在2006年，美国在线发布了许多用户查询的搜索引擎。用户名被替换为随机散列，虽然查询文本没有被修改。事实证明，有些用户查询了自己的名字，或“虚荣查询”，以及像当地企业一样的近距离视频聊天。因此，记者采访AOLuser1并不困难，然后从其余的查询中了解到她的个人详细信息（如病史和病史）。美国在线已经通过在搜索查询中放置每个单词来保护所有用户用随机散列？可能不会；Kumar等[27]指出，词语共现模式将提供哪些散列与哪些词相对应的线索，从而允许攻击者部分重构原始查询。这种隐私问题对网络搜索数据并不是特别的。企业，政府机构和研究团体定期收集有关个人的数据，并出于各种原因（如满足法律要求，满足业务义务，鼓励可重复的科学研究）发布某种形式的数据。但是，在原始数据中，他们还必须保护敏感信息，包括身份，个人事实，商业秘密以及其他应用方面的考虑因素。隐私的挑战是敏感信息可以通过多种方式从数据库中获得。荷马等[20]表明，基因组研究的参与者可以从集合研究结果的发表中确定。 Greveleret al.17显示智能电表读数可以用来识别电视节目和正在观看的电影。 Coull等[6]显示，用户查看的网页可以从网络流量的元数据中推断出来，即使服务器的IP地址被替换为假名。Goljanand Fridrich16展示了如何从照片中识别噪点。在2006年，美国在线发布了许多用户查询的搜索引擎。用户名被替换为随机散列，虽然查询文本没有被修改。事实证明，有些用户查询了自己的名字，或“虚荣查询”，以及像当地企业一样的近距离视频聊天。因此，记者采访AOLuser1并不困难，然后从其余的查询中了解到她的个人详细信息（如病史和病史）。美国在线已经通过在搜索查询中放置每个单词来保护所有用户用随机散列？可能不会；Kumar等[27]指出，词语共现模式将提供哪些散列与哪些词相对应的线索，从而允许攻击者部分重构原始查询。这种隐私问题对网络搜索数据并不是特别的。企业，政府机构和研究团体定期收集有关个人的数据，并出于各种原因（如满足法律要求，满足业务义务，鼓励可重复的科学研究）发布某种形式的数据。但是，在原始数据中，他们还必须保护敏感信息，包括身份，个人事实，商业秘密以及其他应用方面的考虑因素。隐私的挑战是敏感信息可以通过多种方式从数据库中获得。荷马等[20]表明，基因组研究的参与者可以从集合研究结果的发表中确定。 Greveleret al.17显示智能电表读数可以用来识别电视节目和正在观看的电影。 Coull等[6]显示，用户查看的网页可以从网络流量的元数据中推断出来，即使服务器的IP地址被替换为假名。 Goljanand Fridrich16展示了如何从照片中识别噪点。

Preparing data for public release requires significant attention to fundamental principles of privacy.

BY ASHWIN MACHANAVAJJHALA AND DANIEL KIFER

Designing Statistical Privacy for Your Data

IN 2006, AOL RELEASED a file containing search queries posed by many of its users. The user names were replaced with random hashes, though the query text was not modified. It turns out some users had queried their own names, or "vanity queries," and nearby locations like local businesses. As a result, it was not difficult for reporters to find and interview an AOL user[1] then learn personal details about her (such as age and medical history) from the rest of her queries.

Could AOL have protected all its users by also replacing each word in the search queries with a random hash? Probably not; Kumar et al.[27] showed that word co-occurrence patterns would provide clues about which hashes correspond to which words, thus allowing an attacker to partially reconstruct the original queries. Such privacy concerns are not unique to Web-search data. Businesses, government agencies, and research groups routinely collect data about individuals and need to release some form of it for a variety of reasons (such as meeting legal requirements, satisfying business obligations, and encouraging reproducible scientific research). However, they must also protect sensitive information, including identities, facts about individuals, trade secrets, and other application-specific considerations, in the raw data. The privacy challenge is that sensitive information can be inferred in many ways from the data releases. Homer et al.[20] showed participants in genomic research studies may be identified from publication of aggregated research results. Greveler et al.[17] showed smart meter readings can be used to identify the TV shows and movies being watched in a target household. Coull et al.[6] showed webpages viewed by users can be deduced from metadata about network flows, even when server IP addresses are replaced with pseudonyms. And Goljan and Fridrich[16] showed how cameras can be identified from noise in the images they produce.

Naive aggregation and perturbation of the raw data often leave exposed channels for making inferences about sensitive information;[6,20,32,35] for instance, simply perturbing energy readings from a smart meter independently does not hide trends in energy use. "Privacy mechanisms," or algorithms that transform the data to ensure privacy, must be designed carefully according to guidelines set by a privacy definition. If a privacy definition is chosen wisely by the data curator, the sensitive information will be protected.

原始数据的天真聚合和扰动通常会使得信息泄露，从而得出关于敏感信息的推论6,20,32,35例如，简单地扰乱来自智能仪表的能量读数并不隐藏能量使用的趋势，“隐私机制”或算法确保隐私的数据必须根据隐私权定义的指导方针仔细设计。 如果数据馆长明智地选择了隐私权，则隐私信息将受到保护。

ed

ice

mization

ntly leak
sensitive information.

- Focusing on privacy design principles can help mitigate this risk.

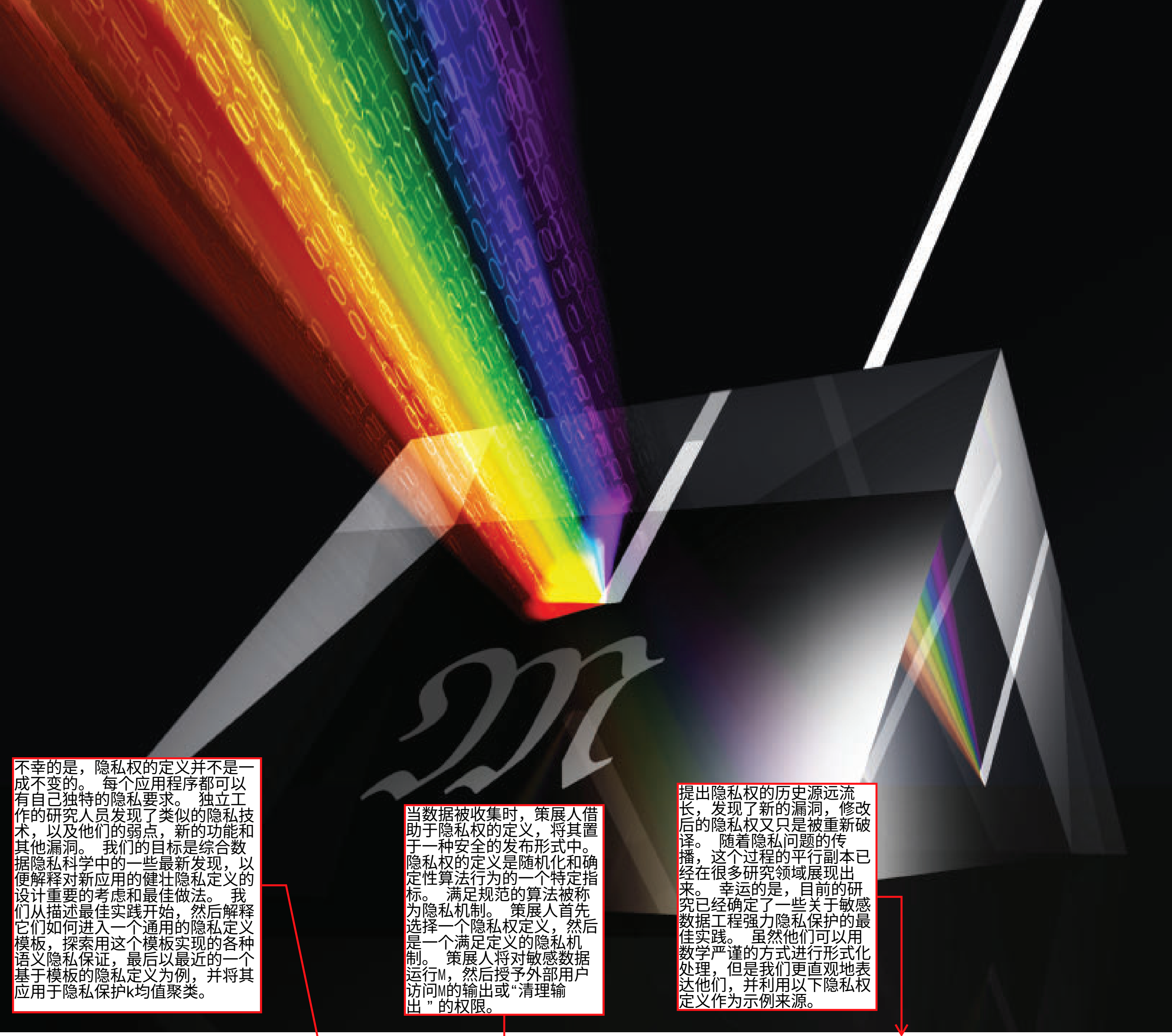

IMAGE BY ANDRIJ BORYS ASSOCIATES/SHUTTERSTOCK

Unfortunately, privacy definitions are not one-size-fits-all. Each application could have its own unique privacy requirements. Working independently, researchers from disparate fields rediscover similar privacy technologies, along with their weaknesses, new fixes, and other vulnerabilities. Our goal here is to synthesize some of the latest findings in the science of data privacy in order to explain considerations and best practices important for the design of robust privacy definitions for new applications. We begin by describing best practices, then explain how they lead to a generic template for privacy definitions, explore various semantic privacy guarantees achievable with this template, and end with an example of a recent privacy definition based on the template and apply it to privacy-preserving k-means clustering.

Desiderata of Privacy Definitions

When data is collected, the curator, with the aid of a privacy definition, puts it in a form that is safe to release. A privacy definition is a specification for the behavior of randomized and deterministic algorithms. Algorithms that satisfy the spec are called privacy mechanisms. The curator first chooses a privacy definition, then a privacy mechanism $\mathfrak{M}$ satisfying the definition. The curator will run $\mathfrak{M}$ on the sensitive data, then grant external users access to the output of $\mathfrak{M}$, or the "sanitized output."

There is a long history of proposed privacy definitions, new vulnerabilities discovered, and amended privacy definitions developed only to be broken once again. As privacy concerns spread, parallel copies of this process are spawned in many research areas. Fortunately, current research has identified many best practices for engineering robust privacy protections for sensitive data. Although they can be formalized in a mathematically rigorous way, we present them at a more intuitive level, leveraging the following privacy definitions as sources of examples.

Definition 1 ($\in$-differential privacy[9,11]). An algorithm $\mathfrak{M}$ satisfies ϵ-differential privacy if for each of its possible outputs ω and for every pair

定义1（∈-差分隐私
9,11）。 如果对于其每个
可能的输出ω和针对每一对
数据库D1，D2的加入或去除
单个记录而不同，则算法M
满足ε-差分保密性。

of databases D_1, D_2 that differ on the addition or removal of a single record, $P(\mathfrak{M}(D_1) = \omega) \leq e^{\epsilon} P(\mathfrak{M}(D_2) = \omega)$.

直观地说，从数据中增加或
删除数据的ε-差分隐私保
证对隐私机制M的输出影响
不大。对于小的ε，这意味
着无论Bob的记录是否在数
据中，M都可能产生相同的
清理输出。

ϵ-differential privacy t adding or removing a e data will have little ef- put of a privacy mecha- mall ϵ, it means $\mathfrak{M}$ will probably produce the same sanitized output regardless of whether or not Bob's record is in the data.

数据馆长应该如何选择ε？
考虑针对个人的高度针对性
的查询（如询问Bob的记录
是否在数据中）。 对于
∈-微分隐私，揭示隐私机
制最容易以概率eε/（1
+eε）回答，错误地以概率
1 /（1 +eε）回答.24当ε
接近0时，这两个概率都是
接近1/2，并且提供的信息
很少 这个机制几乎和真实
的回应一样可能；例如，当
ε= 0.1时，真实答案概率
为≈0.525，当ε= 0.01
时，概率为≈0.502。 我们
建议选择基于馆长希望这个
值与½有多接近

How should a data curator choose ϵ? y targeted query about uch as asking if Bob's data). For ϵ-differen- most revealing privacy swers truthfully with $+ e^{\epsilon})$ and falsely with $+ e^{\epsilon})$.[24] When ϵ is close probabilities are close formation is provided; is almost as likely to ruthfully; for example, when $\epsilon = 0.1$, the true answer probability is ≈ 0.525, and when $\epsilon = 0.01$, the probability is ≈ 0.502. We recommend choosing ϵ based on how close the curator wants this value to be to ½.

The Laplace mechanism is a popular mechanism for ϵ-differential privacy. Let f be a function that computes a vector of query answers on the data. To

拉普拉斯机制是ε-差分隐私机制的一种流行机制。设f是计算数据
查询答案向量的函数。 Toeach查询答案中，拉普拉斯机制增加了
一个独立的拉普拉斯随机变量，其均值为0，标准偏差为S，其中S
（f）是f的全局敏感度 - 由于一个记录的添加或f的最大可能变
化，或者数据库D1， D2在一个记录中不同。 直觉上，噪音掩盖了
任何单个记录对f结果的影响。 现在考虑：

each query answer, the Laplace mechanism adds an independent Laplace random variable with mean 0 and standard deviation $\sqrt{2}S(f)/\epsilon$, where $S(f)$ is the global sensitivity of f– the largest possible change in f due to the addition of one record, or the maximum of $||f(D_1) - f(D_2)||_1$ over pairs of databases D_1, D_2 that differ in one record. Intuitively, the noise masks the influence of any single record on the result of f. Now consider:

定义2（k-匿名.34,35）给
定属性Q，称为准识别符，
一个表是k-匿名的，如果其
中的每条记录与k-1个其他
记录具有相同的准确值。一
个算法满足k- 如果只输出
k-匿名表，则是匿名的。

ymity.[34,35]) Given known as the is k-anonymous the same quasi- 1 other records. An algorithm satisfies k-anonymity if it outputs only k-anonymous tables.

K匿名防御称为“连锁攻
击”的攻击类型 - 加入外
部数据集，该外部数据集将
身份（例如姓名）与准识别
码（例如邮编代码）联系到
包含这个公开可用的准匿名
表 identifer.Its的目标是
防止在k-匿名表中的
anidentity匹配单个元组；
显然，在连接结果中总会击
败至少k个候选者。 匿名机
制通常是通过粗化属性（例
如，从邮政编码中删除数字
并将其变更为年龄范围）来
实现的。 请参见图1，了解
k-匿名表的两个示例。

K-anonymity defends against one type of attack called a "linkage attack"— set that associ- name) with the s ZIP code and able containing quasi-identifier. matching of an in the k-anony- e will always be he join result. K- usually operate (such as dropping digits from ZIP codes and changing ages to age ranges); see Figure 1 for two examples of k-anonymous tables.

Figure 1. Examples of *k*-anonymity: (a) 4-anonymous table; (b) 3-anonymous table.

Zip Code	Age	Disease
130**	25–30	None
130**	25–30	Stroke
130**	25–30	Flu
130**	25–30	Cancer
902**	60–70	Flu
902**	60–70	Stroke
902**	60–70	Flu
902**	60–70	Cancer

(a)

Zip Code	Age	Disease
130**	< 40	Cold
130**	< 40	Stroke
130**	< 40	Rash
1485*	≥ 40	Cancer
1485*	≥ 40	Flu
1485*	≥ 40	Cancer

(b)

Security Without Obscurity

通过隐私机制M清除敏感数
据的过程必须遵循
Kerckhoffs的原则21，并确
保隐私，甚至可以知道M可
能知道细节的攻击者，除了
它可能使用的特定随机比
特。 更好的是，机制M必须
随着消毒输出一起揭示出
来。

The process of sanitizing sensitive data anism $\mathfrak{M}$ must ciple[21] and en- ast adversaries tails of $\mathfrak{M}$, ex- lom bits it may he mechanism $\mathfrak{M}$ must be revealed along with the sanitized output.

众所周知的机制M的原因是
双重的：首先，历史显示
“安全通过安全”在许多应
用中是不可靠的；其次，
Mmust的输出是有用的。 这
种消毒的产出通常采用数据
集或统计模型的形式，可以
用来支持科学研究。 在这
种情况下，统计有效性是一
个重要的考虑因素，只有当
科学家确切地知道什么是转
换被应用到基础敏感数据
时，才能得出统计上有效的
结论。

The reasons for making the mecha- wn are twofold: security through e in many appli- the output of $\mathfrak{M}$ sanitized output a dataset or sta- d be intended to arch. In such a is an important lly valid conclusions can be drawn only when scientists know precisely what transformations were applied to the base sensitive data.

同样，隐私机制设计者应该总是认为攻击者比他
们聪明。只是因为隐私机制的设计者不能从一个
软件的输出中推断出敏感信息，攻击者也将失
败。一个设计良好的隐私定义将会克服这些 不
利于保护敏感信息，防止知道M如何运行的攻击
者。 我们解释如何在后续部分。

Likewise, privacy-mechanism designers should always assume attackers are smarter than they are. Just because the designer of a privacy mechanism cannot deduce sensitive information from the output of a piece of software, an adversary will also fail. A well-engineered privacy definition will overcome these disadvantages, protecting sensitive information from clever attackers who know how $\mathfrak{M}$ operates. We explain how in subsequent sections.

后期处理。 隐私权的定义
决定了数据管理者可以信任
的机制，不泄露敏感信息。
设M是一个这样的机制，假
设A是一个可以用于M的输出
的算法；例如，假设M从其
输入创建合成数据，A构建
决策树。 假设A°M表示首
先将M应用于敏感数据，然
后在M的广义输出上运行A的
复合算法

Post-processing. A privacy definition determines the mechanisms that data curators can sitive informatio mechanism, and algorithm that c output of $\mathfrak{M}$; for creates synthetic and $\mathcal{A}$ builds a notation $\mathcal{A} \circ \mathfrak{M}$ denote the composite algorithm that first applies $\mathfrak{M}$ to the sensitive data and then runs $\mathcal{A}$ on the sanitized output of $\mathfrak{M}$.

如果M是可信的，那么这个
复合算法A°M也是可信的
吗？ 直觉上，答案是肯定
的。 如果一个数据管理者
发布隐私保护合成数据，但
声称从这些数据构建统计模
型，这是非常奇怪的，这是
对隐私的侵犯。

If $\mathfrak{M}$ is trusted, should this composite algorith ? Intuitively, th d be very strang ased privacy-pre but then claim odels from this data is a violation of privacy.

如果A°M满足M规定的隐私
权限制约束，则隐私权定义
在后续处理中关闭。 微分
隐私11满足这个性质，但是
k-匿名性不是.23后置处理
的封闭性有两个重要的后
果：一是保证了隐私权和科
克霍夫原理之间的兼容性。
例如，一些满足k-匿名性的
算法容易受到所谓的最小化
攻击[13，36]。对于每一种
k-匿名机制M，都有可能制
定一个后处理算法A，它取
出M的输出，撤销一些数据
转换， 输出一个新的具有
可能唯一的准确识别值的数
据集，这些数据很容易受到
外部数据的联合攻击。 也
就是说，复合算法A°M不满
足与M或k-匿名相同的条
件，并且常常揭示敏感记录

A privacy definition is closed under post-processing if $\mathcal{A} \circ \mathfrak{M}$ satisfies the constraints defining the privacy definition whenever $\mathfrak{M}$ does. Differential privacy[11] satisfies this property, but k-anonymity does not.[23] Closure under post por- tant conse ures compatibil defi- nition and for example, s tisfy k-anonymi so- called min each such k-an $\mathfrak{M}$, it is possible sing algorithm t of $\mathfrak{M}$, undoes sfor- mations, a aset having rec que quasi-iden ner- able to lin rnal data. That is, the composite algorithm $\mathcal{A} \circ \mathfrak{M}$ does not satisfy the same conditions as $\mathfrak{M}$, or k-anonymity, and often reveals sensitive records.

By contrast, suppose an ϵ-differentially private algorithm $\mathfrak{M}$ is applied to the

相反，假设一个ε-差分私有算法M被应用于数据D，并且结果M（D）被发布。 在给定M的知识的情况下，信息交换者可以设计一个攻击算法A，并在已发布的数据上运行它以获得结果A（M（D））。注意A（M（D））是应用组合算法A°M 对于数据D，由于在后处理过程中ε-差分隐私被封闭，复合算法A°M仍然满足ε-差分隐私，因此具有相同的语义；A°M的输出几乎不受数据库中Bob（或任何其他人）记录的存在或不存在的影响。

lished. Given knowledge of $\mathfrak{M}$, a clever adversary can design an attack algorithm $\mathcal{A}$ and run it on the published data to obtain the result $\mathcal{A}(\mathfrak{M}(D))$. Note $\mathcal{A}(\mathfrak{M}(D))$ is the result of applying the composite algorithm $\mathcal{A} \circ \mathfrak{M}$ to the data D. Since ϵ-differential privacy is closed under post-processing, the composite algorithm $\mathcal{A} \circ \mathfrak{M}$ still satisfies ϵ-differential privacy and hence has the same semantics; the output of $\mathcal{A} \circ \mathfrak{M}$ is barely affected by the presence or absence of Bob's (or any other individual's) record in the database.

The second important consequence of closure under post-processing is how a data curator must express privacy definitions. Consider k-anonymity and ϵ-differential privacy. By analogy to database-query languages, the defi nition of k-anonymity is declarative that is, it specifies what we want fron the output but not how to produce thi output. On the other hand, differen tial privacy is more procedural, speci fying constraints on the input/out put behaviors of algorithms througl constraints on probabilities (such a $P(\mathfrak{M}(D) = \omega)$). This is no coincidence in order to achieve closure under post processing, it is necessary that the privacy definition impose conditions on the probabilities (even when $\mathfrak{M}$ is deterministic) rather than on the syntactic form of the outputs.[22]

在后处理过程中，第二个重要的结果就是数据管理者必须表达隐私权。 考虑k-匿名和ε-差别隐私。 通过类比数据库查询语言，k-匿名的定义是声明式的;也就是说，它指定了我们从输出中得到的东西，而不是如何产生这个输出。 另一方面，差分隐私更为程序化，通过约束概率（例如P（M（D）=ω））来规定算法的输入/输出行为的约束。 这并非巧合，为了在后处理过程中实现封闭，隐私定义必须对概率（甚至当M是确定的时候）而不是产出的语法形式施加条件。

Composition. We introduce the concept of composition with an example. Suppose the 4-anonymous table in Figure 1 was generated from data from Hospital A, while the 3-anonymous table in Figure 1 was generated by Hospital B. Suppose Alice knows her neighbor Bob was treated by both hospitals for the same condition. What can Alice infer about, say, Bob's private records? Bob corresponds to an anonymized record in each table. By matching ZIP code, age, and disease, Alice can deduce that Bob must have had a stroke. Each anonymized table individually might have afforded Bob some privacy, but the combination of the two tables together resulted in a privacy breach. The degradation in privacy that results from combining multiple sanitized outputs is known as "composition."[14]

组成。 我们以一个例子来介绍作文的概念。 假设图1中的4匿名表是从医院A的数据中产生的，而图1中的3匿名表是由B医院产生的。假设爱丽丝知道她的邻居鲍勃在两家医院中都处于相同的状况。 Aliceinfer可以说Bob的私人记录是什么？Bob对应于每个表中的匿名记录。 通过匹配邮编，年龄和疾病，爱丽丝可以推断出鲍勃肯定有中风。单独的匿名表可能会给鲍勃一些隐私，但是这两张表的结合导致了隐私泄露。 多种消毒的产品被称为"成分"

Self-composition. "Self-composition" refers to the scenario where the sanitized outputs are all produced

The privacy challenge is that sensitive information can be inferred in many ways from the data releases.

自组成。 "自我组合"是指所有的产出都是由隐私机制产生的，并且都符合相同的隐私定义。 关于隐私定义能否承受构图的基本限制是由Dinur和Nissim7的结果启发的一个越来越大的文献的一部分，它显示当n个log（n）2统计查询被回答时，大小为n的数据库中的绝大多数记录可以被重构，甚至如果eachanswer被任意改变到o（n）错误；也就是说，一个小于查询答案的自然变化的变形，即对手将从一个更大的人群中收集一个样本。

from privacy mechanisms that satisfy the same privacy definition. Fundamental limits on a privacy definition's ability to withstand composition are part of a growing literature inspired by the results of Dinur and Nissim[7] who showed that the vast majority of records in a database of size n can be reconstructed when $n \log(n)^2$ statistical queries are answered, even if each answer has been arbitrarily altered to have up to $o(\sqrt{n})$ error; that is, a distortion that is less than the natural variation of query answers that an adversary would get from collecting a sample of size n from a much larger population.

尽管这样的负面结果限制了可以安全地查询私有数据库的次数，但是隐私保护的优化性降低了，例如ε-差别隐私。 如果M1，M2，...，Mkare算法使得每个Mi满足εi-微分隐私，那么它们的敏感输出的组合满足ε-微分隐私，ε=ε+ ... +ε；更正式地，这个隐私级别通过算法M 在输入数据上运行机制M1，M2，...，Mk并释放其所有输出。 因此，最终的结果并不确定任何记录，同时仍然满足差异性隐私，但是在隐私参数中具有线性降级

espite such negative results that t the number of times a private base can be queried safely, there be a graceful degradation of pri protections, as in the case of ferential privacy. If $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_k$ algorithms such that each $\mathfrak{M}_i$ sat s ϵ_i-differential privacy, then the bination of their sensitive out satisfies ϵ-differential privacy $\epsilon = \epsilon + \ldots + \epsilon$;[30] more formally, privacy level is achieved by the algorithm $\mathfrak{M}$ running mechanisms $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_k$ on the input data and releases all their outputs. The end result thus does not reveal any record deterministically while still satisfying differential privacy but with a linear degradation in the privacy parameter.

Self-composition has another prac enefit—simplifying the design cy-preserving algorithms. Com l mechanisms can be built rly from simpler mechanisms ame way software is built from ns. By controlling the informa kage of each component indi , a privacy-mechanism design control the information leakage of the entire system. In the case of ϵ-differential privacy, the privacy parameter ϵ of the final mechanism is at most the sum of the privacy parameters of its components.[4,30]

自组合有另一个实际的好处 - 简化隐私保护算法的设计。 复杂的机制可以从更简单的机制模块化构建，就像软件构建的功能一样。 隐私机制设计者通过单独控制每个组件的信息泄露，可以控制整个系统的信息泄露。 在ε-差分隐私的情况下，最终机制的隐私参数ε最多是其组成部分的隐私参数之和。

Composition with other mechanisms. The data curator must also consider the effect on privacy when the mechanisms do not satisfy the same privacy definition. As an example,[24,26] consider a database where each record takes one of k values. Let $x_1, x_2, \ldots, x_k$ denote the number of times each of these values appears in the database; they are histogram counts. Let $\mathfrak{M}_1$ be

其他机制构成。当机制不能满足同一个隐私定义时，数据馆长还必须考虑到隐私的影响。 作为一个例子，24,26考虑一个数据库，其中每个记录都有一个k值。 令x1，x2，...，xk表示每个值出现在数据库中的次数;它们是直方图计数。 设M1是释放和x1 + x2，x2 + x3，...，xk-1 + xk的机制。 注意M1不满足ε-差分隐私。 此外，任何一个计数的知识，结合M1的输出，将显示所有的原始计数。现在考虑一个机制M2，可以从拉普拉斯分布中提取噪声，方差2 / ε2独立于每个直方图计数，so 输出由k个噪声计数x1，...，x2组成。 机制M2确实满足ε差别隐私；9它是前面提到的拉普拉斯机制。

$+ x_2, x_2 + x_3, \ldots, x_{k-1} + x_k$. Note $\mathfrak{M}_1$ does not satisfy ϵ-differential privacy. Moreover, the knowledge of any one count x_i, combined with the output of $\mathfrak{M}_1$, would reveal all the original counts. Now consider a mechanism $\mathfrak{M}_2$ that adds noise drawn from a Laplace distribution, with variance $2/\epsilon^2$, independently, to each histogram count, so its output consists of k noisy counts $\tilde{x}_1, \ldots, \tilde{x}_2$. Mechanism $\mathfrak{M}_2$ does satisfy ϵ-differential privacy;[9] it is the Laplace mechanism mentioned earlier.

What is the effect of the combined release of the sanitized outputs of $\mathfrak{M}_1$ and $\mathfrak{M}_2$? From $\tilde{x}_1$, we have a noisy estimate of x_1. From the quantity $x_1 + x_2$ and the noisy value $\tilde{x}_2$, we can obtain another independent estimate of x_1. Combining $x_1 + x_2$, $x_2 + x_3$, and $\tilde{x}_3$ we get yet another estimate. Overall, there are k independent noisy estimates of x_1 that can be averaged together to get a final estimate with variance $2/(k\epsilon^2)$, which is k times lower than what we could get from $\mathfrak{M}_2$ alone. This example illustrates why there is a recent push for creating flexible privacy definitions that can account for prior releases of information (such as the output of $\mathfrak{M}_1$) to control the overall inference.[2,15,25]

M1和M2消毒产品的联合销售的效果如何？ 从x1，我们有一个嘈杂的估计x1。 从数量x1 + x2和噪声值x2可以得到x1的另一个独立估计。结合x1 + x2，x2 + x3和x3可以得到另一个估计。总的来说，对于x1的k个独立噪声估计值，可以用方差2 /（kε2）进行平均估计，这比我们从M2单独得到的要低k倍。 这个例子说明了为什么最近有推动创造灵活的隐私定义，可以解释信息的先前发布（如M1的输出）来控制整体推论.2,15,25

Convexity. Consider a privacy definition satisfied by two mechanisms, $\mathfrak{M}_1$ and $\mathfrak{M}_2$. We can create an algorithm $\mathfrak{M}^{(p)}$, or their "convex combination," that randomly chooses among them; with probability p it applies $\mathfrak{M}_1$ to its input and with probability $1-p$ it applies $\mathfrak{M}_2$. Why consider mechanisms like $\mathfrak{M}^{(p)}$? Convex combinations like $\mathfrak{M}^{(p)}$ could provide better worst-case error guarantees for some queries than either $\mathfrak{M}_1$ or $\mathfrak{M}_2$ for reasons similar to why mixed strategies may be preferred over pure strategies in game theory.

Now, should we trust $\mathfrak{M}^{(p)}$ to protect privacy? It is reasonable to do so because the only thing $\mathfrak{M}^{(p)}$ does is add additional randomness into the system.[22,23] We say a privacy definition is convex if every convex combination of its mechanisms also happens to satisfy that privacy definition. Convex privacy definitions have useful semantic properties we discuss in more detail in the next section.

凸。 考虑由两种机制M1和M2满足的隐私定义。 我们可以创建一个算法M（p），或者它们的“凸组合”，它们随机地在它们之间选择；以概率p将M1应用于其输入，并且以概率1-p应用M2。 为什么考虑像M（p）这样的机制？ 像M（p）这样的凸组合可以为某些查询提供更好的最坏情况下的错误保证，因为类似于混合策略的原因，M1或M2可能更适合于纯粹的博弈策略。现在，我们是否应该相信M（p）来保护隐私？ 这样做是合理的，因为M（p）所做的唯一事情就是增加对系统的随机性。[22,23]如果机制的每个凸组合都满足隐私定义，我们说隐私定义是凸的。 凸隐私定义具有有用的语义属性，我们将在下一节详细讨论

Minimizing probabilistic failure. Consider a private record that can be expressed in one bit; that is, 1 if Bob has cancer and 0 otherwise. We add noise from a standard Gaussian distribution and release the result, which happens to be 10. If Bob's bit is 1, then we are 13,000 times more likely to observe a noisy value of 10 than if Bob's bit is 0. We have thus almost certainly discovered the value of Bob's bit.

One can argue that observing a noisy value this large is so unlikely (regardless of the value of Bob's bit) that such a privacy breach is very rare and hence can be ignored. Such reasoning has led to relaxations of privacy definitions that allow guarantees to fail with a small probability δ.; one example is the relaxation (ϵ, δ)-differential privacy, which can produce more accurate data-mining results.

最大限度地减少概率失败。考虑一下可以表达的私人记录;也就是说，如果Bob患有癌症，则为1，否则为0。我们从标准高斯分布中addnoise和释放的结果，whichhappens为10。如果Bob的位是1，thenwe 13000倍更有可能观察到的10嘈杂的值比如果Bob'sbit为0。我们现在几乎certainlydiscovered的鲍勃的价值。
人们可以争辩说，观察这个大的嘈杂值是不太可能的（不管鲍勃的价值是多少），隐私泄露非常罕见，因此可以忽略。这种推理导致了隐私定义的放松，使得保证以小的概率δ失败。一个例子是松弛（ε，δ） - 微分隐私，可以产生更准确的数据挖掘结果

Definition 3 (ϵ, δ)-differential privacy.[10,11] Let $\mathfrak{M}$ be an algorithm and

定义3（ε，δ） - 微分隐私。假设M是一个算法，S是它的可能输出集合。如果对所有子集B∈S和所有的数据库对D1满足（ε，δ） - 微分隐私，D2在单个记录的价值上不同，
是否总是提供保证或允许隐私保护以小概率失败的决定是特定于应用程序的并且取决于所涉及的风险。这是一个隐私/效用权衡，具有不同程度的微妙的后果。例如，设M是以概率1-δ输出⊥的算法。并以概率δ输出输入数据集。这个M满足（ε，δ） - 差分隐私的更高的条件。同样，考虑一个算法M *，它从输入数据集中返回随机选择的个体的记录。如果记录的数量是N，并且如果N> 1 / δ，那么M *满足（ε，δ） - 差别隐私但总是侵犯了某些个人的隐私
值得注意的是，ε-差异隐私和宽松（ε，δ）差异隐私都提供了相同的高层次保证 - 一个机制的输出分布几乎不受任何个体记录的影响。不过，隐私放松可能会持续侵犯隐私权，而前者则不会。对攻击者的推理可以帮助数据管理者设置限制这种信息泄漏的参数值14（正如我们后面讨论的）为可实现的保证提供了新的视角。

is that ϵ-differential privacy and the relaxed (ϵ, δ)-differential privacy both offer the same high-level guarantee—the output distribution of a mechanism is barely affected by the value of any individual record. Still, privacy relaxation may consistently cause privacy violations, while the former will not. Reasoning about attackers can help data curators set parameter values that limit such information leakages[14] and (as we discuss later) provide new perspectives on achievable guarantees.

执行问题。就安全性方面而言，从理论到实践都需要非常小心。特别是，即使算法在理论上被证明能够满足所选择的隐私定义的要求，隐私保护算法的幼稚实现也不能保证隐私。一个问题来自旁道。考虑一个对敏感数据库进行处理的程序，其运行方式如下：如果Bob的记录在数据库中，则在一天之后产生输出1；如果Bob的记录不在数据库中，则立即输出1，输出是一样的，不管数据库是什么。但是通过观察结果输出的时间，我们了解一下数据库。
当理论算法将其安全特性建立在可能超出数字计算机极限的精确计算基础上时，另一个问题就出现了。最常见的例子是来自连续分布（如高斯和拉普拉斯）的噪声。对于大多数浮点实现，对位模式的分析会得到关于输入数据的附加信息
最后，许多隐私机制在随机数发生器上。必须保证隐私保护算法的安全实现必须适应比特随机性的质量。

concerns. As with
urity, moving from
requires great care.
ve implementation
ing algorithm may
even though the al-
ally proven to satis-
of a chosen privacy
oblem arises from
nsider a program
sitive database and
If Bob's record is in
duces the output 1
b's record is not in
tputs 1 right away.
me, no matter what
t by observing the
time taken for a result to be output, we learn something about the database.[18]

Another concern arises when the theoretical algorithms base their security properties on exact computation that may be beyond the limits of digital computers.[5,31] The most common example is the addition of noise from continuous distributions (such as Gaussian and Laplace). For most floating-point implementations, an analysis of the bit patterns yields additional information about the input data.[31]

Finally, many privacy mechanisms rely on a random number generator. A provably secure implementation of a privacy-preserving algorithm must be tailored to the quality of the randomness of the bits.[8]

A Generic Recipe

Privacy definitions tha
closed under post-proc

通用食谱隐性定义是凸的，在后处理过程中是封闭的，并且要求保护机制M的所有输出都具有相似的格式，并且可以用线性约束来表示，如下面的通用模板所示：定义4（通用的隐私定义）。设D1，D2，...是可能的输入数据集的集合。对于一些固定的常量，算法M必须满足以下条件，以便可以产生算法ω的每个可能的输出为了评估提出的隐私定义，对当前最佳实践的良好的合理性检查因此是验证算法M是否可以表示为线性约束算法的概率行为，如定义4；例如k-匿名不适用于该模板，但是对于ε-差分隐私，对于每一对数据集Dj1，存在线性约束P（M（Dj1）=ω）-e∈P（M（Dj2）=ω） Dj2在一个记录中存在差异。接下来我们讨论通过这个模板实现的一些语义保证。

for a
have
itten
as in
eneric
the co
s. For
$_2^{(1)}, S_2^{(2}$
ust sat
every p
h proc
$\sum_j S$
opose
nition, a good sanity ch
best practices is thus to

or not the algorithm $\mathfrak{M}$ can be expressed as linear constraints on the probabilistic behavior of algorithms, as in Definition 4; for example, k-anonymity does not fit this template,[28] but with ϵ-differential privacy, there is a linear constraint $P(\mathfrak{M}(D_{j1}) = \omega) - e^{\epsilon}P(\mathfrak{M}(D_{j2}) = \omega) \leq 0$ for every pair of datasets D_{j1}, D_{j2} that differ on the presence of one rec-ord. We next discuss some semantic guarantees achievable through this template.

Good and bad disclosures. Even when published data allows an analyst

好的和坏的披露。即使公布的数据允许分析师对Bob进行更好的推断，Bob的隐私也不一定会被这些数据所破坏。考虑Bob'snosy，但不知情的邻居查理，谁知道鲍勃是一个终生的链式吸毒者，并认为癌症是不相关的吸烟。从吸烟研究中看到的数据后，查理学习吸烟导致癌症，现在相信鲍勃很可能受到伤害。这个推论可能被认为是良性的（或不可避免的），因为它是基于自然的事实。
现在考虑鲍勃参与上述吸烟研究的一个更加细微的情况，数据被M处理，并且结果ω（表示吸烟导致癌症）被发布。查理对鲍勃的信仰可能由于两个因素的结合而改变：通过学习吸烟导致癌症，因为鲍勃的记录可能影响了算法的输出。后一因素提出了隐私风险。有两种方法可以分离和衡量Charley的信念转换是否是由Bob的记录引起的，而不是由于他对自然界的某些法律知识的"了解"，"反事实"[12,25,33]和"模拟性"。

es about Bob,
ecessarily been
Consider Bob's
neighbor Char-
life-long chain-
er is unrelated
g data from a
learns smok-
now believes
to suffer from
be considered
) because it is
e.
nuanced situ-
cipates in the
ng study, the
and the result
moking causes
harley's beliefs
as a result of
factors: by him
causes cancer,
may have af-
output of the algorithm.
factor poses the privacy
are two approaches to iso-
easure whether Charley's
lief is due to Bob's record
to his knowledge of some
e—"counterfactuals"[12,25,33]
tability."[2,15,29]

隐私通过反事实。基于反事实推理的方法12,25,33的根源在于学习人数据库底层的真实分布是可以接受的，但是学习一个特定的个人数据如何偏离这种分布是隐私违反。
考虑一些备选方案（比如"鲍勃有癌症"和"鲍勃不健康"）。如果真实的数据生成分布θ已知，我们可以通过考虑概率Pθ（M个输出ω| Bob具有癌症）和Pθ（M个输出）来理解每个替代方案如何影响M的输出（考虑到数据的不确定性） ω|鲍勃是健康的）。它们的比率被称为"比值比"。它是将具有癌症的鲍勃（在观看ω之前）的初始几率转换为更新后的赔率（乘以ω）的乘法因子。当比值比接近1时，赔率几乎没有变化，鲍勃的隐私得到保护。
为什么这个工作？如果推理是用真实的分布来完成的话，那么由于自然法则的学习，我们已经绕过了信仰的变化。在看到ω之后，Charley信念的变化仅仅取决于Bob受Bob影响的程度（比如它是用Bob的记录计算的）。
如果真实的分布是未知的呢？为了处理这种情况，数据馆长可以指定一组合理的分布，并确保推理任何一个是无害的；相应的优势比都接近1.因此，对于所有可能的ω，基于反事实的隐私定义将强制执行像Pθ（M个输出ω| Bob具有癌症）≤e∈Pθ（M个输出ω| Bob是健康的）的约束，对于各种替代和分布对θ。当从书面的角度来看，这些条件转化为线性约束，如在通用模板（定义4）中

counterfactuals. The first
33 based on counterfactu-
is rooted in the idea that
true distribution underly-
te database is acceptable,
how a specific individual's
from this distribution is a
h.
pairs of alternatives
b has cancer" and "Bob is
the true data-generating
θ is known, we could use
and how each alternative
utput of $\mathfrak{M}$ (taking into ac-
tainty about the data) by

considering the probabilities $P_\theta(\mathfrak{M}$ outputs ω | Bob has cancer) and $P_\theta(\mathfrak{M}$ outputs ω | Bob is healthy). Their ratio is known as the "odds ratio." It is the multiplicative factor that converts the initial odds of Bob having cancer (before seeing ω) into the updated odds (after seeing ω). When the odds ratio is close to 1, there is little change in the odds, and Bob's privacy is protected.

Why does this work? If the reasoning is done using the true distribution, then we have bypassed the change in beliefs due to learning about laws of nature. After seeing ω, the change in Charley's beliefs depends only on the extent to which ω is influenced by Bob (such as it was computed using Bob's record).

What if the true distribution is unknown? To handle this scenario, the data curator can specify a set Ξ of plausible distributions and ensure reasoning with any of them is harmless; the corresponding odds ratios are all close to 1. A counterfactual-based privacy definition would thus enforce constraints like $P_\theta(\mathfrak{M}$ outputs ω | Bob has cancer) $\leq e^{\epsilon}P_\theta(\mathfrak{M}$ outputs ω | Bob is healthy) for all possible ω, for various pairs of alternatives and distributions θ. When written mathematically, these conditions turn into linear constraints, as in the generic template (Definition 4).

Privacy via simulatability. The second approach,[2,15,29] based on simulat-

隐私通过模拟。第二种方法2,15,29基于模拟性，主要是由于关于大量人口的学习统计是可以接受的，但是学习一个人如何与人口不同是隐私违约。主要思想是比较一个算法M，输入D到另一个算法，通常被称为"模拟器"，S具有更安全的输入D'；例如，D'可以是通过从D移除Bob的记录而获得的数据集。如果M和S的输出分布相似那么攻击者对于是通过运行D上的M还是通过D上的S来产生ω是根本不能为力的。现在S不知道Bob的记录，除了它可以从D'的其余部分（例如吸烟和癌症之间的联系）预测的东西。鲍勃的纪录是受保护的。同样，爱丽丝的隐私可以通过考虑爱丽丝的记录被删除而不是鲍勃的记录的不同变化来测试。如果S能够近似地模拟M的行为，不管是否有任何改变，那么每个单独的记录都被保护
基于可模拟性的隐私定义通常比基于反事实的隐私定义要复杂得多。为了检查M是否满足定义，通常需要找到合适的模拟器S.然而，在某些情况下，隐私定义也可以使用线性约束来表示，如通用隐私定义模板。

he idea that
large popu-
eptable, but
differs from
acy breach.
pare the be-
with input
often called
fer input D';
dataset that
Bob's record
of outputs of
an attacker
ut whether ω
$\mathfrak{M}$ on D or by
es not know
cord except
e rest of the
ink between
's record is
Alice's pri-
sidering dif-
lice's record
's record. If

反事实与模拟。反制和模拟方法之间的差异取决于必须保护的数据的性质。当数据记录彼此独立时，数据生成分布的属性和总体属性基本相同（由于大数定律），在这种情况下，两种方法都提供了类似的保护。

数据相关性。当个体之间存在相关性时会产生差异。首先，我们认为一个情景会更适合。假设一个数据库包含有关鲍勃及其亲属的记录。即使鲍勃的记录被删除，鲍勃的各种疾病的易感性可以从其余的数据预测，因为它包含他的家庭的医疗历史。基于可模拟性的隐私定义的总体目标不是要隐藏这个推断，而是要隐藏Bob的实际记录与这个预测的差距。另一方面，如果我们包括疾病如何通过遗传学的概率模型，那么基于反事实的隐私权定义将会试图阻止对Bob和他的家族的预测。直觉上，这是因为实际的家庭病史不是数据生成分布的属性，而是来自该分布的样本。由于家庭医学史与鲍勃的记录相关，因此可以更好地预测鲍勃如何偏离数据生成分布；因此，它也必须得到保护。

接下来，我们研究基于模拟隐私权的情况更为合适。考虑到许多个人公开的社交网络。关于个人的私人信息往往是直接从他们的朋友和联系人的公共部门预测的.37即使鲍勃的私人信息是私人的，也很容易收集与鲍勃相关的信息。在这里，基于模拟性的隐私定义是适用的，允许数据管理者用算法Mthat处理社交网络数据，从而创建输出，从而很难判断Bob的记录是否用于计算。

$\mathcal{S}$ can a
havior
data D i
was pe
record i
Priva
latabilit
than th
To chec
nitions,
the app
in som
can also
straints
nition t
Cou
The diff
and sim
on the
protecte
indepen
of the d
propert
ly the sa
bers), i
provide similar protection.

Data correlations. A difference arises when there is correlation between individuals. First, we consider a scenario when counterfactuals would be more appropriate. Suppose a database contains records about Bob and his relatives. Even if Bob's record is removed, Bob's susceptibility to various diseases can be predicted from the rest of the data because it contains his family's medical history. The general goal of privacy definitions based on simulatability is not to hide this inference but to hide how Bob's actual record differs from this prediction. On the other hand, if we include probabilistic models of how diseases are passed through genetics, then privacy definitions based on counterfactuals will try to prevent predictions about Bob and his family. Intuitively, this happens because the actual family medical history is not a property of the data-generating distribution but of a sample from that distribution. Since the family medical history is correlated with Bob's record, it would allow better predictions about how Bob deviates from the data-generating distribution; hence, it must be protected as well.

Next, we examine a situation where simulatability-based privacy definitions are more appropriate. Consider a social network where many profiles

对差别隐私的解释。这两种为隐私定义定义语义的方法也提供了两种解释ε-差别隐私的方法。模拟性论证显示，满足ε-差分隐私的算法提供了以下保护：攻击者无法检测M是在原始数据上运行，还是在任何给定记录被删除的情况下改变了数据。[14]无论攻击者有多么深入的知识，只要数据转换与数据已知的一致；如果不是这样，则可能发生额外的泄漏，正如前面关于与其他机制组合的讨论中所解释的。从不同的角度来看，反事实假设表明，一个满足ε-差分隐私的算法M可以防止攻击者在所有记录都是独立的情况下精确地学习一个人如何与数据生成分配不同。

of indi vate in-
format s often
predict public
profiles ntacts.[37]
Even if t is easy
to colle orrelat-
ed with initions
based o plicable,
allowin ess the
social r thms $\mathfrak{M}$
that cre it is difficult to tell if Bob's record was used in the computation.

Data constraints. One difficulty in designing privacy definitions is ac-

数据限制。一个不同的隐私权定义是说明输入数据库必须满足的公共知识约束。约束条件可能会使不同记录的值相关联，例如，由于属性之间的函数依赖关系或直方图的先前准确版本而产生的值。由约束产生的相关性提供了推理渠道攻击者可以用来学习敏感信息。因此，隐私权必须解释它们。例如，虽然人口普查数据记录必须以保密方式处理，但某些粗略的人口统计数据必须准确发布，以确定每个州的国会代表人数。更一般地说，如果数据的直方图H被精确地释放，那么adata馆长如何选择隐私定义，并且因此对M中的信息进行约束，以便通过M的后续数据发布能够确保隐私？完整的解决方案如果我们使用以直方图为条件的数据生成分布，或者P（D | H），那么问题是开放的，但似乎更容易基于反事实。[25]对于基于模拟的方法，还有更多的挑战，因为数据变更技术与以前发布的信息必须发展；回想一下，它们提供了一个保证，攻击者不能可靠地确定原始数据集或改变的数据集是否被用于计算。同样重要的是要注意，对输入数据的约束，特别是对以前的版本的约束，可以被利用来获得更好的效用。

co nowledge of
co tabase must
sa correlate the
va ords, arising
du ependencies
ac exact releas-
es tions arising
fr le inference
ch use to learn
se privacy defi-
ni for them; for
ex data records
m tially, certain
co ics must, by
la order to de-
te ongressional
Re state. More
ge H of the data
ha y, how can a
da rivacy defini-
ti nts on $\mathfrak{M}$ to
ac ation in the
hi uent data re-
le sure privacy?
Co his problem
ar be easier for
approaches based on counterfactuals if we use data-generating distributions that are conditioned on the histogram, or $P(D|H)$.[25] For approaches based on simulatability, there is more of a challenge since data-alteration techniques consistent with previously released information must be developed; recall, they provide the guarantee that an attacker would not be able to reliably determine whether the original dataset or altered dataset was used in the computation. It is important to note, too, that constraints on the input data, and especially those arising from prior releases, can be exploited for better utility.

Interpretations of differential privacy. These two approaches for defining semantics for privacy definitions also provide two ways of interpreting ϵ-differential privacy. The simulatability argument shows an algorithm satisfying ϵ-differential privacy provides the following protection: an attacker cannot detect whether $\mathfrak{M}$ was run on the original data or on altered data from which any given record was removed.[2,14] This is true no matter how knowledgeable the attacker is, as long as the data alteration is consistent with what is known about the data; if not, additional leakage can occur, as explained in the earlier discussion on composition with other mechanisms. From a different perspective, the counterfactual argument shows an algorithm $\mathfrak{M}$ satisfying ϵ-differential privacy prevents an attacker from learning how an individual differs from the data-generating distribution precisely when all records are independent.[25]

Example: Blowfish

We illustrate this discussion with Blowfish,[19] a new class of privacy defi-

例子：Blowfish我们用Blowfish来说明这个讨论，19这是隐含定义的一个新类，它遵循定义4中的通用隐私模板。与差分隐私一样，Blowfish定义满足了我们前面概述的许多理想的属性，包括Kerckhoffs的原理，自组合，凸性和关闭后处理。 Blowfishdefnitions的隐私目标既有反面意义也有模拟性解释。除了满足这些性质外，Blowfish定义通过包含数据中个体的私有属性的一般化和形式化指定以及通过记录关于数据中的约束的前外部知识来改善差别隐私。因此Blowfish捕获隐私设计空间的一部分。在本节中，我们将介绍数据所有者如何使用Blowfish来为应用程序定制隐私保护。

Blowfish定义有两个参数：隐私ε（类似于差别隐私）和策略P =（T，G，IQ），允许数据管理者定制隐私保证。在这里，T是可能的记录值集合，Q是数据上一组公开的约束，IQ是与Q一致的所有可能数据集的集合。指定IQ允许数据管理者创建可以与先前的确定性数据发布组合的隐私定义，从而避免了在前面部分讨论的一些困难。为了简化讨论，我们将Q设置为数据集有n条记录的单个约束，其中IQ = T n;有关更复杂的约束，请参阅Hew19关于Blowfish和Kifer以及Pufferfsh框架上的Machanavajjhala25。

generic privacy
. Like differen-
efinitions sat-
ble properties
luding Kerck-
f-composition,
nder post-pro-
als of Blowfish
counterfactual
erpretation. In
ese properties,
nprove on dif-
uding a gener-
ication of what
ual in the data
accounting for
ut constraints
thus captures
n space. In the
describe how
owfish to cus-
ions for their
take two pa-
nilar to differ-
y $P = (\mathcal{T}, \mathcal{G}, \mathcal{I}_{\mathcal{Q}})$
to customize
e, $\mathcal{T}$ is the set
es, $\mathcal{Q}$ is a set of publicly known constraints on the data, and $\mathcal{I}_{\mathcal{Q}}$ is the set of all possible datasets consistent with $\mathcal{Q}$. Specifying $\mathcal{I}_{\mathcal{Q}}$ allows a data curator to create

privacy definitions that can compose with prior deterministic data releases, thus avoiding some of the difficulties discussed earlier in the section on desiderata. To simplify the discussion, we set $\mathcal{Q}$ to be the single constraint that the dataset has n records, in which case $\mathcal{I}_{\mathcal{Q}} = \mathcal{T}^n$; for more complicated constraints, see He[19] on Blowfish and Kifer and Machanavajjhala[25] on Pufferfish frameworks.

The final component of the policy is $G = (\mathcal{T}, E)$, or the "discriminative secret graph." The vertices in G are the possible values a record can take. Every edge $(x, y) \in E$ describes a privacy goal with both counterfactual and simulatability interpretations. From the simulatability viewpoint, changing a single record from x to y (or vice versa) will not cause a significant change in the probability of any output. From the counterfactual viewpoint, if records are independent, an attacker could estimate the odds of a new record having value x vs. y, but estimated odds about any individual in the data would not differ significantly from this value. Using this graph G, we define the concept of neighboring databases, then formally define the Blowfish framework:

Definition 5 (G-Neighbors). Let $P = (\mathcal{T}, G, \mathcal{T}^n)$ be a discriminative secret graph. Two datasets $D_1, D_2 \in \mathcal{T}^n$ are called G-neighbors if for some edge $(x, y) \in E$ and some dataset $D \in \mathcal{T}^{n-1}$, $D_1 = D \cup \{x\}$ and $D_2 = D \cup \{y\}$.

Definition 6 ((ϵ, P)-Blowfish Privacy). Let $P = (\mathcal{T}, G, \mathcal{T}^n)$ be a policy. An algorithm $\mathfrak{M}$ satisfies (ϵ, P)-Blowfish privacy if for all outputs ω of the algorithm $\mathfrak{M}$ and all G-neighbors D_1, D_2 we have $P(\mathfrak{M}(D_1)=\omega) \le e^{\lfloor d(x,y)/10 \rfloor \epsilon} P(\mathfrak{M}(D_2)=\omega)$.

This privacy definition clearly matches the generic template of Definition 4. We now examine some policies and their applications.

Full domain. Consider a policy $P_K = (\mathcal{T}, G, \mathcal{T}^n)$ where K is a complete graph, and every pair of values in the domain $\mathcal{T}$ are connected. The result is that two datasets are neighbors if they differ (arbitrarily) in any one record. (ϵ, P_K)-Blowfish privacy is equivalent to a popular variant of differential privacy[11] that requires $P(\mathfrak{M}(D_1)=\omega) \le e^{\lfloor d(x,y)/10 \rfloor \epsilon} P(\mathfrak{M}(D_2)=\omega)$ for all ω and for all pairs of datasets D_1, D_2 that differ (arbitrarily) in the value (rather than presence/absence) of one record.

Partitioned. Let us partition the do-

政策的最重要组成部分是G =（T，E）或“有区别的秘密报告 ”。G中的顶点是记录可能的值。Everyedge（x，y）∈E描述了具有反事实和模拟性解释的隐私目标。从模拟的角度来看，将单个记录从x更改为y（反之亦然）不会导致任何输出的概率发生显着变化。从事实上的观点来看，如果记录是独立的，那么攻击者可以估计一个具有x和y值的新记录的几率，但是估计数据中有关个体的几率不会大于这个值。使用这个图G，我们定义了相邻数据库的概念，然后正式定义Blowfsh框架：

定义5（G-邻居）。设P =（T，G，T n）是一个有区别的秘密报文。如果对于某个边（x，y）∈E和某个数据集D∈T n-1，D1 =D∪{x}和D2 =D∪{y}，则两个数据集D1，D2∈Tn称为G-邻居。 6（（ε，P）-Blowfsh隐私）。让P =（T，G，T n）为一个策略。算法M满足（ε，P）-Blowfsh隐私，如果算法M的所有输出ω和所有G邻居D1，D2我们有。这个隐私定义明确地匹配定义4的通用模板。现在我们研究一些策略及其应用。

完整的域名。考虑一个策略PK =（T，G，T n）其中K是一个完整的图，并且域T中的每一对值都是连接的。结果是两个数据集是相邻的（如果它们在任何一条记录中是不同的）。（ε，PK）-Blowfshprivacy相当于一个流行的微分隐私变体11，它需要所有ω和所有对数据集D1，D2在一个记录的值（而不是存在/不存在）中不同（任意）

分区。让我们将域T划分为p个互斥子集，其中P = {P1，...，Pp}。考虑图形GP =（T，E），其中任何两个值x，y通过边连接，如果只有x和y出现在相同的分区中，则为唯一。因此，GP的每个连通分量都是对应于Pi中的一个的集合。现在，如果通过用属于相同分区的新值替换一个记录的值，可以从D1获得D2，则两个数据集D1和D2是相邻的。例如，将所有疾病结果分成三组，分别为健康状况，传染性疾病和非传染性疾病。在我们的Blowfsh策略中，我们使用图GP相应的划分。一个满足定义6的算法M带有保证，如果一个传染病被另一个传染病或另一个健康病例替代，或者模仿性解释。

那么用传染病取代非传染性疾病呢？在这种情况下，算法的输出概率是否会显着不同？答案是肯定的。实际上，这个策略允许算法公布每种疾病的每个个体健康，传染性或非接触性和近似性的准确状态。但是，具体细节（如哪个人有哪些传染性疾病）受到保护。这种行为在某些保健应用中可能是理想的，其中必须披露一些事实，但是进一步的细节保持保密

距离阈值。许多应用程序涉及记录之间的距离的概念;例如，两个年龄值之间的距离可以是绝对差值，并且平面上的两点之间的距离可以是直线欧氏距离或曼哈顿距离的一个网格。给定一个距离度量d，可以定义一个有区别的秘密图Gd，θ，其中只有附近的点连通。也就是说，对于某个阈值q，只有当d（x，y）<0时，（x，y）∈E;例如，如果T是地球上所有点的集合，且d是点对之间的正整数距离， θ = 10英里，所以有效的记录位置连接到彼此相距10英里以内的其他有效记录位置。一般来说，如果个人的位置x（在数据集D1中）被改变到另一个点y（导致相邻的数据集D2），那么用此策略满足Blowfsh的算法将保证所有的输出ωAn对手可以检测到一般地理一个目标个体的区域，但不能通过一个分辨率不到10英里的位置。处理位置数据时，这种宽松的隐私概念是合理的;个人可能不希望披露他们的确切位置，但不太担心以粗糙的粒度（可能从其他来源获得）披露他们的信息。正如我们后面所显示的那样，与使用满足差别隐私的严格性的机制产生的数据相比，通过机制的数据输出满足放松的隐私概念允许数据挖掘结果的准确性更高。

main $\mathcal{T}$ into p mutually exclusive subsets, with $\mathcal{P} = \{P_1, \ldots, P_p\}$. Consider a graph $G^{\mathcal{P}} = (\mathcal{T}, E)$, where any two values x, y are connected by an edge if and only if x and y appear in the same partition. Each connected component of $G^{\mathcal{P}}$ is thus a clique corresponding to one of the P_i. Now, two datasets D_1 and D_2 are neighbors if D_2 can be obtained from D_1 by replacing the value of one record with a new value belonging to the same partition. For example, let $\mathcal{T}$ be the set of all disease outcomes, partitioned into three subsets: healthy cases, communicable diseases, and non-communicable diseases. Let us use the graph $G^{\mathcal{P}}$ corresponding to this partition in our Blowfish policy. An algorithm $\mathfrak{M}$ satisfying Definition 6 comes with the guarantee that the probabilities of its outputs do not change substantially if one communicable disease is replaced with another communicable disease or a healthy case with another healthy case, or a simulatability interpretation.

What about replacing a noncommunicable disease with a communicable disease? Can the algorithm's output probabilities be significantly different in such a case? The answer is yes. In fact, this policy allows algorithms to publish the exact status of each individual—healthy, contagious, or noncontagious—and approximate histograms of each disease. However, specific details (such as which person has which contagious disease) are protected. Such behavior may be desirable in certain health-care applications where some facts must be disclosed but further details kept confidential.

Distance threshold. Many applications involve a concept of distance between records; for instance, the distance between two age values can be the absolute difference, and the distance between two points on a plane can be the straightline Euclidean distance or the Manhattan distance along a grid. Given a distance metric d, one can define a discriminative secret graph $G^{d,\theta}$ in which only nearby points are connected. That is, $(x, y) \in E$ only when $d(x, y) < 0$ for some threshold q; for example, if $\mathcal{T}$ is the set of all points on Earth, and d is the orthodromic distance between pairs of points, we can set θ = 10 miles, so valid record locations are connected to other valid record locations that are within 10 miles of each other. In general, if an individual's location x (in dataset D_1) was changed to another point y (resulting in a neighboring dataset D_2), then an algorithm satisfying Blowfish with this policy will have the guarantee that for all outputs ω

$$P(\mathfrak{M}(D_1)=\omega) \le e^{\lfloor d(x,y)/10 \rfloor \epsilon} P(\mathfrak{M}(D_2)=\omega)$$

An adversary may thus be able to detect the general geographic region of a target individual but unable to infer the location with a resolution better than 10 miles. Such a relaxed notion of privacy is reasonable when dealing with location data; individuals may not want disclosure of their precise locations but be less worried about disclosing their information at a coarser granularity (that may be obtained from other sources). As we show later, data output by mechanisms that satisfy such relaxed notions of privacy permit data mining results with greater accuracy than if data is generated using mechanisms that satisfy the stricter notion of differential privacy.

Attribute. Let $\mathcal{T}$ be a multi-attribute domain with m attributes $\mathcal{T} = A_1 \times A_2 \times \ldots, \times A_m$. Consider a graph $G^{attr,c}$ connecting any two values x and y that differ in at most c attribute values. A Blowfish policy with this graph is useful for location traces and genome data. For the former, attributes correspond to locations of an individual at different times. Neighboring datasets thus differ in at most c locations of a person, hiding the specific details about every sequence of c consecutive locations of an individual. In the genome case, an attribute corresponds to a specific position on the genome. Under this policy, an algorithm's output would be insensitive to changes to a block of up to c positions on the genome.

Answering queries with Blowfish. Recall that adding Laplace noise with 0 mean and $\sqrt{2}S(f)/\epsilon$ standard deviation to a function f (where $S(f)$ is the sensitivity of f) ensures ϵ-differential privacy. Blowfish, with a policy $P = (\mathcal{T}, G, \mathcal{T}^n)$ is also compatible with additive Laplace noise and requires an often smaller standard deviation of $\sqrt{2}S(f,G)/\epsilon$ where $S(f, G)$ is the policy-specific global sensitivity of f—the largest difference $||f(D_1)-f(D_2)||_1$ over all datasets D_1, D_2 that are G-neighbors.

Consider a multidimensional record domain $\mathcal{T} = A_1 \times A_2 \times \ldots, \times A_m$ where each attribute is numeric. Let q_{sum} denote the function that sums all the records together; that is, for each attribute, it computes the sum of the values that appear in the data. Let a_i and b_i denote the maximum and minimum values in attribute A_i. The global sensitivity $S(q_{sum})$ of q_{sum} is $\sum_{i=1}^{m} \max\{|a_i|, |b_i|\}$. The policy-specific global sensitivity of q_{sum} under Blowfish policies is usually much smaller. In the case of the distance threshold policy $G^{d,\theta}$ with d being the L_1 Manhattan distance, $S(q_{sum}, G^{d,\theta})$ is only θ. Consider a single attribute domain Age and further suppose the age values range from 0 to 100. The global sensitivity of q_{sum} is 100. The policy-specific sensitivity of q_{sum} under $G^{L_1,5}$ is only 5. If, instead, the policy used a partition graph $G^{\mathcal{P}}$ that partitions age into ranges (such as $\{0-10, 11-20, 21-30, \ldots, 91-100\}$), then the policy-specific global sensitivity is only 10. Finally, with the attribute policy, $S(q_{sum}, G^{attr,1}) = \max_i(a_i - b_i)$.

***K*-means clustering.** For a specific data-mining result, consider an application of Blowfish to k-means clustering.

Definition 7 (K-means clustering). Given a set of n vectors $\{x_1, \ldots, x_n\}$, the k-means clustering problem is to divide these n records among k clusters $S = \{S_1, \ldots, S_k\}$, where $k \le n$, so as to minimize the objective function

$$\sum_{i=1}^{k} \sum_{\mathbf{x}_j \in S_i} ||\mathbf{x}_j - \mu_i||_2^2, \qquad (1)$$

where $\mu_i = \frac{1}{|S_i|} \sum_{\mathbf{x}_j \in S_i} \mathbf{x}_j$ is the mean of cluster S_i.

The iterative (non-private) k-means clustering algorithm initializes a set of k centroids $\{\mu_1, \mu_2, \ldots, \mu_k\}$, one for each cluster. These centroids are iteratively updated in two steps: assign each x_j to the cluster with the nearest centroid, and set each centroid μ_i to be the mean of the vectors of its corresponding cluster. The algorithm terminates after a certain number of iterations or when the centroids do not change significantly.

Each iteration (the two steps) are easily modified to satisfy ϵ-differential privacy[4,30] and Blowfish.[19] These steps require access to the answers to two queries: q_{hist}, which returns the number of points in each cluster, and q_{sum}, or the sum of the points in each cluster. As discussed earlier, q_{sum} can be answered through the Laplace mechanism. Analogously, q_{hist} can be answered with the Laplace mechanism because it has global sensitivity $S(q_{hist}) = 1$ (for differential privacy) and policy-specific global sensitivity $S(f, G) = 2$ for all Blowfish policies discussed here. The policy-specific sensitivity of the q_{sum} query under Blowfish policies is typically much smaller than its global sensitivity so we would thus expect more accurate clustering under the Blowfish privacy definitions.

Figure 2 confirms this improvement in utility. For the clustering task,

Figure 2. *K*-means under several Blowfish policies.

属性。设T是一个具有m个属性的多属性域，T = A1×A2×...， ×Am。考虑一个图Gattr，c连接任何两个值x和y，它们的大部分c属性值不同。这个图的Blowfshpolicy是有用的位置跟踪和基因组数据。对于前者，属性在不同的时间对应于个人的对抗。因此，相邻数据集在人的至多c个位置差异很大，隐藏关于个体的c个连续位置的每个序列的特定细节。在基因组情况下，属性对应于基因组上的特定位置。在这个策略下，一个算法的输出将不会对基因组上的多达c个位置的变化产生影响回答带有Blowfish的查询。回想一下，将具有0平均值和标准偏差的拉普拉斯噪声加到函数f（其中S（f）是f的灵敏度），确保ε-差分隐私。使用策略P =（T，G，T n ）也与加性拉普拉斯噪声兼容，并且要求S（f，G）通常小标准偏差是f的政策特定的全局敏感性 - 作为G邻域的所有数据集D1，D2的最大差异。

考虑一个多维记录域T = A1×A2×...， ×每个属性都是数字的。设qsum表示将所有的索引相加的函数;也就是说，对于每个属性，它计算出现在数据中的值的总和。令ai和bi表示属性Ai中的最大值和最小值。 qsum的全局敏感度S（qsum）是.Blowfsh策略下qsum的策略特定的全局敏感度通常较小。在距离阈值策略Gd的情况下，其中d是L1曼哈顿距离，S（qsum，Gd， θ）仅为θ。考虑单个属性域Age，并进一步假设年龄值的范围是0到100.qsum的全局敏感度是100. GL1,5下qsum的policspecifc敏感度只有5。如果相反，如果使用隔开图GP分割时间（qsum，Gattr，1）= 1，...， （10） maxi（ai - bi）。

K均值聚类。定义7（K均值聚类）给定一个n向量{x1，...，xn}的集合，k均值聚类问题是将这些集合分解n个记录在k个簇S = {S1，...，Sk}中，其中k≤n，以使目标函数最小化（1）其中，是簇Si迭代（非私有）k-均值聚类算法初始化一个集群k个质心{μ1，μ2，...，μk}。这些质心迭代地分两步更新：将xj分配到具有最接近的中心点的聚类，并且将每个质心μi设置为其相应聚类的向量的均值。该算法在经过一定次数或质心不明显改变之后终止

每个迭代（两个步骤）都很容易被修改，以满足ε-differentialprivacy4,30和Blowfsh.19这些步骤需要访问两个查询的答案：qhist，它返回每个集群中的点数，qsum或点的总和在每个群集中。正如前面所讨论的，qsum可以通过拉普拉斯机制来答复。类似地，qhist可以用拉普拉斯机制来回答，因为它具有全局敏感度S（qhist）= 1（用于差分隐私）和policyspecifc全局敏感度S（f，G）= 2这里讨论的所有Blowfsh策略。在Blowfsh策略下的查询通常比它的全局敏感性要小得多，所以我们期望在Blowfsh隐私方面更精确的聚类。

we used a small sample of the skin-segmentation dataset,[3] or 1%, which is approximately 2,500 instances, in order to make the problem challenging. Each instance corresponds to the RGB intensities from face images, and each intensity ranges from 0 to 255. The *x*-axis is the privacy parameter ϵ, and on the *y*-axis (note the log scale) we report the error incurred by the privacy-preserving algorithms. We measure the error as the ratio between the squared error (Equation 1) attained by the privacy-preserving algorithms to that achieved by the non-private *k*-means algorithm after 10 iterations that was sufficient for the convergence of the non-private algorithm. The Laplace mechanism for ϵ-differential privacy incurred the most error. Using the $G^{attr,1}$ policy already reduces the error by at least a factor of 1.5. The error is further reduced when using $G^{L_1,\theta}$, for $\theta \in \{256, 128, 64, 32\}$. It is interesting to note the error does not increase monotonically as we increase $\theta - G^{L_1,128}$—an improvement of 3x and 2x over differential privacy for $\epsilon \leq 0.5$ and $\epsilon > 0.5$, respectively. One explanation is that small amounts of error can help avoid local minima while clustering.

Conclusion

Privacy definitions are formal specifications an algorithm must satisfy to protect sensitive information within data. Our experience shows that designing robust privacy definitions often requires a great deal of subtlety. Our goal is to present some of the major considerations in this design process, along with example privacy definitions and resulting privacy mechanisms. We hope this discussion inspires additional curiosity about the technical nature of privacy.

Acknowledgment

This work is supported by the National Science Foundation under Grants 1054389 and 1253327.

图2显示了这种效用的改善。对于聚类任务，我们使用了皮肤分割数据集的一个小样本，3或1%，大约2,500个实例，以使问题具有挑战性。每个实例对应于来自面部图像的RGB强度，并且每个强度范围从0到255 x轴是隐私参数ε，在它们的轴上（注意对数尺度），我们报告了隐私保护算法引起的误差。我们测量隐私保留算法得到的平方误差（方程1）与非私有k均值算法经过10次迭代得到的误差之间的比率的误差，这对非私有算法的收敛是足够的。 ε-差分隐私的Laplace机制引发了mosterror。使用Gattr，1策略已经将错误减少了至少1.5倍。当对于θ∈{256,128,64,32}使用GL1，θ时，误差进一步减小。值得注意的是，误差并没有单调递增，因为我们增加了θ-GL1128-对于ε≤0.5和ε> 0.5，分别改善了3x和2xover差分隐私。一种解释是，在集群时，少量的错误可以帮助避免局部最小值。

结论隐私权定义是一种算法必须满足的条件，用数据来保护敏感信息。我们的经验表明，设计健壮的隐私权定义往往需要大量的细微之处。我们的目标是提出一些在这个设计过程中的主要考虑因素，以及示例隐私权的定义和产生的隐私机制。 Wehope这个讨论激发了对隐私技术性质的另外的好奇心

致谢这项工作得到了美国国家科学基金会（National Science Foundation）的资助（Grant）10554389和1253327的支持

References

1. Barbaro, M. and Zeller, T. A face is exposed for AOL searcher no. 4417749. *The New York Times* (Aug. 9, 2006).
2. Bassily, R., Groce, A., Katz, J., and Smith, A. Coupled-worlds privacy: Exploiting adversarial uncertainty in statistical data privacy. In *Proceedings of the 54th IEEE Annual Symposium on Foundations of Computer Science* (Berkeley, CA, Oct. 27–29). IEEE Computer Society Press, Washington, D.C., 2013, 439–448.
3. Bhatt, R. and Dhall, A. *Skin Segmentation Dataset.* Machine Learning Repository Center for Machine Learning and Intelligent Systems, University of

Languages and Programming (Venice, Italy, July 9–16). Springer-Verlag, Berlin, Heidelberg, 2006, 1–12.

10. Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., and Naor, M. Our data, ourselves: Privacy via distributed noise generation. In *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Saint Petersburg, Russia, May 28–June 1). Springer-Verlag, Berlin, Heidelberg, 2006, 486–503.
11. Dwork, C., McSherry, F., Nissim, K., and Smith, A. Calibrating noise to sensitivity in private data analysis. In *Proceedings of the Theory of Cryptography Conference* (Columbia University, New York, Mar. 4–7). Springer-Verlag, Berlin, Heidelberg, 2006, 265–284.
12. Evfimievski, A., Gehrke, J., and Srikant, R. Limiting privacy breaches in privacy-preserving data mining. In *Proceedings of the 22nd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems* (San Diego, CA, June 9–12). ACM Press, New York, 2003, 211–222.
13. Fang, C. and Chang, E.-C. Information leakage in optimal anonymized and diversified data. In *Proceedings of the 10th Information Hiding* (Santa Barbara, CA, May 19–21). Springer-Verlag, Berlin, Heidelberg, 2008, 30–44.
14. Ganta, S.R., Kasiviswanathan, S.P., and Smith, A. Composition attacks and auxiliary information in data privacy. In *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (Las Vegas, Aug. 24–27). ACM Press, New York, 2008, 265–273.
15. Gehrke, J., Lui, E., and Pass, R. Towards privacy for social networks: A zero-knowledge-based definition of privacy. In *Proceedings of the Theory of Cryptography Conference* (Providence, RI, Mar. 28–30). Springer-Verlag, Berlin, Heidelberg, 2011, .432-449.
16. Goljan, M. and Fridrich, J. Camera identification from scaled and cropped images. In *Proceedings of Electronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents* (Feb. 26, 2008); http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=812538
17. Greveler, U., Justus, B., and Loehr, D. Forensic content detection through power consumption. In *Proceedings of the IEEE International Conference on Communications* (Ottawa, Canada, June 10–15). IEEE Press, Psicataway, NJ, 2012, 6759–6763.
18. Haeberlen, A., Pierce, B.C., and Narayan, A. Differential privacy under fire. In *Proceedings of the 20th USENIX Conference on Security* (San Francisco, CA, Aug. 8–12). USENIX Association, Berkeley, CA, 2011, 33–33.
19. He, X., Machanavajjhala, A., and Ding, B. Blowfish privacy: Tuning privacy-utility trade-offs using policies. In *Proceedings of the ACM SIGMOD/PODS International Conference on Management of Data* (Snowbird, UT, June 22–27). ACM Press, New York, 2014, 1447–1458.
20. Homer, N., Szelinger, S., Redman, M., Duggan, D., Tembe, W., Muehling, J., Pearson, J.V., Stephan, D.A., Nelson, S.F., and Craig, D.W. Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density snp genotyping microarrays. *PLoS Genetics 4*, 8 (Aug. 2008).
21. Kerckhoffs, A. La cryptographie militaire. *Journal des Sciences Militaires 9* (Jan. 1983), 5–83.
22. Kifer, D. and Lin, B.-R. Towards an axiomatization of statistical privacy and utility. In *Proceedings of the 29th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems* (Indianapolis, IN, June 6–11). ACM Press, New York, 2010, 147–158.
23. Kifer, D. and Lin, B.-R. An axiomatic view of statistical privacy and utility. *Journal of Privacy and Confidentiality 4*, 1 (2012), 5–49.
24. Kifer, D. and Machanavajjhala, A. No free lunch in data privacy. In *Proceeding of the ACM SIGMOD/PODS International Conference on Management of Data* (Athens, Greece, June 12–16). ACM Press, New York, 2011, 193–204.
25. Kifer, D. and Machanavajjhala, A. A rigorous and customizable framework for privacy. In *Proceedings of the 31st Symposium on Principles of Database Systems* (Scottsdale, AZ, May 20–24). ACM Press, New York, 2012, 77–88.
26. Kifer, D. and Machanavajjhala, A. Pufferfish: A framework for mathematical privacy definitions. In *Transactions on Database Systems 39*, 1 (Jan. 2014), 3:1–3:36.
27. Kumar, R. Novak, J., Pang, B., and Tomkins, A. On anonymizing query logs via token-based hashing. In *Proceedings of the 16th International World Wide Web Conference* (Banff, Alberta, Canada, May 8–12). ACM Press, New York, 2007, 629–638.
28. Lin, B.-R. and Kifer, D. Towards a systematic analysis of privacy definitions. *Journal of Privacy and Confidentiality 5*, 2 (2014), 57–109.
29. Machanavajjhala, A., Gehrke, J., and M. Götz. Data publishing against realistic adversaries. In *Proceedings of the 35th International Conference on Very Large Data Bases* (Lyon, France, Aug. 24–28, 2009), 790–801.
30. McSherry, F.D. Privacy integrated queries: An extensible platform for privacy-preserving data analysis. In *Proceedings of ACM SIGMOD/PODS International Conference on Management of Data* (Providence, RI, June 29–July 2). ACM Press, New York, 2009, 19–30.
31. Mironov, I. On significance of the least significant bits for differential privacy. In *Proceedings of the 19th ACM Conference on Computer and Communications Security* (Raleigh, NC, Oct. 16–18). ACM Press, New York, 2012, 650–661.
32. Narayanan, A. and Shmatikov, V. Robust de-anonymization of large sparse datasets. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy* (Oakland, CA). IEEE Computer Society Press, Washington, D.C., 2008, 111–125.
33. Rastogi, V., Hay, M., Miklau, G., and Suciu, D. Relationship privacy: Output perturbation for queries with joins. In *Proceedings of the 28th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems* (Providence, RI, June 29–July 2). ACM Press, New York, 2009, 107–116.
34. Samarati, P. Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering 13*, 6 (Nov. 2001), 1010–1027.
35. Sweeney, L. *K*-anonymity: A model for protecting privacy. *International Journal of Uncertainty Fuzziness and Knowledge-Based Systems 10*, 5 (Oct. 2002), 557–570.
36. Wong, R., Fu, A., Wang, K., and Pei, J. Minimality attack in privacy-preserving data publishing. In *Proceedings of the 33rd International Conference on Very Large Data Bases* (University of Vienna, Austria, Sept. 23–27). VLDB Endowment, 2007, 543–554.
37. Zheleva, E. and Getoor, L. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th International World Wide Web Conference* (Madrid, Spain, Apr. 20–24). ACM Press, New York, 2009, 531–540.

Ashwin Machanavajjhala (ashwin@cs.duke.edu) is an assistant professor in the Department of Computer Science at Duke University, Durham, NC.

Daniel Kifer (dkifer@cse.psu.edu) is an associate professor in the Department of Computer Science & Engineering at Penn State University, University Park, PA.