 영향을 미치는지, 경제 사회적인 측면에서 인센티브는 있는지, 이용자들의 의욕을 저하시키지는 않는지 등 다양한 시각으로 분석해야한다. 또 다문학적인 접근방법을 통해 프라이버시가 어떤 시각으로 접근되었을 때 가장 효과적인지 알아봐야 한다. 기술적으로 설명되었을 때인지, 윤리와 정책면에서 설명될 때인지, 학문융합적 접근일 때인지 등 프라이버시에 대한 이해를 돕고 연구 결과를 최대한 적용하는 것을 목표로 삼아야한다.

개인정보보호 관련 장치들이 잘 적용되기 위해서는 시장 비효율 (market inefficiency)도 고려해야 한다. 시장 비효율이란 소비자와 판매자 간의 정보 불균형이다. 제품을 선택하는데 있어 특정한 제품품질에 대한 정보나 인지가 제한적일 경우, 소비자들은 특정품질에 대한 중요성을 알지 못할 수 있으며 판매업자들은 지속적으로 특정 품질에 대한 개발이나 정보공개를 거부할 수 있다. 여기서 특정한 제품품질은 정보보호 관련 요소들이다. 잠재적으로 시장비효율이 나타날 수 있는 영역(e.g. 제품 안전, 환경오염)들을 사례연구대상으로 삼아 시장비효율을 개선할 수 있는

방안들을 찾아봐야 할 것이다.

3.2 프라이버시 욕구와 영향에 대한 이해와 측정

프라이버시 욕구는 주로 다양하고, 맥락 중심적이며 예측하거나 측정하기 어렵다. 개인정보와 관련된 디지털 시대에는 프라이버시에 대한 욕구, 기대, 행동 규범과 규칙, 정보공개, 데이터 흐름 등을 파악할 수 있는 기술과 연구방법이 개발되어야 한다. 맥락 안에서 프라이버시 욕구를 이해할 수 있는 기술이 개발된다면 개인정보보호 관련 다양한 기술개발이 일어날 것으로 전망된다. 이용자들은 특정 맥락에 맞는 개인정보처리를 선택할 수 있을 것이며, 개인정보보호 시스템을 마련하기 위해 조건들을 검토할 수 있을 것이다. 이를 통해 프라이버시로 인해 이용자와 사회가 얻을 수 있는 혜택 또한 연구가 필요할 것이다.

시스템 설계자와 개발자들은 이용자들이 프라이버시 관련해서 무엇을 가장 중요하게 여기는지, 욕구와 기대는 무엇이며 어떤 방법으로 프라이버시가 위반될 수 있는지 등 사용자들의 입장을 존중하는 연구개발을 해야 한다. 사용자들의 니즈 (needs)를 이해할 때, 그들의 활동과 선택에 필요한 정보를 제공할 수 있고 최적화된 사회적 법적 제도적 장치를 마련할 수 있기 때문이다.

하지만, 소비자들의 관심을 이해하기 쉽지 않다. 프라이버시에 대한 사용자들의 욕구는 세대, 하위문화집단, 국익, 사회경제적 지위 등 다양한 이유로 다를 수 있기 대문이다. 이러한 차이는 프라이버시에 대한 전반적인 규범 (norm)을 정의하고 향후 어떻게 변할지에 대해 추측하는데 어려움이 있다. 또, 끊임없이 변하는 기술과 상황들은 프라이버시 규범을 정하는데 어려움을 더한다.

현재의 기술로는 여론이나 대중들이 원하는 프라이버시를 이해하는데 한계가 있다. 서베이 처럼 자기평가를 하는 것은 "프라이버시 패러독스 (privacy paradox)"에 빠뜨릴 수 있다 (프라이버시 걱정을 많이 한다고 주장하면서 온라인 활동은 걱정한 수준과 다르게 행동할 수 있다). 여론조사를 위해 개발된 새로운 기술 (e.g. 소셜미디어 분석)도 여론 이해에 도움이 될 수 있지만, 시스템 편향 (system bias) 문제나 조작 의혹 비판을 받을 수 있다. 특정한 IT환경에서 이용자들의 행동을 평가하고 측정하는 것도 문제가 있다. 이용자들은 실험이라는 것과 익숙하지 않은 IT환경으로 인해 평소와 다른 형태의 프라이버시 욕구를 드러낼 수 있다. 따라서 이러한 실험참여도 이용자들의 프라이버시 욕구를 이해하는데 좋은 지표는 아니다.

프라이버시 욕구와 함께 프라이버시 영향력도 측정해서 같이 비교해 봐야 한다. 프라이버시 효과는 특정한 사건 (e.g. 데이터 침해나 새로운 기술, 처리과정의 도입)으로 인해 만들어질 수 있다. 또 각기 다른 영역에서 축적된 데이터가 결합되었을 때 드러나는 비밀 정보도 프라이버시

영향력에 포함된다. 프라이버시 영향력과 욕구를 체계적으로 파악하고 분석해서 개인, 기업, 사회와 어떤 관계를 맺는지 (e.g. 어떤 편리함을 제공하는지, 얼만큼 비용이 절감되는지, 공공의료와 보안에 어떻게 사용되고 있는지 등) 관찰해야 할 것이다.

프라이버시 규칙, 규범, 욕구 등이 지켜지지 않을 경우 다양한 피해가 나타난다. 새로운 연구와 기술개발은 이와 같은 문제가 발생했을 때 쉽게 문제를 발견하고, 이해하고, 분석할 수 있도록 해야 한다. 특히, 알고리즘이 적합하지 않은 정보를 사용해서 결정을 내리거나 이용자들이 모르는 사이에 문제가 발생했을 때를 대비해 특정한 솔루션 개발이 필요하다. 프라이버시 사례들을 연구할 경우, 기술이 사회와 사람들에게 어떠한 영향을 주는지, 이용자들의 온라인활동을 어떻게 장려하고 저하시킬 수 있는지 (chilling effect) 등 다방면에서 알아봐야 할 것이다.

이번 전략은 프라이버시 욕구와 영향을 이해, 측정하고 필요한 기술이 무엇인지 연구하는데 의의를 둔다. 사회적 관행 출현과 체계화, 검토를 위한 기술개발과 프라이버시 관련 사례들이 만드는 효과들을 측정할 수 있는 방법을 연구해야한다. 이러한 이슈를 언급할 때는 기술적, 태도적, 경제적, 문화적, 사회적, 교육적, 심리학적, 민족적, 역사적 관점들을 다 포함하여 분석해야한다.

프라이버시 욕구와 영향을 세밀하게 이해하기 위해서는 프라이버시 관련 다양한 목표 (e.g. 개인정보 통제, 신뢰성, 맥락에 대한 이해와 존중, 투명성 등)를 정의할 수 있어야하며, 정보시스템이 프라이버시 목표를 달성할 수 있을지 측정하는 능력도 포함된다. 이러한 연구결과는 이용자들이 프라이버시 관련 선택을 하거나 기계의 분석 및 추리 결과를 신뢰하는데 기여할 것이다.

주요 연구 문제들은 아래와 같다.

- 어떤 연구 방법이 가장 정확하게 특정 또는 여러 커뮤니티의 프라이버시 욕구, 기대, 행동, 생각, 관심 등을 측정할 수 있는가?
- 프라이버시 욕구, 기대, 행동, 생각과 관심은 세대, 하위문화집단, 국익, 사회경제적 지위 등에 따라 어떻게 다른가?
- 프라이버시 욕구, 기대, 행동, 생각과 관심이 달라지는 이유는 무엇이며, 어떻게 달라지는가? 변화에 영향을 주는 특정한 요인들이 있는가?
- 프라이버시 관련 기술, 정책, 관행을 도입하는데 어떤 인센티브가 효과적일까?
- 프라이버시 인센티브는 사회가치 (e.g. 사회 정의, 경제성장, 보안, 혁신)에 어떤 효과를 가져올까?

- 프라이버시 관련 인센티브는 (e.g. 무료 서비스를 위해 개인정보공유를 허락) 이용자들이 프라이버시에 갖는 기대, 행동, 생각과 관심을 얼만큼 제한하는가?
- 어떤 방법과 기술이 프라이버시 사건과 영향을 파악하는데 효과적인가? 어떤 방법으로 측정 결과를 관련 단체나 시스템에 효율적으로 공개할 수 있는가?
- 어떻게 프라이버시 사건이 프라이버시 침해로 해석될 수 있는가? 프라이버시 침해는 어떻게 확인, 측정, 분석될 수 있는가?
- 프라이버시 사례들은 사용자들의 행동에 어떤 영향을 주는가? 프라이버시 사례로 인해 생기는 사용자들의 "chilling effect"는 어떻게 측정될 수 있는가?
- 이용자들의 요구를 정책적, 규제적, 법적 기관들에게 효율적으로 전달할 수 있는 방법은 무엇인가?
- 이용자들은 기술과 경제적 요인들이 개인의 프라이버시에 영향을 주는지 얼만큼 인지하고 있는가? 또, 이용자들은 데이터 수집자와 데이터 사용자들과의 정보 불균형에 대해 얼만큼 알고 있는가?
- 국가마다 다를 수 있는 프라이버시 욕구, 기대, 행동, 생각과 관심은 프라이버시 관련 법과 규제에 차이가 있는가?
- 어떤 형식으로 프라이버시 목표와 영향을 정의할 수 있을까? 정보시스템이 프라이버시 관련 목표를 잘 달성하고 있는지 어떤 기술과 메트릭 (metric)을 이용할 수 있을까?
- 프라이버시 목적은 개인, 기업, 사회의 목적과 어떤 관계를 형성하고 있으며, 어떻게 이해하고 분석될 수 있는가?
- 프라이버시 정책의 효과가 프라이버시 사례와 시장에 주는 영향을 어떻게 국내외적으로 평가할 수 있는가?

3.3 프라이버시에 대한 이용자들의 욕구, 필요조건, 규제를 포함한 시스템 디자인 개발

시스템 공학은 기술과 경영의 노력을 체계화하는데 사용되는 학제적 접근방법으로서 이해관계자의 니즈와 기대, 제한을 솔루션으로 변화시켜 지속적으로 솔루션을 지지하는 것이다. 시스템이 수집, 분석, 생산, 공개, 보관 등 다양한 방법으로 이용자들의 개인정보를 처리할 때 이용자들의 프라이버시에 영향을 줄 수 있다. 시스템 설계자들은 이용자들을 솔루션 개발에 있어 이해관계자 (stakeholder)로 생각해야한다. 하지만 현재 프라이버시 엔지니어링 솔루션

(engineering solution)은 이해관계자들의 관심을 이해하는데 있어 부족하다. 여기서 엔지니어링 솔루션이란 적합한 보호 방법과 이해관계자들의 프라이버시 관련 관심을 파악하는 것을 의미한다. 프라이버시 관련 설계를 할 때는 이용자들의 프라이버시 욕구를 시스템 조건 및 제어들과 잘 연결하여 이용자들의 기대에 충족시킬 수 있는 기술개발이 이뤄져야한다.

하지만, 이런 시스템 개발에는 여러 한계가 있다. 예를 들어, 시스템 설계자들은 최적화된 프라이버시 시스템을 설계하는데 필요한 도구가 부족하다. 또 시스템이 프라이버시에 줄 수 있는 영향을 이해하고 체계적으로 접근하는데 한계가 있다. 따라서 프라이버시를 설계에 포함시켜도 시스템이 프라이버시에 줄 수 있는 위험이나, 시스템에 필요한 프라이버시 요건들을 파악하고 장치를 디자인하는데 어려움이 있는 상황이다. 더불어 다른 영역과 비교했을 때, 프라이버시는 위험을 수량화할 수 있는 모델이 부족하다.

리스크 식별 (Risk Identification)과 관리는 시스템 공학의 일부이다. 시스템 기술자들은 지속적으로 프라이버시 목표를 기억하며 프라이버시 정책이 각 개발 단계마다 적용될 수 있도록 해야한다. 시스템 오너 (owner)들은 기업의 다양한 이익 (효율성, 비용, 기능성, 미션, 시스템 품질 요인 등)과 기회비용을 고려해서 결정해야 한다. 프라이버시 엔지니어링 목표가 공유되지 않으면 시스템 오너들과 기술자들은 프라이버시가 다른 시스템 목표들과 어떻게 상호작용하는지 분석하기 어렵기 때문이다. 기술자들이 프라이버시와 다른 시스템 목표들과 공존할 수 있는 솔루션을 만들기 위해서는 가이드라인을 제공해줄 수 있는 연구가 필요하다.

시스템 디자이너들이 다양한 프라이버시 제어기능 중에서 선택, 시험, 증명 하는데 필요한 도구 개발과 프라이버시 보호 장치들을 결합해 운영 시스템에 기여할 수 있는 방법도 연구해야한다. 예를 들어, 프라이버시 원칙이 시스템에 원활하게 실행되기 위해서는 디자인 패턴을 활용해 다양한 솔루션을 적용하고 공유할 수 있을 것이다.

개선된 프레임워크와 도구는 시스템제어와 시스템설계에 어떻게 적용될 수 있을지 연구에 기여함으로써, 프라이버시 엔지니어링과 위험관리 분야 발전에 기여할 수 있다. 프라이버시 제어를 기업의 통제로 분류할 수 있지만, 암호기법(cryptography-based)을 이용한 기술들을 시스템 레벨에 적용함으로써 더 긍정적인 프라이버시 결과를 가져올 수 있다. 프레임워크, 위험 모델, 제어 기술을 협력하여 만듦으로써 프라이버시 위험 분석능력을 향상시키고 다른 프라이버시 통제들과 비교하는데 도움이 될 것이다. 이러한 기술개발을 통해 개인정보와 프라이버시 측정을 종단간 측정 (end-to-end determinations)으로 변환하는 것이 목표이다.

지속적으로 변하고 있는 프라이버시 욕구를 시스템 디자인과 발전에 도입하기 위한 연구가 필요하다. 보안 위험은 변할 수 있어도 보안 관련 목표, 디자인, 엔지니어링은 고정적이며, 위험 대응도 기존의 위험 처리과정을 기반으로 진행되고 있다. 변하는 기술 환경과 프라이버시 욕구의

접점을 이해하기 위해서는 프라이버시 관련 목표와 처리 과정을 정의하는 것이 중요하다.

주요 연구 문제들은 아래와 같다.

- 프라이버시 리스크 확인과 관리를 위해서는 어떻게 모델화 되어야하는가?
- 프라이버시 관련 정책과 원칙은 시스템의 어떤 특징들과 합쳐져서 적용될 수 있을까 ?
- 프라이버시 특징들은 어떻게 구분, 분석, 수량화 될 수 있을까?
- 어떤 프라이버시 디자인 패턴과 사용 사례가 시스템 개발자들의 솔루션 개발에 도움이 될까? 특히, 사이버 물리 시스템 (cyber-physical systems)과 IoT 환경에서 도움될 프라이버시 디자인 패턴과 사용 사례는 무엇인가?
- 프라이버시를 향상시키는 암호기법 기술 (cryptographic technologies)은 어떻게 개발되고 현 시스템에 적용될 수 있는가?
- 어떤 메트릭(metrics)이 프라이버시 통제 효과를 분석할 수 있는가?
- 프라이버시 위험은 시스템과 데이터 사용에 있어 어떻게 고려되고 통제되어야 하는가?
- 어떤 메트릭과 측정이 프라이버시와 시스템 유틸리티를 각각 측정하고, 둘 사이의 트레이드오프(tradeoff)를 이해하고, 둘을 최대한으로 활용할 수 있는 시스템을 개발할 수 있는가?

3.4 데이터 수집, 공유, 이용, 보관에 대한 투명성 향상

이용자들은 오늘날의 복잡하고 다이나믹한 정보 생태계에 상당한 부담을 느낀다. 어떤 정보는 투명한 방법으로 수집될 수 있지만, 많은 정보는 개인이 모르는 사이에, 아무 관련이 없는 사람들이 수집한다. 예로 가정과 공공장소에서 센서 사용이 늘어나면서 엄청난 양의 개인정보가 축적되고 있지만, 데이터 수집과 이용이 비공개로 이루어지면서 개인의 데이터가 어떤 목적으로 수집되고 있는지 알 수 없으며 제3자에게는 어떤 방식으로 공유되고 있는지도 모른다. 비공개로 데이터가 수집, 처리, 공유되면서 온라인 사용자들은 자신들이 누리는 혜택이 어떤 선택에 의한 결과인지 알 수 없는 상황이다.

데이터 수집과 사용의 투명성을 향상시키기 위해 기획된 이번 연구전략은 사용자들이 프라이버시의 영향과 잠재적인 혜택에 대해 더 잘 이해 및 평가하고, 데이터 수집자와 데이터 사용자들이 개인의 정보를 더 보호하고 프라이버시 욕구를 존중할 수 있도록 연구하는 것이다. 데이터의 투명성 확보는 프라이버시 기술자들의 솔루션 개발에 기여하고, 개인과 데이터 수집자들의 니즈를 더 잘 반영할 수 있을 것이다. 또 투명한 시스템 실행은 규제기관들에게 데이터 수집과 사용의 모습을 더 시각적으로 바라볼 수 있을 것이다.

Notice-and-choice 접근은 비공개적인 활동의 투명성을 제고하고자 노력했다. 많은 데이터

수집자들은 프라이버시 정책에 따라 데이터 관련 활동들을 공개한다. 회사의 프라이버시 정책이 공개됨으로써 책임감 있는 데이터 수집 및 처리가 요구되는 상황이다. 하지만, 프라이버시 정책은 주로 찾기 어렵고, 과도한 전문용어나 개방형 의미를 가지고 있는 표현으로 기술되어 있어 이용자들이 이해할 수 없게 만들어져 있다. 사용자들이 프라이버시 정책을 읽고 이해하는 부담은 사용하는 기기에 따라 더 커진다. 모바일 환경에서 정책을 읽는 이용자들은 100장 이상 스크린을 넘기며 읽어봐야 한다. 이러한 부담을 줄이고자 일부 데이터 수집자/사용자들은 "just-in-time"과 같은 방법을 통해 간략하게 필요한 내용만 거래할 때 보여준다. 미국 정부는 여러관계자들을 동원해 프라이버시 정책이 모바일 애플리케이션에 표준화되어 보여질 수 있도록 노력하고 있지만, 투명성 메커니즘을 개선하고 데이터 처리과정의 공개를 위한 연구는 계속되어야 한다.

데이터는 항상 유효하다. 온라인 보관은 저렴하고 저장 공간도 많이 차지하지 않기 때문에 데이터 수집가들은 예전에 비해 대량의 정보를 수집하고 오래동안 보관할 수 있게 되었다. 개인정보를 어떤 목적과 용도로 사용할지 이용자들에게 알리는 시스템 개발은 이용자와 데이터 수집자, 데이터 사용자간의 정보 불균형을 완화시킬 수 있을 것이다

프라이버시에 대한 이용자들의 인식을 향상시키고, 오늘날의 시스템, 사업활동, 정보 흐름에 대해 이해를 높이는 활동이 매우 적은 상황이다. 따라서 특정한 비즈니스 모델이나 개인정보사용에 대한 통제 권한, 데이터에 대한 프라이버시 영향과 혜택 등에 대한 이해를 높이면 현재 이용자들과 데이터 수집/사용자들 사이의 정보격차를 줄일 수 있을 것이다.

주요 연구문제들은 아래와 같다.

- 정보 불균형을 발견하기 위해서는 어떤 실험 방법을 선택해야하는가?
- 정보 흐름을 측정하고 알리기 위해서는 어떤 도구나 자동 시스템을 설치해야 하는가? 개인정보 침해를 더 확산하지 않고 정보 흐름을 측정할 수 있는가?
- 이용자들에게 데이터 수집자와 데이터 사용자들의 개인정보 사용을 어떻게 알릴 수 있을까? 또, 데이터 수집자/사용자들에게 이용자들의 프라이버시 욕구와 선호는 어떻게 알릴 수 있을까?
- 시간에 따라 불가피하게 변하는 기술을 감안했을 때, 산업별로 다른 데이터 사용을 어떤 형식과 언어로 표준화할 수 있을까? 이용자들은 데이터 수집자와 데이터 사용자들의 데이터 접근 방식을 비교할 수 있을까? 프라이버시 보호를 위해 수집자와 사용자간의 경쟁을 장려할 수 있을까?
- 데이터 취급의 변화를 예측하는데 있어 얼만큼의 투명성 수준이 적합한가? 변화의 영향은 어떻게 측정될 수 있는가?
- 이용자들과 소통하지 않고 데이터를 수집하는 수집자들의 관행을 어떻게 알릴 수 있을까?

- 이용자들의 개인정보 사용에 대한 합의와 알림을 어떻게 표준화할 수 있을까? 또 어떤 방법으로 이해관계자들에게 전달했을 때 자동화된 시스템으로 거래비용을 줄일 수 있는가?
- 이용자들이 쉽게 프라이버시 정책을 읽고 이해하기 위해서는 어떻게 개선할 수 있는가? 텍스트, 폰트, 아이콘과 그래픽은 어떻게 표현될 수 있는가?
- 데이터 수집자와 데이터 사용자들은 개인정보 데이터와 관련하여 이용자들에게 의미있게 전달할 수 있을까? 특히 모바일과 비슷한 기기에서는 어떤 방법으로 전달해야 하는가? 또, "just-in-time"방법은 얼만큼 효과적인가?
- 다른 보호책이 없다고 가정할 때, Notice-and-choice 접근은 어떤 상황에서 비효과적인가?
- 투명성 메커니즘의 효과는 어떻게 평가될 수 있을까?

3.5 데이터 수집, 공유, 이용, 보관에 대한 투명성 향상

이용자들은 정보 흐름과 개인정보에 대한 규칙을 이해하고, 자신들의 개인정보가 규칙에 따라 잘 처리되고 있다는 확신을 얻을 수 있어야 한다. 향후 연구는 고도화된 기술들이 상황에 맞는 규칙에 따라 개인정보를 처리하고 있다는 것을 입증할 수 있어야 한다. 또, 가공된 데이터 결과에 대한 신뢰성 연구도 필요하다. 결과가 입력된 데이터로부터 나온 값인지, 규칙에 따라 수집, 처리, 활용된 데이터인지 알 수 있어야 한다. 맥락에 맞는 이용자들의 욕구와 정보사용을 구체적으로 분석하고, 코드(code)화 하기 위해서는 새로운 컴퓨터 모델과 언어가 필요할 것이다.

예를 들어, 데이터가 수집된 맥락을 잘 보존하여 표시(tag)하고 처리할 수 있는 기술이 필요하다. "맥락(context)"은 광범위한 의미로서 사람들의 동의나 선호, 법적인 조건, 지리적 위치, 데이터사용합의를 포함할 수 있다. 태그 기술은 이용자들의 사전 동의를 얻은 데이터로서, 수집자와 데이터 사용자들도 이용자들의 의견을 존중하고 사용허가가 된 데이터를 처리하는 것이다. 이런 기술개발은 개인정보 사용에 대한 이용자들의 권한을 표현하고 주장하는데 기여할 것이다.

코드를 규칙과 연관시키는 것도 중요하다. 코드가 규칙에 따라 데이터를 수집, 활용하는 것이 공개되면서 데이터 처리에 대한 객관성을 다른 코드들로부터 확인 받을 수 있을 것이다. 코드의 규칙화와 다른 코드들이 객관성을 입증해주는 방법은 시스템 책무성을 강화하여 프라이버시 정책의 침해를 발견하고 피해자들에게 알리는 것에 기여한다.

데이터 관리를 위한 기술개발은 데이터처리 및 보관하는 기업들이 기밀 정보를 법적, 윤리적 기준에 맞춰 잘 관리하고 있는지 확인하고, 잘못된 정보는 수정하고 삭제하는데 기여할 것이다.

또, 이용자들의 개인정보를 더 효율적으로 관리하고 이용자들의 선택을 존중할 수 있을 것이다. 데이터 수집자, 처리자, 서비스 제공자들과 이용자들 사이의 균등한 관계는 사회규범 형성에 기여하고 적합하지 않은 데이터 행동들을 자제시킬 것으로 기대된다.

주요 연구문제들은 아래와 같다.

- 정보흐름 관련 제어를 위해서 어떤 방법으로 구체화하고 관리할 수 있을까?
- 신뢰할만한 실행 환경(execution environment)을 만드는데 필요한 하드웨어와 소프트웨어는 정보흐름과 프라이버시 정책준수의 안전한 관리에 어떻게 도움이 될 수 있는가?
- 데이터와 소프트웨어의 출처를 밝히고 확인하고 보관하는 방법은 프라이버시 준법감시에도 사용될 수 있는가?
- 데이터 출처는 프라이버시를 침해하지 않고 찾아낼 수 있는 것인가?
- 프라이버시 정책언어와 다양한 정보흐름 성질들은 어떤 프로그램으로 분석 될 수 있는가? (여기서 분석 프로그램은 법적 전문가들에게도 의미 있고 시스템 기술자들도 시스템 책무성을 위해 개인정보 관련 코드를 관리할 수 있는 것을 의미한다)
- 컴퓨터 프로그램 시스템에 있는 개인정보 데이터 흐름을 효과적으로 이해하는 방법은 있는가?
- 데이터 처리에 적용되는 프라이버시 규범은 어떤 방법으로 입력(input), 처리(processing), 맥락(context)과 관련된 프라이버시 규범들에서 얻어지는가?
- 다른 데이터와 결합되면서 생기는 데이터 가치와 민감성의 변화는 어떻게 고려되어야 하는가? 정보처리 시스템은 이런 상황에서 어떻게 취급해야 하는가?
- 접근제어 시스템과 관련된 이용제한과 목적제한은 현재 시스템 디자이너들이 고민하는 프라이버시 이슈에 포함되는가?
- 효과적인 정보공개 통제, 데이터 de-identification방법, 데이터 de-identification방법을 평가할 수 있는 잣대가 있는가?
- 익명의 컴퓨팅, 암호화된 데이터 컴퓨팅, 그리고 다중의 신분 관리는 효율적이고 실용적인가?
- 현재 사용되고 있는 인터넷 infrastructure와 protocol은 프라이버시를 더 보호하기 위해

재설계 될 수 있는가 (i.e., 익명성을 지원하고, 검열 저항, metadata-hiding 커뮤니케이션)? 프라이버시는 사이버보안에 악영향을 주지 않고 인터넷 핵심 서비스에 도입될 수 있는가?

3.6 프라이버시 침해 시 해결방안과 복구 방법

직간접적으로 프라이버시 침해를 당했을 경우 복구를 위한 해결방안이 필요하다. 현재 프라이버시 침해에 대한 법적 조치나 인정이 이루어지는 편은 아니다. 또, 기존의 복구 메커니즘은 제한적이고 효능도 일관되지 않다. 복구의 어려움은 프라이버시 위험에 대한 중요성을 확대시키고 이용자와 데이터 수집자, 데이터 사용자 간의 불균형 문제를 증가시ㅣㅋ고 있다. 데이터 관련 행동(수집, flow, 사용, 특정 정보 공개 등)이 어떻게 운영되고, 피해를 끼칠 수 있는지 이해함으로써 복구에 대한 해결방안이 고안되어야 한다.

현재 사용되고 있는 기술적, 경제적, 법적 배상 메커니즘 (임금동결과 모니터링, 프라이버시 보호 보험, 프라이버시 타협에 대한 책임체제)의 효능과 배상이 없을 때의 결과 예측이 필요하다. 프라이버시 침해 시 실현될 수 있는 쉬운 복구 방법이 연구개발되어야 한다. 예를 들어, 데이터 위반과 유출에 민첩하게 대응할 수 있는 기술개발 외에도 잘못된 개인정보를 수정하거나 삭제할 수 있고, 적합하지 않은 데이터를 제거하고, 시스템 검열과 수정을 할 수 있어야 할 것이다. 더불어 배상관련 연구 (데이터를 가치 없게 만들거나, 정보 삭제 또는 "잊게" 만드는 메커니즘)도 필요하다.

주요 연구문제들은 아래와 같다.

- 어떤 기술적인 메커니즘이 프라이버시 침해 시 효과적으로 처리할 수 있는가?
- 프라이버시 침해 시 도입되는 해결방안과 복구 메커니즘의 효과는 재정적, 심리적, 사회적인 영향 면에서 어떻게 측정될 수 있는가?
- 프라이버시 해결방안과 복구 메커니즘의 존재는 프라이버시 침해 사례 가능성에 어떠한 영향을 미치는가?
- 해결방안과 복구 메커니즘 사용은 고도화된 프라이버시 기술 투자에 어떠한 영향을 미치는가?
- 프라이버시-보호 기술과 프라이버시-복구 기술을 어떻게 통합하면 더 효과적이고 효율적인 솔루션이 될 수 있을까?

3.7 분석적 알고리즘의 프라이버시 위험 감소

사람들의 행동과 태도를 예측하고, 사기혐의를 확인하는 알고리즘은 정부와 기업들 사이에서 오랫동안 사용되어 왔다. 사람들의 행동을 예측하는 알고리즘은 이용자들에게 혜택을 줄 수 있는 반면 특정한 성질들로 분류하게 되면서 개인의 선택이나 기회를 제한시킬 수도 있다.

최근 분석 알고리즘이 대량의 데이터들과 결합되고, 알고리즘의 결정에 의존한 시스템들이 늘어나고 있다. "분석적 알고리즘(Analytical Algorithm)"은 데이터를 우선적으로 처리하고, 분류하고, 필터하고, 예측할 수 있다. 이 알고리즘 사용은 잘못되거나 적합하지 않은 데이터 이용, 잘못된 결정, 부당한 배상, 알고리즘으로 인한 이용자들의 자율성 제한 또는 프라이버시 침해 등으로 인한 다양한 프라이버시 이슈와 관련이 있다.

데이터 집약적인 분석적 알고리즘의 다양성과 사용목적, 오용과 남용에 대한 가능성에 대해 대중들은 많이 모르며, 이런 알고리즘이 성별, 나이, 인종, 경제적 지위에 따라 다른 영향을 주는지도 명확하지 않다. 따라서 채용, 주택공급, 치안유지 등 중요한 부문에서의 알고리즘 사용은 균등한 기회에 대한 헌법과 관련되어 있으므로 알고리즘 투명성이 특별히 요구된다. 물론, 소비자의 신용 거래 데이터 제공과 관련하여 1970년 공정 신용보고법 (Fair Credit Reporting Act)이 도입되었다. 하지만, 공정 신용보고법은 오늘날 알고리즘이 소비자들을 차별하는 것은 아닌지 측정하고 이해하기 어렵다. 오래동안 학계에서는 알고리즘 차별 위험성에 대한 이슈를 제기했지만, 이런 연구를 진행하는 것은 엄청난 시간과 노력이 필요하고, 주 또는 하루 단위로 알고리즘 시스템을 바꿀 수 있는 상황에서 연구를 진행하기는 어렵다.

알고리즘을 예측목적으로 사용 할 경우, 책무성, 투명성, 감사를 위해 결과가 설명될 수 있어야 한다. 경우에 따라 이용자들은 어떤 개인정보가 알고리즘에 이용되고 있는지 통제할 수 있는 권한이 있어야 한다. 예를 들어, 1974년 대출기회균등법 (Equal Credit Opportunity Act)는 인종, 종교, 국적, 성별, 혼인 여부에 따른 신용 차별을 금지하고 있다. 하지만, 분석적 알고리즘은 이러한 영역에서 어떻게 운영되고 있는지 명확하지 않다.

따라서 현재 사용하고 있는, 또는 사용 계획이 있는 알고리즘에 대한 이해와 알고리즘에 대한 투명성, 책무성을 개선시키기 위한 연구가 필요하다. 이용자들의 개인정보사용 우려를 안심시킬 수 있는 능력, 정보사용권한 통제 방법, 알고리즘 애플리케이션 개발에 대한 정보 공유 방법 등에 대한 연구와 개선도 요구된다. 알고리즘으로 인해 생길 수 있는 문제들을 발견하고, 수정하고, 배상할 수 있는 기술도 필요할 것이다.

주요 연구문제들은 아래와 같다.

- 분석적 알고리즘과 시스템을 통해 얻은 결과가 개인과 단체에게 어떤 방법으로 나쁜

영향을 줄 수 있는가?

- 인터넷 사용자들이 이용분석 알고리즘 관련해서 갖는 고민은 무엇인가? 이런 고민을 표현하기 위해서는 어떤 정보가 필요한가? 사용자들이 필요한 정보는 어떻게 효과적으로 전달될 수 있을까?
- 개인 또는 단체에 대한 결정을 하는데 사용하는 데이터의 품질, 정확성, 출처는 어떻게 평가될 수 있는가?
- 데이터세트와 분석적 알고리즘의 호환성은 어떻게 평가될 수 있는가?
- 분석적 알고리즘이 부정확하거나 잘못된 데이터를 사용했을 때 개인과 그룹에게 미치는 영향은 어떠한가?
- 분석적 알고리즘이 내리는 결정과 예측이 법적 요구사항들을 잘 충족했는지 어떻게 측정하고 평가할 수 있는가?
- 분석적 알고리즘을 어떻게 설계하면 투명성, 책무성, 감사작업을 향상 시키고, 개인과 그룹에게 미칠 수 있는 악영향을 줄일 수 있을까? 개인과 정부, 산업을 위한 실용적인 알고리즘과 개입 매커니즘은 무엇인가?
- 분석적 알고리즘은 개인의 자율성과 에이전시(i.e., 독립적이고 자율적으로 선택할 수 있는 능력)에 어떤 영향을 미치는가? 분석적 알고리즘은 어떤 구조로 개인의 선택을 제한 또는 영향을 주는가?
- 새로운 기술과 알고리즘, 기술과 알고리즘의 결합은 개인정보보호 데이터 분석에 있어 어떤 실용적이고 이론적인 의미를 도출할 수 있는가?

이런 연구 질문들을 다 언급하기 위해서는 폭넓은 연구 의제를 설정해야 할 것이다. 기계학습과 통계 외에도 이번 연구 전략은 알고리즘과 이용자들간의 상호작용을 알아보기 위해 인간 요소(human factor)들도 필요로 한다.

4. 국가차원에서의 프라이버시 연구 전략 실행

이 연구전략은 프라이버시 관련 우선시되어야 할 연구주제들을 제시하며, Federal Networking and Information Technology Research and Development (NITRD)과 관련된 정부기관과 협력으로 제안되었다. 본 논문은 전략적인 계획안으로서 행정부, 정책 입안자, 연구자들, 그리고 대중에게 가장 효율적으로 자원을 투자해서 최대의 이익을 얻을 수 있는 가이드라인을 제시한다. 행정부 내 각 부서는 각자의 능력과 미션의 맥락에 맞게 제안 주제들을 연구 계획과 프로그램에 잘 수용해야 할 것이다.

National Privacy Research Strategy의 실행 여부는 각 정부기관 내에서 R&D활동을 계획하고 실행하는 부서들의 능력과 미션에 따라 결정된다. NITRD 프로그램의 보조금은 담당 부처들과 계획했으며, 참여 기관들은 국가의 프라이버시 연구가 안전하게 진행되기 위해 서로의 활동을 공유하여 중복되지 않도록 한다. 또 각 부처의 좋은 활동들은 서로 홍보 및 공유하고, 효과를 확대하고, 다양한 기관들과 협력하여 전반적인 NITRD 프라이버시 연구 포트폴리오에 기여해야 한다.

이번 프라이버시 연구를 통해 다양한 기대를 할 수 있다. 현재 실현되고 있는 정보 생태계 관한 연구는 프라이버시 이슈에 대해 여론에게 알리고, 정책 입안자들에게 유용한 정보를 제공해 줄 것이다. 새로운 프라이버시 이론과 연구모델을 적용하여 만든 프레임워크는 개인 (인터넷 이용자)이 프라이버시를 더 이해하는데 기여할 것이며, 프라이버시 도구 제작 안내를 제공하여 이론적인 발전에 더 기여할 것이다. 또, 프로토타입(prototype)과 관련 상품들을 통해 사회가 개인정보에 대한 희생 없이 정보기술 혜택을 누릴 수 있도록 노력 할 것이다.

본 연구 전략을 실행하는데 있어 제일 중요한 것은 포괄적인 선행연구를 통해 관련 주제들에 대한 기존 지식을 평가하는 것이다. 많은 영역에서 진행되고 있는 프라이버시 관련 연구들과 적용사례들을 파악함으로써 NPRS 연구에 의미 있는 기여를 할 수 있을 것이다.

펀딩 기관 (funding agencies)들은 연구자들이 연구하는 동안 잠재적인 실무자들, 대중과 만날 수 있는 기회를 적극적으로 마련해줘야 한다. 사회의 니즈를 파악하고 실무자들의 의견을 수렴하여 연구결과가 실제 사회에 필요한 연구가 되어야 하기 때문이다. 예로 "matchmaking" 이벤트를 통해 연구자들과 실무자들이 각자의 연구와 니즈를 공유함으로써 대중 또는 잠재적인 소비자들과도 향후 지속 가능한 관계를 맺을 수 있을 것이다. 또, 실제 데이터에 프로토타입 (prototype)을 시험해볼 수 있는 기회와 파일럿 스터디 (pilot study), 필드 스터디 (field study)를 위한 정부의 지원도 받을 수 있어야 한다. 투자자들은 연구 프로포절을 내는 연구자들이 연구 프로젝트가 마무리 됐을 때, 자신들이 연구한 기술을 잠재적인 고객들에게 넘길 수 있는지의

여부도 확인해야 할 것이다. 펀딩 기관들은 프라이버시의 다문학적인 성향을 고려하여 두 분야 이상의 공동연구도 장려해야 한다.

프라이버시-보호 기술과 솔루션이 특별한 애플리케이션에 적용되도록 만들어져도 어디서나 호환되어 문제 해결하는데 사용될 수 있다. NITRD 기관들은 개인정보보호 솔루션과 관련된 카탈로그나 공유 메커니즘 생산을 적극적으로 지원해줌으로써 솔루션이 각 기관과 대중들에게 공유될 수 있도록 해야 한다. 더불어 새롭고 개선된 방법과 도구가 채택될 수 있도록 정부는 인센티브나 다양한 조건들을 마련해야 한다.

Appendix A: 국가 프라이버시 연구 전략 배경

개인정보보호를 위한 미국정부의 노력은 다양하다. 예로 1929년 미국 인구 조사국의 한 요원이 기밀 자료를 공개함으로써 시행된 Census Act 이후 기밀 자료의 제공에 대한 엄격한 제한을 두고 있다. 이처럼 프라이버시를 지원하고 가능케 하는 것은 미국 정부의 주된 정책 원칙 중 하나이다. *Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 문서에는 소비자 프라이버시에 대한 정부의 정책이 표현되어있다. 또, 정보기술 중심의 현대사회가 직면하고 있는 프라이버시에 대한 문제들을 언급하고 법적 제안서 초안을 포함시켰다.

개인정보보호를 위한 기술문제와 기회는 지속적으로 관심을 받아왔다. 오바마 정부의 과학기술자문위원회 (President's Council of Advisors on Science and Technology (PCAST))의 2015년, 2013년, 2010년 NITRD 프로그램 리뷰에 따르면 디지털 시대에 개인정보보호에 대한 어려움은 대규모 네트워킹, IT시스템으로부터 오는 혜택을 누리는데 엄청난 장애임을 지적한다. 사회적 혜택에 얼만큼 악영향을 미치는지 알아보기 위해 National Telecommunications and Information Administration (NTIA)로부터 국가적 조사를 실시했다. 조사 결과 45%의 온라인 가정들이 프라이버시와 보안상의 이유로 온라인 활동 (금융거래, 제품/서비스 구매, 논란이 되는 주제에 대한 의사 표현)을 꺼려한다는 것을 알 수 있었다.

PCAST는 정부의 연구 기관들이 협력하여 프라이버시 보호에 필요한 과학적이고 공학적인 기반의 공동연구를 통해 기술과 솔루션 개발을 위한 장을 만들어달라고 요구했었다.

2014년 NITRD프로그램의 National Coordination Office (NCO)는 정부 기관을 대상으로 8천만 달러규모의 프라이버시 관련 R&D 노력들을 분석했다. *Report on Privacy Research within NITRD*에 따르면 NITRD는 혁신적인 연구 프로젝트를 진행하고 있으며 각 기관마다 프라이버시 관련 문제를 다루는 것으로 인식되었지만, 연구 효과를 극대화하고 R&D협력을 위해서는 각 기관간의 리서치 프레임워크 공유가 필요하다는 결과가 나왔다.

NITRD는 이러한 필요성을 인지하고 프라이버시를 향상시키기 위해 정부와 사회의 수요를 파악하고, 정부의 R&D투자와 관련하여 어떤 프레임워크를 정의하면 좋을지에 대한 고민을 했다. 2014년 9월 NITRD Cyber Security and Information Assurance Research and Development Senior Steering Group (CSIA R&D SSG)는 다양한 정부기관의 대표를 소집하여 "task group"을 소집했다. 정부지원 프라이버시 연구에 필요한 연구 전략과 목표, 우선순위 등을 정하고, 프라이버시 보호를 위한 R&D 개발, 종합적인(multidisciplinary) 학문적 접근을 통해 정부의 책임감과 사회의 수요 반영, 디지털 시대의 개발을 위한 기회 확보 등 프라이버시 관련 프레임워크를 계획하도록 했다.

CSIA R&D SSG의 특명을 받은 'task group'은 각 정부의 수요와 프라이버시 관련 기존의 연구

동향을 살펴보았으며, 대중의 의견도 세가지 방법으로 아래와 같이 살펴보았다. 1) 2014년 9월 미국 Federal Register에 게재된 정보 요청, 2) 2015년 2월 National Privacy Research Strategy 워크샵 3) Computing Community Consortium이 제안한 *Towards a Privacy Research Roadmap for the Computing Community*에 실린 리포트 검토 (자세한 사항은 NITRD 웹사이트 참고)

Appendix B: 프라이버시에 대한 법적, 정책적 맥락

미국 프라이버시 규제는 크게 세가지 영역 (상업적인 기관에 대한 규제, 정부 기관의 서비스, 국가 보안과 법 집행)을 아우르고 있다. 각 영역은 정부와 사업자들로부터 개인정보 침해를 막기 위해 오랫동안 법과 정책을 만들어왔으며, 최근에는 프라이버시에 대한 개념적 구상을 마련하기 위해 기본적인 기대와 가치, 통제와 접속 등에 대한 원칙에 집중하고 있다. .

공공부문에서의 프라이버시는 Fair Information Practice Principles (FIPPs)가 국가법, 규제, 지도(guidance) 형성에 영향을 미쳤다. 국가 차원에서 처음 제시된 프라이버시 보호는 1974년 제안된 개인 정보 보호법 (Privacy Act)이며 미국 다른 주에서도 비슷한 법령이 존재한다. Privacy Act는 국가나 공공기관이 수집. 관리하고 있는 개인정보를 보호하기 위한 법으로서 정보 수집, 정확한 정보 시스템 기록, 정보 공개 조건, 개인정보 접근 제공, 데이터 공유 수준 등을 다룬다. 개인 정보 보호법은 주로 기업 수준에서 세금정보, 인구조사 정보, 학생 정보 등 구체적으로 보호되는 내용의 정보에 따라 추가적인 규정과 규제가 적용된다. 기업 수준에서의 개인정보보호법이 강화되는 것은 이 외에도 FIPPs의 원칙인 사용제한, 목적 구체와, 보안 장치, 책무성을 반영해야 하기 때문이다. NIST Special Publication 800-53의 "Appendix-J"와 Security and Privacy Controls for Federal Information Systems and Organizations에는 정부가 도입한 25개의 각기 다른 프라이버시 통제가 기술되어있다. 여기에는 기업들을 위한 안내와 통제에 대한 법적 타당성도 포함되어있다. FIPPs와 관련된 모범 사례들에 따르면 프라이버시 통제 카탈로그(privacy control catalog)는 국가 정보보안 프로그램들을 보안 및 증가시키고, 프라이버시와 정보보안프로그램과의 민첩한 관계를 반영하는 것이다.

IT개발로 인해 개인정보가 다양한 산업에서 활용되면서 상업적 기관 규제는 미국 프라이버시 구조에서 매우 중요한 영역을 차지한다. 다른 국가들의 프라이버시 정책들은 개인정보를 전반적으로 보호하지만, 미국의 소비자 데이터 보호 구조는 통합적으로 모든 부문을 보호하라는 것이 법에 명시되어있지 않다. 대신 미국의 접근은 분야별로 접근하여 헬스케어, 교육, 커뮤니케이션, 금융 서비스에 데이터 보호 규제가 적용된다. 분야별 접근방법은 특정한 맥락에서의 통제를 제한하지만 틈을 남겨놓을 수도 있다. 예를 들어, 1974와 2004년까지 미국은 정부 데이터뱅크 (1974), 교육 기록 (1974), 금융 기록 (1978), 케이블 텔레비전 기록 (1984), 이메일 (1986), 비디오 대여 기록 (1988), 원하지 않는 전화수신 (1991), 운전면허 기록 (1994), 헬스케어 기록 (1996), 텔레커뮤니케이션 데이터 (1996), 어린이들의 온라인 정보 수집 (2001), 위성 텔레비전 기록 (2004)에 대한 프라이버시 보호 정책을 강화했다. 각 사례마다 의회는 서비스 받는 도중 수집된 시민들의 개인정보는 보호해줬다. 더불어 미국연방거래위원회 (Federal Trade Commission, FTC)는 "불공정하거나 거짓된" 프라이버시 행동을 하는 기업들을 규제한다. 예를 들어, 프라이버시 또는 데이터 보안에 대해 거짓된 보도를 하거나 적합한 보안방법을 사용하지

않을 경우 소비자들에게 상당한 피해를 입힐 수 있다.

미국에서는 자기규제가 상업시장을 감시하는데 매우 중요한 역할을 했다. 무역협회 또는 증명된 프로그램을 통한 자기규제는 정부보다 더 빨리 맞춤화 되어 규제를 실행할 수 있다. 자기규제는 시장기반의 솔루션으로서 이용자들의 니즈와 욕구에 맞춰 상품과 정책을 전달할 수 있고, 가장 빠른 방법으로 기업들에게 보상을 줄 수 있다. 또, 자기규제는 다양한 일 (규칙 만들기, 법률 시행 및 판결 참여)을 감당할 수 있다. Notice-and-choice모델은 이용자들이 어떤 개인정보 수집 및 사용에 합의하는지 (또는 합의하지 않는지)를 알아보는 것이다. 이 모델은 기업들로 하여금 자체 프라이버시 정책을 개발하고, 정보수집과 사용 목적에 대한 내용을 서술함으로써 개인정보관련 선택하는데 도움을 준다. 일부 비평가들은 자기규제와 notice-and-choice모델이 의미 있는 프라이버시 보호를 하는데 실패했다고 한다. 이용자들에게 시장선택의 권한을 늘리고 투명성을 제공하는 것 대신 길고 이해하기 어려운 프라이버시 정책들만 제공하고 있다고 주장한다. 또, 사전동의를 받은 데이터라고 해도 notice-and-choice 모델은 때에 따라 공격적으로 많은 양의 데이터를 공유할 때도 있다.

FTC의 미션대로 자유시장경쟁을 장려하고 "거짓되거나 불공정 관행"은 방지하기 위해 FTC는 자기규제 구조에서 백스톱(backstop)과 같은 지원역할을 하고 있다. 만약 기업이 소비자들에게 거짓된 보도를 할 경우, FTC는 FTC ACT에 따라 적합한 조치를 취할 것이다. 각 주 변호사도 비슷한 소비자 보호 권한이 있으며 FTC와 합작해서 중요한 역할을 맡고 있다.

2012년 미국정부는 *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting in Innovation in the Global Digital World*를 발표했다. 이 논문에서는 프라이버시 보호를 위해 4가지 주요 젼략 (Consumer Privacy Bill of Rights (CPBR) 채택, 여러 이해관계자과 행동규범 제작, FTC 단속강화, 글로벌 정보처리 상호 운영 개선)을 제시한다. CPBR 주요 원칙 (i.e., 는 맥락과 개인 통제에 대한 존중)을 세우고 각 기업의 재량권 아래 지켜지게 하겠다고 밝혔다. 정부는 또 CPBR를 성문화하고 행동강령을 제정하기 위한 법안을 발의했다. 이 법안으로 인해 FTC는 코드들에게 "harbor status"를 부여할 수 있게 되었다. 마지막으로, 백서에는 글로벌 정보처리 상호 운영을 위한 목표를 제시했다. 백서에 제시된 프레임워크는 2015년 정부의 Consumer's Privacy Bill of Rights Act Discussion Draft에서 실현 가능한 형태로 재조명되었다. 비록 이 초안은 의회에서 공개되지 않았지만, 미국 정부는 2012년, 2015년에 제시한 프레임워크가 소비자 프라이버시 보호와 신뢰성 확보, 혁신과 성장을 위한 유연성 유지에 적합한 프레임워크라고 믿고 있다.

프라이버시 법과 정책 만드는데 있어서 중요한 세 번째 영역은 법 시행과 국가 보안이다. 오늘날 법 시행국과 정보국은 데이터를 수집, 접속, 분석할 수 있는 능력이 있다. 많은 양의 데이터를 통해 "가상의 사진 (virtual picture)"을 만들고, 범죄예방, 공격방지, 테러범 추적에 도움을 줄 수

있다.

이들의 활동도 프라이버시 문제들을 만들 수 있기 때문에 법의 제제를 받는다. 예를 들어 미국 헌법에 규정된 첫 번째 권리 (표현의 자유)와 네 번째 권리 (부당한 검색 또는 압수)에 따라 제제당 할 수 있다. 법 시행국과 정보국의 활동도 Electronic Communications Privacy Act (ECPA), Privacy Act, Foreign Intelligence Surveillance Act (FISA)의 기관들로부터 법적 규제를 받고 있다.

프라이버시에 대한 걱정 없이 이용자들이 정보기술의 혜택을 누릴 수 있도록 효과적인 접근방법을 세우는 것은 어려운 일이다. 개인의 이해력, 태도, 기대, 행동 등에 있는 차이와 급진적으로 기술이 발전하기 때문에 접근방법을 세우는 것은 더 어렵다. 하지만 연구의 어려움과 연구결과를 해석해 정부정책과 상업적 기업들에게 공유하는 것을 우선순위로 둠으로써, NPRS는 프라이버시 이슈 관련 정책과 법 제정의 어려움 해결에 힘쓰고 있다.

National Science and Technology Council (NSTC)

NSTC 는 과학기술 정책의 종합조정을 담당 및 계획하는 위원회로서 미국 R&D 사업을 구성하는 다양한 엔티티(entity)에게 전달한다. NSTC 의 주된 목표 중 하나는 국가 과학기술 투자를 위한 명확한 목표를 세우는 것이다. NSTC 는 다양한 국가 목표를 이루기 위한 R&D 패키지를 준비한다. NSTC 는 5 개의 소위원회(Environment Natural Resources and Stability; Homeland and National Security; Science, Technology, Engineering, and Mathematics (STEM) Education; Science; and Technology)로 구성된다. 각 위원회는 과학기술에 대한 관점이 다른 각 소위원회 및 다른 그룹들의 일을 감독한다.

Office of Science and Technology Policy (OSTP)

OSTP 는 1976 년 National Science and Technology Policy, Organization, and Prioritization Act 에 의해 설립되었다. OSTP 의 책임은 대통령에게 정책 제정에 대한 조언과 과학기술 연구관련 필요한 투자예산 계획하는 것이다. 또 대통령의 사회기술 정책과 프로그램을 설명하고 국가, 주, 지방정부, 산업과 학계에 있는 과학 커뮤니티와의 우호적인 관계를 맺어야 한다. OSTP 이사는 대통령의 과학과 기술 부문 보조로 섬기면서 NSTC 도 관리한다.

Subcommittee on Networking and Information Technology Research Development (NITRD)

NITRD 의 소위원회인 Subcommittee on Networking and Information Technology Research Development 는 NITRD 프로그램으로도 불린다. NSTC 의 Committee on Technology (CoT) 부서에 속해있는 프로그램으로써 NITRD subcommittee 는 다양한 에이전시(agency)를 위한 R&D 프로그램을 계획하여 정보기술에서의 미국 리더십 유지에 기여한다. 예로 네트워킹과 정보기술에 대한 연구개발 계획안을 제안하고, 고도화된 네트워킹과 정보 기술에 대한 미국 정부의 요구를 만족시키고, 네트워킹과 정보기술 개발 및 도입을 가속화하는데 주력한다. 또 High-Performance Computing Act of 1991 과 America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science Act of 2007 (COMPETES) 같이 관련 있는 provision 도 실현한다. (더 자세한 내용은 www.nitrd.gov. 참고)