数据隐私保护体系

1. 数据资源按格式可以分为结构化、半结构化、非结构化数据。
2. 数据按内容敏感程度可以分为公开、半公开和敏感数据，而敏感数据在国家、企业和个人等不同层面又有不同的体现形式。在个人层面，如身份证、手机号、邮政编码等信息都属于隐私数据；对于相同的敏感数据，个人和团体对其可能又有不同的敏感等级划分。
3. 从隐私对抗（）的角度来看，
4. 在隐私数据的发布阶段，需要对敏感数据进行识别和脱敏，如通过自然语言处理技术对文本类的敏感数据进行识别，通过匿名算法等来对要发布的数据进行脱敏；
5. 在数据的存储阶段，
6. 与特定情境相关的隐私数据，比如移动终端产生的位置数据、轨迹数据；
7. 针对社交网络中好友检索服务的隐私保护问题，本文提出一种基于重匿名技术的粒度化好友搜索架构F-Seeker． 对用户发布的位置信息采用增强的 k 匿名策略—( k，m，e) -匿名，用以防止“好奇”的搜索服务提供方对用户隐私的推测． 在处理好友搜索服务过程中，由服务提供方根据粒度化的可视策略对数据实施重匿名， 实现了对用户位置信息粒度化的访问控制． 此外，文中对发布数据采用 Z 序编码并在搜索过程中通过运用剪枝策略提高搜索效率． 实验结果表明，文中提出的匿名策略在保护用户隐私的同时并没有大幅度地增加计算开销．