

Flexible Privacy via Disguising and Revealing

by

Lillian Tsai

A.B., Harvard University (2017)
S.M., Harvard University (2017)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2024

© Massachusetts Institute of Technology 2024. All rights reserved.

Author
Department of Electrical Engineering and Computer Science
May 3, 2024

Certified by
M. Frans Kaashoek
Charles Piper Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Co-Certified by
Malte Schwarzkopf
Professor of Computer Science, Brown University
Thesis Co-Supervisor

Accepted by
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

Flexible Privacy via Disguising and Revealing

by

Lillian Tsai

Submitted to the Department of Electrical Engineering and Computer Science
on May 3, 2024, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

Many users today have tens to hundreds of accounts with web services that store sensitive data, from social media to tax preparation and e-commerce sites [12, 28, 65]. While users have the right to delete their data (via e.g., the GDPR [27] or CCPA [11]), users want and deserve more nuanced controls over their data that don't exist today. For example, a user might wish to hide and protect data of an e-commerce or dating app profile when inactive, but also want their data to be present should they return to use the application. Today, however, services often provide only coarse-grained, blunt tools that result in all-or-nothing exposure of users' private information.

This thesis introduces the notion of *disguised data*, a reversible state of data in which sensitive data is selectively hidden. To demonstrate the feasibility of disguised data, this thesis also presents Edna—the first system for disguised data—which helps database-backed web applications allow users to remove their data without permanently losing their accounts, anonymize their old data, and selectively dissociate personal data from public profiles. Edna helps developers support these features while maintaining application functionality and referential integrity via *disguising* and *revealing* transformations. Disguising selectively renders user data inaccessible via encryption, and revealing enables the user to restore their data to the application. Edna's techniques allow transformations to compose in any order, e.g., deleting a previously anonymized user's account, or restoring an account back to an anonymized state. With Edna, web applications can enable flexible privacy features with reasonable developer effort (<1k LoC for a 160k real web application) and moderate performance impact on application operation throughput (1–7% in the common case, and up to 28% in the worst case).

This thesis and Edna thus demonstrate that with disguised data, applications can support flexible privacy features beyond what they offer users today. [lyt: I want to end with something a bit more summary, but not sure this is the right way?]

Thesis Supervisor: M. Frans Kaashoek

Title: Charles Piper Professor of Electrical Engineering and Computer Science

Thesis Co-Supervisor: Malte Schwarzkopf

Title: Professor of Computer Science, Brown University

Acknowledgments

Better acks

This thesis is based off prior work on Edna, published at SOSP 2023 [69]. I am immensely grateful to my collaborators on Edna over the many years: Hannah Gross, Eddie Kohler, Malte Schwarzkopf, and Frans Kaashoek. Without you all, Edna would not exist today. I would also like to thank Akshay Narayan, Anish Athalye, Aurojit Panda, Derek Leung, Gohar Irfan Chaudhry, Henry Corrigan-Gibbs, James Mickens, Kevin Liao, Kinan Dak Albab, Matthew Lentz, Nick Young, Nickolai Zeldovich, MIT’s PDOS group, Brown’s ETOS group, the SystemsResearch@Google Team, and all our anonymous reviewers: you generously donated your time and insights that greatly improved Edna.

While working on Edna, I am grateful to have had the support of an NSF Graduate Research Fellowship. CloudLab [26] also provided essential resources to develop the Edna prototype and evaluate its artifact. Work on Edna was also supported by NSF awards CNS-2045170 and CSR-1704376, a Google Research Scholar award, and funding from VMware.

But Edna and this thesis would not have been possible without the many people who stood by my side (and, in some cases, gave me much-needed nudges) throughout the past six-plus years.

Contents

1	Introduction	15
1.1	Motivation	15
1.2	Disguised Data: A New Abstraction for Flexible Privacy	16
1.3	Challenges	16
1.4	Our Approach	17
1.5	Contributions	18
2	Related Work	21
2.1	Compliance Tools	21
2.2	Policy Enforcement Systems	21
2.3	Encrypted Storage Systems	22
2.4	Other Related Work	22
3	Overview	25
3.1	Example: Lobsters Topic Anonymization	26
3.2	Disguise Specifications	27
3.3	User Reveal Credentials	28
3.4	Database Management Operations	29
3.5	Guarantees and Threat Model	30
4	Edna’s Design	31
4.1	Disguising	31
4.2	Revealing	33
4.3	Database Management Operations	34
4.3.1	Application Updates.	34
4.3.2	Schema Migrations	37
4.3.3	Consistency Checks for Internal Invariants	38
4.4	Shared Data	38
4.5	Composing Disguising Transformations	42
4.6	Authenticating As Pseudoprincipals	44
4.7	Design Limitations	45

4.8	Security Discussion	46
5	Implementation	49
5.1	Secure Record Storage	49
5.2	Reveal Credentials	49
5.3	Application Updates Replay Log	50
5.4	Batching	50
5.5	Concurrency	50
6	Case Studies	51
6.1	Lobsters	51
6.2	WebSubmit	52
6.3	HotCRP	52
7	Evaluation	55
7.1	Edna Developer Effort	55
7.2	Performance of Edna Operations	56
7.2.1	Edna Performance Drill-Down	58
7.2.2	Composing Disguising Transformations.	59
7.3	Edna Overheads	60
7.3.1	Space Used By Edna.	60
7.3.2	Impact On Concurrent Application Use.	60
7.4	Comparison to Qapla	62
7.5	Edna+CryptDB	63
7.6	Database Management Operations	65
7.6.1	Supporting Updates	65
7.6.2	Performance of Reveals with Updates	67
7.7	Summary	68
8	Conclusion	69
8.1	Deploying Disguised Data	69
8.2	Disguising Beyond Edna: Flexible Access Control	70
8.3	Final Thoughts	71

List of Figures

3-1	Developers write disguise specifications and add hooks to invoke Edna from the application (green); in normal operation, clients use these hooks in the application to disguise and reveal their data in the database (blue).	25
3-2	Lobsters topic-based anonymization disguise specification (JSON pseudocode), which decorrelates comments and removes votes on stories with the specific topic tag.	26
3-3	The Lobsters developer adds a hook in the UI and code to perform topic-based anonymization.	26
3-4	Lobsters topic-based anonymization disguise specification (JSON pseudocode), which decorrelates comments and removes votes on stories with the specific topic tag.	27
4-1	When Edna applies topic-based anonymization to Bea’s comments on stories tagged “Star Wars” (red), these comments are decorrelated to pseudoprincipals (“Anon-Pig”, “AnonFox”). Edna stores encrypted speaks-for records mapping Bea to their pseudoprincipals, and diff records containing the comments with modified foreign keys.	32
4-2	Pseudocode for revealing a disguising transformation while application principal uid exists. Recursive revealing (the else clause) walks the speaks-for chain to reveal composed records of pseudoprincipals created by other disguising transformations if necessary (§4.5).	33
4-3	When the application applies updates like moderations of explicit words, it can invoke Edna to log the update. Edna then applies the update to disguised data in diff records prior to reveal. Yellow highlights changes to the application data or Edna’s data.	35
4-4	Similar to a moderations update, the application can notify Edna of a schema migration to apply to diff records prior to reveal. Yellow highlights changes to the application data or Edna’s data. For simplicity, only the placeholder data of a pseudoprincipal row is shown; in reality, placeholder data exists as part of e.g., a decorrelation diff record.	36

4-5	Edna supports joint ownership semantics, where shared data is not removed until all users have disguised their accounts. Owners can return in any order, and the message remains decorrelated from unrevealed owners.	39
4-6	Edna implements joint ownership semantics by storing a fully decorrelated REMOVE diff for the shared data (modifications to the shared message data are depicted using [owner→pseudoprincipal] notation). Owners can only see pseudoprincipals for the other owners in their disguised data. This allows Edna to disguise and reveal in any order.	41
4-7	Edna allows multiple decorrelations to compose, and can reveal them in any order such that the data remains decorrelated until the user reveals <i>all</i> applied decorrelations. The speaks-for chain encoded in speaks-for records (shown in blue) allows Edna to handle recorrelation of intermediate pseudoprincipals. When Bea requests reveal of their “Star Wars” posts (4) after revealing “bears” posts (3), Edna walks the speaks-for chain backwards from P_2 to find the latest principal that can speak-for P_2 and has not yet been recorrelated. Thus, Edna restores ownership back to Bea.	43
7-1	Edna adds no latency overhead to common application operations and modestly increases the latencies of disguising operations compared to a manual implementation that lacks support for revealing or composition. Bars show medians, error bars are 5 th /95 th percentile latencies.	57
7-2	Applying disguising transformations to previously-decorrelated accounts increases latency linear in the number of pseudoprincipals involved. Hatched lines indicate the proportion of cost attributed to cryptographic operations.	59
7-3	Continuous disguising/revealing operations in Lobsters have <7% impact on application request throughput when disguising a random user; an extreme case of a heavy-hitter user with lots of data repeatedly disguising and revealing causes up to 8% drop in throughput without transactions, and up to 28.3% drop in throughput with transactions.	61
7-4	Edna achieves competitive performance with a manual baseline and outperforms Qapla on nearly all common WebSubmit operations (2k users, 80 answers/user). Bars show medians, error bars are 5 th /95 th percentile latencies.	63
7-5	Latencies of WebSubmit (2k users, 80 answers/user) operations when implemented with Edna+CryptDB (adding encrypted database support). Bars show median latency; error bars are 5 th /95 th percentile latencies.	64
7-6	Schema migrations that affect entire tables require writing separate update function for Edna. Applying these updates adds greater overheads per story than per user or per other table row, as more updates apply to the stories table.	65

7-7	Out of the most recent 20 Lobsters database management operations, the majority (75%) are table operations which require developers to write separate update specifications for Edna, 15% are row operations which can be reused as updates without additional effort, and 10% are unsupported because they denormalize the schema in order to cache aggregate results.	66
7-8	Schema migrations that affect entire tables require writing separate update function for Edna. Applying these updates adds greater overheads per story than per user or per other table row, as more updates apply to the stories table.	66

List of TODOs

1. (§0.0) Better acks	5
2. (§1.0) more tools? account deactivation?	15
3. (§2.0) evidence	21
4. (§3.4) do we still need to say why this is a challenge?	29
5. (§5.0) table with components and loc	49
6. (§7.0) Update with numbers from Google Cloud	55
7. (§7.0) Fix figures	55
8. (§7.7) check	68

Chapter 1

Introduction

Many users today have tens to hundreds of accounts with web services that store sensitive data, from social media to tax preparation and e-commerce sites [12, 28, 65]. While users have the right to delete their data (via e.g., the GDPR [27] or CCPA [11]), users want and deserve more nuanced controls over their data that don't exist today. For example, a user might wish to hide and protect data of an e-commerce or dating app profile when inactive, but also want their data to be present should they return to use the application. Today, however, services often provide only coarse-grained, blunt tools such as permanent account deletion **more tools?** **account deactivation?** that result in all-or-nothing exposure of users' private information, and fail to achieve the flexible privacy that users want and deserve.

This thesis introduces the notion of *disguised data* for flexible data privacy. Disguised data is a reversible state of data in which sensitive data is selectively hidden. To demonstrate the feasibility of disguised data, this thesis also presents Edna—the first system for disguised data—which helps database-backed web applications allow users to remove their data without permanently losing their accounts, anonymize their old data, and selectively dissociate personal data from public profiles. Edna lets developers support these features while maintaining application functionality and referential integrity via *disguising* and *revealing* transformations. Disguising selectively renders user data inaccessible via encryption, and revealing enables the user to restore their data to the application.

This chapter motivates the need for data disguising for flexible privacy; describes the challenges in disguising and revealing data; introduces our approach to achieve data disguising; and summarizes the contributions of this thesis.

1.1 Motivation

User today lack desirable controls over their personal data stored by web applications. Consider Twitter: after a change in management [18], many users wanted to leave the platform and try out alternatives (e.g., Mastodon [45]). But each user faced a tricky question: should they keep their Twitter account, or should they delete it? Advice on how to quit Twitter [6, 46]

highlight how keeping an inactive account leaves sensitive information (e.g., private messages) vulnerable on Twitter’s servers; but deleting the account prevents the user from changing their mind and coming back, causing them to permanently lose all their followers and content. Hence, many users left Twitter but kept their accounts [5, 50, 58]. A better solution would let users temporarily revoke Twitter’s access to their data while having the option to come back.

Similarly, users give dating apps personal data, and frequently deactivate and reactivate their accounts. This sensitive data should be protected from the application and potential data breaches [23, 49] when a user deactivates their account, but be readily available when they choose to return.

Users may also prefer old data, such as past purchases in an online store or their passport details with a hotel, to be inaccessible to the service after some time of inactivity, and therefore protected from leaks or service compromises [54, 67]. Or users may prefer to—explicitly or automatically—dissociate their identity from old data, such as teenage social media posts or old reviews on HotCRP. Today, users work around the lack of such support by explicitly maintaining multiple identities (e.g., Reddit throwaway accounts [53] and Instagram “finstas” [73]), an inflexible and laborious solution.

Providing this functionality can benefit both the service and the user. It helps the service comply with privacy regulations, reduces its liability on data breaches, and appeals to privacy-conscious users; meanwhile, the user can rest assured that their privacy is protected, but can also get their data back and reveal their association with it if they want.

1.2 Disguised Data: A New Abstraction for Flexible Privacy

This desired flexible privacy functionality describes an in-between state of user data in web applications: where users are not quite gone, because they can return to the application; but they are also not quite there, because some or all of their data has been removed.

To capture this new state of data, this thesis introduces the new abstraction of *disguised data*. Disguised data represents a state of data where (i) some or all of the user’s original sensitive data is rendered inaccessible to the application; (ii) some data may be replaced with placeholders to keep the application structure intact (e.g., placeholder parent comments to maintain comment thread structure); and (iii) the data can be restored with the user’s authorization.

Systems for disguised data move closer to an Internet where users can leave services and return at any time, where old data on servers is protected by default, and where services provide users with control over their identifying data visible to the service and other users.

1.3 Challenges

Today, disguised data for flexible privacy remains out of reach for users of web applications in part because getting it right is hard. Real applications store their data in a database with com-

plex schemas and have complex notions of privacy, data ownership, and data sharing. Simple solutions that e.g., delete all data associated with a user can create orphaned data or break referential integrity—the invariant that if a table row references another row via a foreign key, the referenced row must exist—which require application changes to handle correctly. These solutions also lack support for users to return. To solve this manually, a developer would have to carefully perform application-specific database changes to remove data, store any data removed to be able to later restore it, and correctly revert the database changes on restoring.

Developers would also have to reason about interactions between multiple data-redacting features, and how these features would compose. For example, imagine an application that supports both account deletion and anonymizing old data: if a user wants to delete all their posts after they have been anonymized, a SQL query must somehow determine which anonymized posts belong to the user in order to remove them. And if the user later wants to return, the developer must account for the applied anonymization and restore posts as anonymized.

Furthermore, stored removed data must be inaccessible to the application and protected against data breaches, but must be accessible if the user chooses to return. The developer also needs to provide user-friendly ways for users to prove their ownership of the stored data.

[lyt: Finally, application databases often undergo management operations, such as schema migrations. However, these operations would fail to affect any data disguised at the time, because the disguised data remains inaccessible to the application or developer. However, the disguised data would need to reflect these global database changes in order to preserve correctness upon reveal, which would require the developer to remember and reapply these management operations on disguised data before revealing it.]

1.4 Our Approach

To realize disguised data, we present a general system that helps developers specify and apply two kinds of transformations: *disguising transformations*, which move the user’s data into a disguised state; and *revealing transformations*, which restore the original data at a user’s request. Disguising transformations aim to protect the confidentiality of users’ disguised data (e.g., links to throwaway accounts or old HotCRP reviews) even if the application is later compromised (e.g., via a SQL injection or a compromised admin’s account).

We demonstrate our approach in Edna, a system that realizes disguising and revealing transformations for database-backed web applications via a set of primitives that have well-defined semantics and compose cleanly. Developers specify the transformations that their application should provide, and Edna takes care of correctly applying, composing, and optionally reverting them, while maintaining application functionality and referential integrity.

Our approach for Edna’s approach faces three challenges, which we describe next, along with Edna’s solution.

First, Edna needs to present a simple, yet versatile interface for developers to specify dis-

guising transformations. Edna addresses this challenge with a restricted programming model centered around three primitives: remove, modify, and decorrelate (which reassigns data to placeholder users). This model limits the potential for developer error, and lets Edna derive the correct disguising and revealing operations, while supporting a wide range of transformations.

Second, to work with existing applications in practice, Edna’s disguising transformations should require minimal application modifications. To achieve this, Edna introduces *pseudoprincipals*, anonymous placeholder users that are inserted into the database on disguising and exist solely to own data decorrelated from real users (e.g., because the application requires the data to continue operating) and maintain referential integrity. Pseudoprincipals can also act as built-in “throwaway accounts,” as they let the user disown data after-the-fact, as well as potentially later reassociate with it. To correctly reason about ownership when data may be decorrelated multiple times (e.g., by global anonymization after throwaways have been created), Edna maintains an encrypted *speaks-for chain* of pseudoprincipals that only the original user can unlock and modify.

Third, Edna needs to have access to the original data for users to be able to reveal their data and return to the application, but the whole point is to make that data inaccessible to the service. While Edna could ask users to store their own disguised data, this would be burdensome. Instead, Edna stores the disguised data on the server in encrypted form as *diff records*, and unlocks and restores data to the service only when a user provides their *reveal credentials* (e.g., a password or a private key).

1.5 Contributions

The main contribution of this thesis is the identification and exploration of *disguised data* for flexible user data privacy in web applications. As part of this, this thesis contributes:

1. The abstraction of *data disguising via disguising and revealing transformations*, including disguise specifications written with a small, composable set of data-anonymizing primitives (remove, modify, and decorrelate to pseudoprincipals), and reveal credentials to allow users to reveal their data (Ch. 3).
2. Design techniques to realize disguised data, including diff records and speaks-for chains (Ch. 4).
3. Edna, a prototype Rust library for MySQL-backed web applications that implements user data control via disguising and revealing, which is open-source at <https://github.com/tslilyai/edna> (Ch. 5).
4. Case studies that integrate Edna with three real-world web applications and demonstrate Edna’s ability to enable composable and reversible transformations (Ch. 6).
5. An evaluation of Edna’s effectiveness and performance, including how Edna contrasts with and complements related work (Qapla [47] and CryptDB [55]) (Ch. 7).

While disguised data can help developers to add more flexible user data controls, the abstrac-

tion and its implementation in Edna have some limitations. First, disguised data is a concept scoped for single applications, and does not tackle the problem of data sharing between services. Edna also assumes bug-free disguise specifications, and that applications use Edna correctly. Furthermore, Edna does not aim to protect undisguised data in the database against compromise; combining Edna with an encrypted database can add this protection. Finally, attacks to identify users from Edna’s metadata (e.g., the size of stored disguised data) or placeholder data left in the database (e.g., embedded text) are out of scope.

Chapter 2

Related Work

evidence

Edna addresses the problem of disguised data for flexible data privacy in web applications. Existing systems aim instead to support data deletion, prevent unauthorized data access, or protect against database server compromise—valuable, but complementary goals to achieving disguised data.

2.1 Compliance Tools

Compliance tools such as K9db [20] and GDPRizer [2] help correctly extract or delete data in correspondence to compliance-related requests. These tools include systems to support whole-sale user data extraction or deletion by tracking data ownership by modifying the data layout [20, 63], tracking information flow [42], or changing the storage hardware [37].

Tools like DELF at Meta [17] focus on the related problem of data deletion, letting developers specify deletion policies via annotations on social graph edges and object types. DELF ensures correct cascading data deletion, both for compliance-related data deletion requests, and for normal application deletions.

While disguising data can provide GDPR-compliant account deletion, disguising also supports more nuanced use cases beyond simple deletion: for example, Edna allows users to return after deletion, hides old data for inactive users, or hides some but not all data so the user can continue using the application.

2.2 Policy Enforcement Systems

Policy enforcement systems aim to prevent unauthorized access to data and protect against leakage via compromised accounts or SQL injections. They enforce developer-specified visibility and access control policies via information flow control [16, 30, 35, 61, 75], authorized views [9], per-user views [44], or by blocking or rewriting database queries [47, 52, 77].

Policy-enforcing systems do not help users anonymize data or maintain application integrity constraints, which is the explicit goal with disguised data. Database contents of sensitive data—the data under disguise—are also modified so the data is no longer available in the database, and thus unavailable even to the service itself. This is unlike policy enforcement systems, which can deny access to sensitive data, but will still retain it in the database.

2.3 Encrypted Storage Systems

Encrypted storage systems such as CryptDB [55] and Mylar [56] protect against database server compromise, with some limitations [33]. These systems encrypt data in the database, and ensure that only users with access to the right keys can decrypt the data. Applications must handle keys, and send queries either through trusted proxies that decrypt data [55], or move application functionality client-side [56]. Encrypted databases have orthogonal goals to systems for disguised data: while they protect data at all times against attackers who do not have the keys, encrypted databases do not help applications anonymize or temporarily remove data, which systems for disguised data do. Any user with legitimate access can view the data in an encrypted database, whereas disguised data is removed from the database.

2.4 Other Related Work

Other work has also focused on protecting user data and giving users more control over their data’s exposure. However, these systems differ from Edna in the specific problem they aim to solve, the threat model against which they protect, and how they can be deployed with today’s applications.

Some platforms focus on enforcing user-defined policies, instead of developer-defined policies like Edna. They prove that server-side processing respects user-defined data policies via cryptographic means [10] or systems security mechanisms [72]. However, this may restrict feasible application functionality (e.g., to additively homomorphic functions), or restrict combining data with different policies, and requires extensive modifications to existing applications to redeploy.

Systems like Pesos [41] and Ironsafe [70] use trusted execution environments (TEEs) to enforce policy compliance in third-party storage platforms without trusting them with user data. Ryoan [36] also runs data processing applications as sandboxed modules within TEEs, thus protecting user data against untrusted applications in addition to untrusted platforms. These systems rely on the security of TEEs, which allows them to protect against their stronger threat models. However, this requires applications to be written with the systems’ specific architecture in mind, making these systems more difficult to deploy in today’s applications. By contrast, Edna trusts developers to be well-intentioned, and undisguised data can be accessed by the application.

Decentralized platforms such as Solid [60], BSTORE [15], Databox [48], and others [3, 13, 14, 43, 51] put data directly under user control, since users store their own data. But decentralized platforms burden users with maintaining infrastructure, lack the capacity for server-side compute, and break today’s ad-based business model. By contrast, Edna leaves the data and business models unchanged, and stores all data, including disguised data, on the application’s servers.

Devices using iOS [4], Android [4], or CleanOS [66] revoke data access via encryption, like Edna does. However, these systems operate in settings that store only a single user’s data; disguised data applies in settings that include multiple users’ data and shared data.

Vanish [29] provides users with self-destructing data and a proof of data deletion using decentralized infrastructure and cryptographic techniques (with limitations against Sybil attacks [74]). Unlike Edna, Vanish cannot restore deleted data and requires extensive application restructuring to deploy.

Sypse [24] pseudonymizes user data and partitions personally identifying information (PII) from other data. Instead of partitioning data, Edna modifies the database and stores disguised data encrypted.

Finally, oblivious object stores like Dory [21] and Snoopy [22] protect data and search access patterns against powerful adversaries who can e.g., compromise the entire cloud software stack and view metadata like network traffic and access patterns. To provide strong security, these systems rely on complex encryption schemes, oblivious RAM, and other cryptographic techniques; however, these techniques more greatly affect performance and deployability compared to Edna.

Chapter 3

Overview

This section introduces the concept of disguised data by illustrating how developers and users would interact with an application that supports data disguising and data revealing.



Figure 3-1: Developers write disguise specifications and add hooks to invoke Edna from the application (green); in normal operation, clients use these hooks in the application to disguise and reveal their data in the database (blue).

Edna helps developers realize new options for users to control their data via *disguising transformations*; and add support for users to invoke *revealing transformations*. The developer integrates an application with Edna by writing disguise specifications and adding hooks to disguise or reveal data using Edna’s API (Figure 3-1). This proceeds as follows:

(1) An application registers users with a public–private keypair that either the application or the user’s client generates; Edna stores the public key in its database, while the user retains the private key for use in future reveal operations.

(2) When the application wants to disguise some data, it invokes Edna with the corresponding developer-provided disguise specification and any necessary parameters (such as a user ID). Disguise specifications can remove data, modify data (replacing some or all of its contents with placeholder values), or decorrelate data, replacing links to users with links to pseudoprincipals (fake users). Edna takes the data it removed or replaced and the connections between the user and any pseudoprincipals it created, encrypts that data with the user’s public key, and stores the resulting ciphertext—the *disguised data*—such that it cannot be linked back to the user without the user’s private key.

(4) When a user wishes to reveal their disguised data, they pass credentials to the application, which calls into Edna to reveal the data. Credentials are application-specific: users may

```
// Decorrelate comments on stories w/tag {{TAG}}
"comments": [{
  "type": "Decorrelate",
  "predicate": "tags.tag = {{TAG}}",
  "from": "comments JOIN stories ON comments.story_id = stories.id
          JOIN taggings ON stories.id = taggings.story_id
          JOIN tags ON...",
  "group_by": "stories.id",
  "principal_fk": "comments.user_id" } ],
// Remove votes on stories w/tag {{TAG}}
"votes": [{
  "type": "Remove",
  "predicate": "tags.tag = {{TAG}}",
  "from": "votes JOIN stories...",
  "principal_fk": "votes.user_id",
}, ... ]
```

Figure 3-2: Lobsters topic-based anonymization disguise specification (JSON pseudocode), which decorrelates comments and removes votes on stories with the specific topic tag.

either provide their private key or other credentials sufficient for Edna to re-derive the private key. Edna reads the disguised data and decrypts it, undoing the changes to the application database that disguising introduced.

Edna provides the developer with sensible default disguising and revealing semantics (e.g., revealing makes sure not to overwrite changes made since disguising).

3.1 Example: Lobsters Topic Anonymization

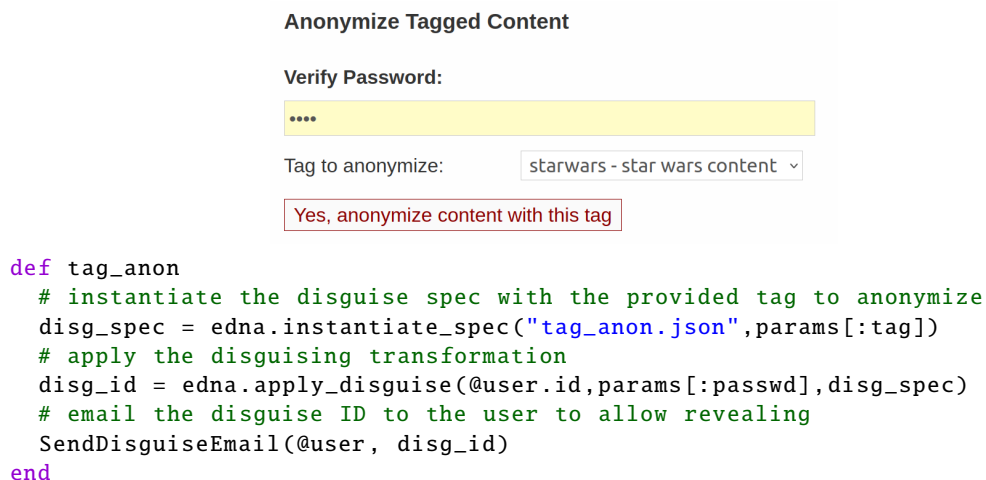


Figure 3-3: The Lobsters developer adds a hook in the UI and code to perform topic-based anonymization.

We illustrate how Edna's API and disguise specifications work via a disguising transformation for Lobsters [1]. Lobsters [1] is a link-sharing and discussion platform with 15.4k users. Its database schema consists of stories, tags on stories, comments, votes, private messages, user

```

// Decorrelate comments on stories w/tag {{TAG}}
"comments": [{
  "type": "Decorrelate",
  "predicate": "tags.tag = {{TAG}}",
  "from": "comments JOIN stories
          ON comments.story_id = stories.id
          JOIN taggings
          ON stories.id = taggings.story_id
          JOIN tags ON...",
  "group_by": "stories.id",
  "principal_fk": "comments.user_id" } ],
// Remove votes on stories w/tag {{TAG}}
"votes": [{
  "type": "Remove",
  "predicate": "tags.tag = {{TAG}}",
  "from": "votes JOIN stories...",
  "principal_fk": "votes.user_id",
}, ... ]

```

Figure 3-4: Lobsters topic-based anonymization disguise specification (JSON pseudocode), which decorrelates comments and removes votes on stories with the specific topic tag.

accounts, and other user-associated metadata. Users create accounts, submit URLs as stories, and interact with other users and their posted stories via comment threads and votes.

Consider **topic-based anonymization**, which allows users to hide their interest in a topic (a “tag” in Lobsters) by decorrelating their comments and removing their votes on stories with that tag. For instance, a Lobsters user Bea who posts about their interests—Rust, static analysis, and Star Wars—might want to hide associations with Star Wars before sharing their profile with potential employers. This is currently not possible in Lobsters.

The Lobsters developer can realize topic-based anonymization as a disguising transformation. First, the developer writes a disguise specification that instructs Edna to decorrelate comments and remove votes on “Star Wars” stories (Figure 3-4), and provides it to Edna. They also add frontend code and UI elements that allow authenticated users to trigger the disguising transformation (Figure 3-3). When Bea wants to anonymize their contributions on content tagged “Star Wars,” Lobsters invokes Edna with the provided specification.

When Bea wants to deanonymize their “Star Wars” contributions, Lobsters invokes Edna with Bea’s reveal credentials and the disguise ID, and Edna reveals Bea’s associations with “Star Wars” posts.

3.2 Disguise Specifications

Edna’s developer interface is designed so that developers need to reason only about the high-level semantics of disguising expressed in the disguise specification. Edna takes care of applying disguise transformations, composing it with other disguising and revealing transformations, and creating and storing disguised data.

Disguise specifications tell Edna what application data objects to disguise and how to dis-

guise them. A disguise specification identifies objects by database table name, principal, and predicate, where a predicate is a SQL `WHERE` clause. Edna by default disguises all objects related to the given principal, as defined by a foreign-key relationship provided in the disguise specification (using `principal_fk`), but predicates can narrow the transformation’s scope (e.g., to stories with specific tags). For each selected group of objects, developers choose to *remove*, *modify*, or *decorrelate* them. The example specification in Figure 3-4 decorrelates all comments and removes all votes on stories with a particular tag, specified by the `TAG` parameter provided at invocation time.

Modification and decorrelation require Edna to generate placeholder content for modified columns and/or new pseudoprincipals. Developers use one of Edna’s generation policies to tell Edna how to generate per-column placeholder values. The current prototype supports constants (e.g., “removed”), random values (e.g., a random email address), and values derived from the prior value (e.g., a redacted phone number with only area code visible); We can imagine expanding Edna’s generation specifications to take as input a database query dependent on external state to generate new values.

To ensure that decorrelation preserves referential integrity, Edna generates pseudoprincipals to replace the original principal. Decorrelation can use pseudoprincipals at different granularities. In the extreme, the disguise specification may tell Edna to create a unique pseudoprincipal for each decorrelated application object. In our example, however, all comments by the same user on the same story decorrelate to the same pseudoprincipal (`"group_by": "stories.id"`), thus keeping same-story comment threads intact. The same user’s comments on different stories, however, decorrelate to different pseudoprincipals; an alternative might group comments by `comments.user_id`, so a single pseudoprincipal adopts all of a user’s `TAG`-related comments (effectively creating a “Star Wars” throwaway account).

Developers can inform Edna to, upon revealing, check for any objects added after disguising that refer to pseudoprincipals; for example, a decorrelated comment might have new responses. This enables Edna to preserve referential integrity for data referring to pseudoprincipals. Edna provides three options if it finds such objects: (i) change the object’s reference to point to the original principal; (ii) delete the object; and (iii) continue referring to the pseudoprincipal. This option is global; another design for Edna could also support a menu of options, such as per-table checks and fixes (where the developer specifies per-table policies) or per-inserted-object ones (where the developer makes application modifications to log all added references to pseudoprincipals).

3.3 User Reveal Credentials

Edna provides developers and users with the abstraction of *reveal credentials*, which users provide to the application to authorize revealing their data. Reveal credentials allow applications that use Edna to support familiar user authentication workflows when users want to reveal their

disguised data.

Edna supports two forms of reveal credentials: (i) the principal's private key itself; or (ii) the principal's application password or a recovery token (in case they forget their password), either of which Edna can use to rederive the private key. Developers can use either or both of these credentials depending on application needs. In the Lobsters example, Edna rederives the user's private key using their password. Password or keypair changes require an application to re-register the user with Edna, which generates new recovery tokens and re-encrypts the user's disguised data.

3.4 Database Management Operations

do we still need to say why this is a challenge? Databases constantly undergo management operations initiated by an admin or developer, like schema changes or global updates (e.g., normalizing URLs of all stories). When one such operation is performed, the developer writes a corresponding application update specification that captures the effects of the operation and invokes Edna's `record_update` API call with the specification. Edna stores these updates in a replay log, which lets Edna reveal disguised data without overwriting the associated application changes.

Edna expects developers to provide application update specifications that takes a user's disguised data rows and produces updated-disguised data rows. Oftentimes, these updates may be a subroutine of the bulk management operation. For example, if a developer wants to normalize all URLs in Lobsters `stories`, they might first read all stories, then normalize the URL in each story individually, and finally `INSERT . . . UPDATE` the normalized stories. An application update given to Edna could just capture the normalization step, producing normalized URL stories for the stories in a user's disguised data.

In other situations, no such update exists as a subroutine of the bulk operation because the bulk operation uses queries that apply to entire database tables instead of rows. In these scenarios, the developer must write a separate update specification for updating disguised data rows. For example, Lobsters has a schema migration that adds a column to the `users` table. The bulk operation simply performs an `ALTER TABLE` query, while the update given to Edna receives user rows without the column as input, and outputs user rows with the column.

Edna assumes that either (i) updates are pure functions deterministic in their input (placeholder or disguised rows) and do not have side effects; or (ii) any nondeterminism or update side effects will maintain application correctness. As an example of an unsupported update, take an update that calculates the current vote count of a story to store as a story's `vote_count` attribute, and say that a disguise has removed both a user's story and its votes. This update thus depends on other disguised rows, namely `vote` rows. When Edna reveals the disguise, Edna will first reveal the diff records for stories before revealing those for votes in order to maintain referential integrity. But when applying the `vote_count` update to story diff records, Edna will

find 0 votes for the story, because the votes have not yet been restored. Edna supports this update only if this is correct application behavior (scenario (ii)).

3.5 Guarantees and Threat Model

Edna protects the confidentiality of disguised data between the time when a user disguises their data and the time when they reveal it. During this period, Edna ensures that the application cannot learn the contents of disguised data, nor learn what disguised data corresponds to which user, even if the application is compromised and an attacker dumps the database contents (e.g., via SQL injection). Edna stores disguised data encryptedly, so its confidentiality stems from “crypto shredding,” a GDPR-compliant data deletion approach based on the fact that ciphertexts are indistinguishable from garbage data if the key material is unavailable [25, 31, 57, 68].

We make standard assumptions about the security of cryptographic primitives: attackers cannot break encryption, and keys stored with clients are safe. If a compromised application obtains a user’s credentials, either because the user provides them to the application for reveal, or via external means such as phishing, Edna provides no guarantees about the user’s current or future disguised data. Edna also expects the application to protect backups created prior to disguising, and external copies of the data (e.g., Internet Archive or screenshots) are out of scope.

While Edna hides the contents of disguised data and relationships between disguised data and users, it does not hide the existence of disguised data. (An attacker can see if a user has disguised some data, but cannot see which disguised data corresponds to this user.) An attacker can also see any data left in the database, such as pseudoprincipal data or embedded text. Edna puts out of scope attacks that leverage this leftover data and metadata to infer which principal originally owned which objects.

Edna’s choice of threat model and its limitations stem from Edna’s goal of practicality and usability by existing applications, and from design components that support this goal. For example, decorrelation with pseudoprincipals removes explicit user-content links, but leaves placeholder information in the database to avoid application code having to handle dangling references. Similarly, leveraging server-side storage to hold disguised data leaves metadata available to attackers, but avoids burdening users with data storage management.

Chapter 4

Edna's Design

This chapter describes the design of Edna and the techniques Edna uses to support disguising and revealing. We first look at how Edna performs disguising transformations, and then dive into the details of how Edna reveals disguised data. We then describe the more complicated scenarios possible with Edna, namely disguise composition, shared data, and action as pseudoprincipals. This chapter concludes with an analysis of the security of Edna's design with respect to the threat model described in §3.5.

4.1 Disguising

To apply a disguising transformation, Edna creates a unique *disguise ID* and queries for the data to disguise based on the disguise specification predicates. To preserve referential integrity, Edna constructs a dependency graph between tables based on foreign key relations (assuming no circularity), and first performs removes from tables in topologically-sorted order. Edna then performs decorrelations and modifications in specification order, potentially generating and storing pseudoprincipals.

Next, to record disguised data, Edna generates *diff records* that contain (i) the original data row(s), and (ii) placeholder data rows the disguise inserted or rewrote in the application (e.g., pseudoprincipals or the value of any modified columns). All types of diff records also contain the disguise ID. The original and placeholder rows contained by a diff record varies by disguise operation as follows:

- Remove diff records contain (i) the removed original row, and (ii) no placeholder rows;
- Modify diff records contain (i) the unmodified row, and (ii) the row with the modified value; and
- Decorrelate diff records contain (i) the referencing row with the original foreign key value, and (ii) the referencing row with the placeholder foreign key value pointing to a pseudoprincipal, and the pseudoprincipal's row.

For each new pseudoprincipal, Edna generates a public-private keypair and adds a *speaks-for record*, which adds a link to the original principal's *speaks-for chain*. A speaks-for record contains



Figure 4-1: When Edna applies topic-based anonymization to Bea’s comments on stories tagged “Star Wars” (red), these comments are decorrelated to pseudoprincipals (“AnonPig”, “AnonFox”). Edna stores encrypted speaks-for records mapping Bea to their pseudoprincipals, and diff records containing the comments with modified foreign keys.

a pair of (original principal, pseudoprincipal) IDs and the pseudoprincipal’s private key. Edna registers the pseudoprincipal with its public key to enable composition of disguises (§4.5). Edna then encrypts the diff and speaks-for records with the principal’s key, and stores them in the database. Finally, Edna returns the disguise ID to the application. A client can use the disguise ID and the principal’s credentials to reveal the transformation later.

To perform Bea’s topic-based anonymization (Figure 4-1), Edna thus: (i) queries the database to fetch comments and votes by Bea affiliated with “Star Wars”; (ii) creates a pseudoprincipal (e.g., “AnonFox”) for every “Star Wars”-tagged story that Bea commented on, and inserts it as a new user; (iii) modifies the database by rewriting comment foreign keys to point to the created pseudoprincipals, and removing Bea’s votes on those stories; (iv) creates new speaks-for records that map Bea to the created pseudoprincipals and create new links in Bea’s speaks-for chain; diff records containing Bea’s votes on “Star Wars” stories; and diff records that document Bea’s original ownership of “Star Wars”-tagged comments and the placeholder pseudoprincipal data; (v) encrypts the speaks-for and diff records with Bea’s public key, stores them; and (vi) returns a unique disguise ID to the application.

Edna adds a *disguise table* and a *principal table* to the application database to store principals’ disguised data. The disguise table contains lists of per-principal diff and speaks-for records encrypted with the principal’s public key. The principal table is indexed by application user ID; each row contains the principal’s public key, and a list of disguise table indexes encrypted with the public key. To store records for principal p , Edna (i) encrypts the records with p ’s public key; (ii) stores the ciphertext in the disguise table under index idx ; (iii) encrypts idx (salted to prevent rainbow table attacks) with p ’s public key; and (iv) appends the encrypted idx to p ’s list of encrypted disguise tables indexes in the principal table.

This allows Edna to store records without needing access to the principal’s private key, and to do so securely: the principal table adds a layer of indirection from user ID to encrypted records, so an attacker cannot link principals to their records. At reveal time, Edna can efficiently find


```

Reveal(disgID, uid, privkey):
    encrypted_disg_table_idx := principal_table[uid]
    decrypted_disg_table_idx :=
        decrypt(encrypted_disg_table_idx, privkey)
    for idx in decrypted_disg_table_idx:
        records = decrypt(disg_table[idx], privkey)
        for rec in records:
            if rec.disgID == disgID:
                // apply rec to application database
                // remove rec from disg_table
            else if rec.type == SPEAKS_FOR:
                // recursively reveal for pseudoprincipal
                // generated by another disguise
                Reveal(disgID, rec.pp_uid, rec.pp_privkey)

```

Figure 4-2: Pseudocode for revealing a disguising transformation while application principal uid exists. Recursive revealing (the else clause) walks the speaks-for chain to reveal composed records of pseudoprincipals created by other disguising transformations if necessary (§4.5).

disguised data for a given user by decrypting and using disguise table indexes in the principal table.

Disguising transformations may completely remove a principal from the application database. When this happens, Edna moves the corresponding list of encrypted disguise table indexes from the principal table to a *deleted principal table* indexed opaquely, e.g., by the public key. This removes the user ID from the database while allowing future reveal operations by the principal to find their disguise table indexes. Edna also stores a special type of remove diff record that contains the principal’s ID and the principal’s public key when a disguise removes a principal. This allows Edna to restore the principal to Edna’s principal table if a user later reveals the disguise.

4.2 Revealing

To apply a reveal transformation, Edna first locates and decrypts the corresponding diff and speaks-for records using a disguise ID and the user’s reveal credentials.

Edna’s reveal procedure (Figure 4-2) first looks up all disguise records related to the provided reveal credentials via Edna’s principal and disguise tables. Edna then applies diff records created for the disgID disguise transformation to the database, thus restoring the relevant application objects to their pre-disguised state.

To preserve referential integrity, Edna restores disguised data that was removed from tables in topologically-sorted order (again constructing the dependency graph). Edna then reveals any modifications, and finally performs recorrelations. In general, to reveal a diff record, Edna removes the placeholder row and inserts the original row (both of which are recorded in the diff record). However, for efficiency, Edna first checks if a placeholder row in diff records has the same identifiers (e.g., a primary key) as an original data row in the diff record, and if so, will update the relevant columns of the placeholder row instead.

Finally, Edna de-registers any pseudoprincipal who no longer has any associated disguised data, removing them from the principal table and the application’s users table. Developers can configure Edna to also check for references to pseudoprincipals prior to removing them, and depending on the application’s needs, configure Edna to delete, rewrite, or leave the references in place. After revealing, the disguised data is no longer needed, so Edna clears the corresponding diff and speaks-for records.

In the example, if Bea wants to reveal their “Star Wars” contributions, Lobsters invokes Edna with the disguise ID and Bea’s password as reveal credentials. Edna uses the password to reconstruct Bea’s private key, retrieve and decrypt Bea’s records, and filter those records for those with the disguise ID. Edna then restores deleted votes and Bea’s ownership of decorrelated comments.

4.3 Database Management Operations

Edna’s revealing as described thus far may accidentally reveal data that ignores database management operations applied since the time of disguise, such as global application updates to undisguised data or schema migrations. To prevent this, Edna utilizes developer-provided information about important updates and schema migrations to apply them to disguised data prior to revealing it, ensuring that revealed data reflects the current state of the database. Prior to revealing the updated data, Edna will also perform consistency checks to guarantee adherence to internal database invariants, such as uniqueness constraints. Here, we describe how developers specify application updates and schema migrations; how Edna applies these updates to data to reveal; and Edna’s consistency checks.

4.3.1 Application Updates.

In order for revealing to preserve application correctness, Edna must know about application updates that alter invariants over application data. Consider an example where a moderator periodically edits all posts to remove swear words, creating an implicit invariant that all posts created prior to the last moderation pass should contain no swear words. If a user’s disguise removes their posts, then a moderation pass occurs, and then the user wants to restore their posts, Edna would not know about these moderation updates to posts of the application and incorrectly restore the original post content with swear words present upon reveal. However, Edna could correctly restore the post if it knew to remove the swear words prior to reveal.

Figure 4-3 demonstrates how Edna applies application updates to disguised data using a replay log.

- (1) Edna disguises some user data.
- (2) The application invokes Edna when it performs operations that need to hold over disguised data when it is revealed—e.g., moderations—and Edna records these updates in its replay log.



Figure 4-3: When the application applies updates like moderations of explicit words, it can invoke Edna to log the update. Edna then applies the update to disguised data in diff records prior to reveal. Yellow highlights changes to the application data or Edna's data.



Figure 4-4: Similar to a moderations update, the application can notify Edna of a schema migration to apply to diff records prior to reveal. Yellow highlights changes to the application data or Edna's data. For simplicity, only the placeholder data of a pseudoprincipal row is shown; in reality, placeholder data exists as part of e.g., a decorrelation diff record.

- (3) When revealing data, Edna applies, in order, every entry in the replay log added since the time of disguise to the disguise's diff records. Updates map the original data and the placeholder data in diff records to corresponding updated-original and updated-placeholder data.
- (4) After applying all updates to placeholder data, Edna reveals the updated rows in the diff record like normal.

In the swear words moderation example, Edna queries the replay log, sees the swear words moderation entry, and then applies the swear words moderation to the removed post data in the diff record. Only then does Edna restore the post with no swear words.¹

4.3.2 Schema Migrations

Applications also constantly undergo database management operations which migrate its schema to reorganize data or add new application features. When these occur, Edna must know how to manipulate any disguised data structured in the old database layout to match that of the current database. At first glance, global application updates like URL normalization might seem like a different class of database management operation than structural changes like schema migration, and require a different approach. However, the technique described in §4.3.1 for application updates allows Edna to handle schema migrations as well.

Take, for example, a developer of an application with a `users` table that contains rows with `usernames`, `addrs`, and `emails`. The developer may choose to allow users multiple addresses via a schema migration. To do so, they would create a new `addrs` table, with a foreign key to the `users` table, and populate `addrs` using the address data in `users`. Finally, they would remove the `addr` column from `users`.

Figure 4-3 demonstrates how Edna applies such a schema migration to disguised data.

- (1) Edna disguises some user data.
- (2) The application invokes Edna when it performs the schema migration; Edna records these the migration update in its replay log.
- (3) When revealing data, Edna applies the schema migration update to diff record data, which maps an original `users` data row to both a row in `users` with username `uid` and a row in `addrs` that has a foreign key of `uid` to `users`. The update also generates two rows for any placeholder `users` data row in a diff record.
- (4) Edna then respectively restores and removes the migrated original data and placeholder data respectively, both of which now consist of one `users` and one `addrs` row.

¹Note that in this example, the diff record contains no placeholder data that replaced the removed post; in other scenarios such as decorrelation or modification, Edna would apply the logged update to placeholder data as well. The updated placeholder data would then be removed.

4.3.3 Consistency Checks for Internal Invariants

After applying any developer-specified migrations or updates since the time of disguising, Edna performs consistency checks on the data to reveal to ensure that revealing will not violate the database's integrity. These checks allow revealing only if the revealed data: (i) will still satisfy uniqueness and primary key constraints; (ii) will not overwrite modifications that occurred while data was disguised; and (iii) will maintain referential integrity.

For (i), Edna checks that *removed* disguised data is still removed from the database.

For (ii), Edna ensures that *modified* disguised data is in the same modified state and *decorrelated* disguised data is still affiliated with the same pseudoprincipal in the database using the new value stored in the diff record. By default, Edna performs checks at column-granularity. For example, an application database row can have two modified columns, but at the time of reveal, Edna finds that only one column still is at the modified state that Edna expects. The other column must have been updated since the time of the disguise. Edna will then only reveal the one matching column that passed the check in order to avoid overwriting application updates, thus partially restoring the modified row. Developers can optionally specify that rows must be completely revealed, i.e., if any column fails the check, Edna should not reveal *any* column in the row.

To ensure (iii), Edna checks for the existence of all objects referenced by the data to reveal (e.g., a post referenced by a to-be-revealed comment).

Edna is conservative and will never reveal rows for which checks fail; the affected data remains disguised. For example, if a developer chooses not to register conflicting application updates or schema migrations, Edna's checks may fail, preventing disguised data from being revealed. Edna could log encountered conflicts, giving the application a chance to fix them so a later reveal can pass the checks.

4.4 Shared Data

Many applications support shared data; in Lobsters, for example, messages between users are owned by both users. Edna's default semantics for shared data implement an ownership model inspired by a common treatment of messages as jointly owned. When a user disguises shared data, Edna decorrelates the data from the disguising user, but preserves the data and its association with other owners. Edna removes the data once all users have disguised it and all ownership links are to pseudoprincipals. Any owner can reveal the message, which restores the message to the database if it does not exist, and recorrelates only the revealing user; all disguised owners remain decorrelated as pseudoprincipals until they also choose to reveal the message. Regardless of the reveal order, if all owners reveal the message, Edna returns the message to its original state.

For instance, consider the scenario in Figure 4-5 where Bea and Chris share a Lobsters message:



Figure 4-5: Edna supports joint ownership semantics, where shared data is not removed until all users have disguised their accounts. Owners can return in any order, and the message remains decorrelated from unrevealed owners.

- (1) When Bea disguises the message, the message is owned by Chris and a pseudoprincipal;
- (2) If Chris then disguises the message, Edna removes it.
- (3) If Bea reveals the message, this restores the message to the database and recorrelates only Bea; Chris remains decorrelated as a pseudoprincipal.
- (4) When Chris reveals the message, Edna returns the message to its original state.

Edna’s Solution. Edna supports these joint ownership semantics with the following design, depicted in Figure 4-6.

- (1) The first time any owner removes the data, Edna generates pseudoprincipals for each owner of the data, and creates a fully-decorrelated version of the shared data row.

This decorrelated row is stored as a (plaintext) remove diff record in a *partially-removed* table created by Edna, indexed by the row’s unique identifier columns (e.g., a primary key id).

- (2) When another owner’s disguise removes the data, Edna stores a copy of the fully-decorrelated diff record for the disguise, diff records recording the associated pseudoprincipal row and foreign key rewrite for the owner, and a speaks-for record recording which pseudoprincipal the owner can speak-for.

As shown in this example, if the owner also happens to be the last remaining owner (all other owners are pseudoprincipals, i.e., all other owners have removed the data), Edna removes the shared data row from the application database, and the fully-decorrelated diff record from Edna’s partially-removed table.

- (3) When *any* owner chooses to return, Edna first restores the fully-decorrelated row from the copy of the fully-decorrelated diff record in the owners’s disguised data. Edna then rewrites the foreign key for the pseudoprincipal who currently owns the shared data to recorrelate with the owner, and removes that pseudoprincipal, revealing the other diff records like normal.
- (4) If a subsequent owner reveals the shared data, Edna’s consistency checks will prevent the reveal of the fully-decorrelated row (inserting the row will cause a duplicate row in the table). However, Edna will still rewrite the foreign key for that owner’s pseudoprincipal to the original owner, and remove the pseudoprincipal from the database.

Thus, Edna can disguise and reveal shared data no matter the order in which its owners decide to remove or reveal it. If an owner never removes the shared data, they will continue to be correlated and have access to the data even if other owners remove it (and become pseudoprincipals); similarly, if an owner never restores the shared data, the data will remain forever owned by the owner’s pseudoprincipal if other owners choose to restore it.



Figure 4-6: Edna implements joint ownership semantics by storing a fully decorrelated REMOVE diff for the shared data (modifications to the shared message data are depicted using [owner→pseudoprincipal] notation). Owners can only see pseudoprincipals for the other owners in their disguised data. This allows Edna to disguise and reveal in any order.

4.5 Composing Disguising Transformations

Edna supports composition of disguising transformations, which occurs when a transformation applies to data that Edna had previously disguised in some other way. Reasoning about composition of transformations can be broken down to reasoning about the composition of primitive operation pairs, e.g., remove after modify, or remove after decorrelation. Many pairs result in trivial composition: no operation can be composed after a remove (the data is gone), and any operation after a modify updates the data as expected.

However, operations after decorrelation results in more complex composition scenarios. For instance, decorrelation after decorrelation could occur if a user decorrelates some posts, after which an administrator decorrelates *all* posts. In this scenario, the administrator’s disguising operation applies to pseudoprincipal-owned posts in the same way as it does to unmodified posts. This creates pseudoprincipals that can speak-for other pseudoprincipals. Edna uses the pseudoprincipal’s registered public key to encrypt pseudoprincipal diff and speaks-for records, so Edna does not need to know its link to an original principal in order to encrypt and disguise its data.

Removal or modification after decorrelation also require special handling. For instance, a Lobsters user might first decorrelate some of their comments and then request to delete all their comments (e.g., by deleting their account). But the decorrelated comments are no longer linked to the original user; how can the deletion transformation find them? Edna addresses this question by accepting optional reveal credentials as part of the disguise operation. These credentials let Edna decrypt the user’s previous diff and speaks-for records, find all pseudoprincipals corresponding to that user, and apply disguising transformations on behalf of those pseudoprincipals as well as the user. Edna uses pseudoprincipal private keys in decrypted speaks-for records as credentials to recursively find pseudoprincipals from multiple decorrelations.

Out-of-Order Reveals. Edna must also handle reveals of transformations in any order. As before, many scenarios are straightforward: revealing removals is trivial (data can only be removed and restored once), and revealing modified data simply restores the original (subject to consistency checks). Handling out-of-order reveals of multiple decorrelations presents the greatest challenge. Edna’s semantics enforce that data that is decorrelated multiple times will not be recorrelated until all disguises are removed. For example, as shown in Figure 4-7 (left-hand side), if Bea separately decorrelates their comments on “bears” and “Star Wars” posts, then later reveals the “bears” posts, they might want Ewok-related comments (tagged both “Star Wars” and “bears”) to remain disguised, even though they were initially disguised under the “bears” transformation. To support this, Edna maintains a chain of speaks-for records that represent speaks-for relationships between pseudoprincipals. All reveal operations walk the full speaks-for chain to reveal all necessary records (cf. Figure 4-2).

Furthermore, if reveal operations perform recorrelations out of order, Edna removes an intermediate link in the speaks-for chain. To describe how this works, take the example of two



Figure 4-7: Edna allows multiple decorrelations to compose, and can reveal them in any order such that the data remains decorrelated until the user reveals *all* applied decorrelations. The speaks-for chain encoded in speaks-for records (shown in blue) allows Edna to handle recorrelation of intermediate pseudoprincipals. When Bea requests reveal of their “Star Wars” posts (4) after revealing “bears” posts (3), Edna walks the speaks-for chain backwards from P_2 to find the latest principal that can speak-for P_2 and has not yet been recorrelated. Thus, Edna restores ownership back to Bea.

disguises that decorrelate comments on “bears” and “Star Wars” posts respectively (Figure 4-7).

- (1) First, the “bears” decorrelation rewrites Ewok posts to pseudoprincipal P_1 .
- (2) Next, the “Star Wars” decorrelation composed on top decorrelates Ewok posts from P_1 to pseudoprincipal P_2 . At this point, Edna has speaks-for records for Bea that encode a speaks-for chain from $\text{Bea} \rightarrow P_1 \rightarrow P_2$.
- (3) If Bea first reveals the “bears” anonymization—the first applied disguise—on their data, Edna finds all accessible speaks-for records given Bea’s reveal credentials (cf. Figure 4-2), and constructs Bea’s speaks-for chain as a graph of principal-to-principal edges (namely $\text{Bea} \rightarrow P_1 \rightarrow P_2$). Edna finds that P_1 ’s “Ewok” posts no longer exist in the database (they belong to P_2 due to the composed “Star Wars” disguise), and thus does not restore “Ewok” posts to Bea. Edna does still remove pseudoprincipal P_1 in the process of restoring “bear” diff records, and once done, clears all “bear” diff records from its encrypted disguise table. Importantly, however, Edna still retains the speaks-for record for $\text{Bea} \rightarrow P_1$, since P_1 still has associated disguised data (namely a speaks-for record to P_2)!
- (4) Now, if Bea reveals the second applied disguise—“Star Wars”—Edna finds diff records for decorrelated “Ewok” posts whose original rows have P_1 as owner. However, Edna cannot reveal the diff record directly and restore the decorrelated posts to P_1 , as this will fail referential integrity consistency checks, and also result in incorrect composition semantics. Instead, Edna walks the speaks-for chain ($\text{Bea} \rightarrow P_1 \rightarrow P_2$) backwards from P_2 to determine the *next valid* user in the chain who speaks-for P_2 , which in this case is Bea. Validity is determined by whether the user is a natural principal or a pseudoprincipal yet to be recorrelated. If a pseudoprincipal has a decorrelate diff record from any disguise still present in Bea’s disguised data, Edna knows the pseudoprincipal has not yet been recorrelated.

After determining Bea is the next valid user in the speaks-for chain to P_2 , Edna rewrites the “Ewok” diff record to reference Bea instead of P_1 , and then restores the diff record like normal. Finally, Edna deletes the diff records for the “Star Wars” disguise, the speaks-for records for P_2 (which no longer has any associated disguised data), and the speaks-for records for P_1 (which also has no associated disguised data after P_2 is removed). This implicitly truncates the speaks-for chain to simply be Bea.

Edna enforces the invariant that the chain only truncates at link L once all pseudoprincipals recursively generated in the chain beyond L have been recorrelated.

4.6 Authenticating As Pseudoprincipals

As described so far, if Bea wanted to modify a decorrelated “Star Wars” comment, they would have to reveal the comment, edit it using their normal credentials, and then redisguise the

comment. Edna applications can also let users modify decorrelated records without the reveal step. To support this, an application accepts reveal credentials along with a modification request. Edna uses these credentials to validate that the user speaks-for a specific pseudoprincipal by walking the speaks-for chain (cf. Figure 4-2) and ensuring that the user can access a speaks-for record linked to the pseudoprincipal. After validating the user’s request, Edna updates the database with the modification.

4.7 Design Limitations

Disguises. Edna assumes that all desired disguises are captured with the three primitive operations (remove, modify, and decorrelate). Furthermore, disguising transformations may affect data processing of application data (e.g., aggregates over the number of users), or application side effects dependent on application data (e.g., sending notifications). Edna currently expects the developer to correctly handle these scenarios, and ensure that any modified aggregations or placeholder data does not violate application correctness.

API. Edna’s API assumes that:

1. the application uses a relational database;
2. rows to disguise have direct foreign key relationships to a users table, where each user corresponds to a row of that table;
3. all rows to disguise are owned by one or more principals; and
4. all rows can be uniquely identified (e.g., via primary key).

Applications that do not satisfy these assumptions—e.g., because they have complex ownership chains or use a NoSQL database—could be supported with extensions to Edna’s design. Edna could use techniques from DELF [17] to support multiple data models; and K9DB’s data ownership graph [20] to handle indirect data ownership. If no user owns a data item, Edna should likely perhaps refuse to disguise it, and flag the developer to review the disguise specification. Finally, to address the unique identification requirement, Edna could add unique IDs for every data object, so Edna can refind the object when revealing. However, this method requires more invasive changes to application data.

Edna’s Replay Log. Updates in replay logs only apply to diff records, which contain the actual data changes, and not speaks-for records; Edna assumes that the identifiers for principals in speaks-for records that encode the speaks-for chain remain consistent as the database changes, allowing Edna to use its composition techniques with speaks-for chains (§4.5) to reveal multiple disguises in any order.

Furthermore, as described in §3.4, Edna assumes that either (i) updates are pure functions deterministic in their input and do not have side effects; or (ii) any nondeterminism or update side effects will maintain application correctness. One potential solution would be for develop-

ers to indicate the data dependencies of each update, so Edna could know to e.g., restore votes before posts in the vote count example from §3.4. However, this requires Edna to disable foreign key checks and carefully check for referential integrity after restoring posts, since restoring votes first can now inadvertently leave dangling pointers. A perhaps more realistic but more limited solution might require developers to schedule cron jobs to habitually perform the update to “fix up” any rows that have been revealed since the update. However, this only works for an idempotent update, as it should not incorrectly update already-updated rows again.

4.8 Security Discussion

Edna’s design achieves confidentiality of disguised data between the time of disguising and revealing, its key goal. Some aspects of Edna’s design help make Edna practical and deployable without major application modifications, but give up stronger security in exchange for usability.

Under Edna’s threat model, Edna achieves:

1. confidentiality of disguised data, via encrypting disguised data using asymmetric encryption, so only the owning user’s private key can reveal it;
2. confidentiality of which encrypted disguised data belongs to which user, via opaque, encrypted indexing to reference a user’s disguised data; and
3. reduced linkability between parts of a user’s data, via splitting data ownership among pseudoprincipals.

However, an attacker sees all application database content and code, and Edna’s disguise, principal, and deleted principal tables. Thus, what the attacker learns includes:

1. any undisguised data in the application database;
2. the active principals that have disguised data, via Edna’s principal table;
3. the pseudoprincipals currently registered, from Edna’s principal table and the application DB;
4. the number of deleted principals, via the size of the deleted principal table;
5. the amount of disguised data in Edna; and
6. the disguise specifications, from application code.

Edna provides decorrelation with pseudoprincipals to ease integration with existing applications, even though pseudoprincipals (and their mere existence) can reveal information to the attacker. Pseudoprincipals preserve application data and referential integrity, ensuring that e.g., every post always has an author, or that vote counts on posts remain unchanged, without requiring the developer to handle special cases of deleted users and orphaned data. However, this necessarily leaves information in the database.

Similarly, leveraging the application database to store disguised data increases Edna’s practicality as it reuses existing server-side storage and avoids burdening users with managing their disguised data, but leaves potentially exploitable metadata available to attackers. An attacker could leverage pseudoprincipal groupings (e.g., a pseudoprincipal owning posts in both “CMU

2018” and “BayArea” topics), undisguised data (e.g., comments signed with the user’s name), and Edna metadata (e.g., that some anonymous user has more disguised data than another, as Edna stores disguised data without padding for efficiency) to infer the identity of the original owning principal.

Finally, Edna makes no guarantees for users who actively use disguised data after compromise (e.g., by revealing or editing decorrelated data): after an attacker compromises the application at time t , they can harvest private keys that clients provide after t . However, Edna always protects users’ disguised data if they remain inactive.

The attacker never has access to a user’s private key unless the user actively provides their credentials. The attacker also cannot access the private key of any pseudoprincipal because it is in an encrypted speaks-for record. If an application uses password-based reveal credentials, Edna guarantees security equivalent to the security of the user’s password.

Chapter 5

Implementation

table with components and loc Edna’s prototype consists of $\approx 10k$ lines of Rust, and supports MySQL. Edna also provides an API server that exposes a JSON-HTTP API that applications can use to invoke Edna.

5.1 Secure Record Storage

When encrypting diff and speaks-for records, Edna appends a random nonce to the record plaintext to prevent known-plaintext attacks. It then generates a new public/private keypair for x25519 elliptic curve key exchange. Using the newly created private key and the principal’s public key, Edna performs the x25519 elliptic curve Diffie-Hellman ephemeral key exchange to generate a shared secret. Edna encrypts the record data with the shared secret, and saves the ciphertext along with the freshly generated public key (required to decrypt the data given the principal’s private key). This public key algorithm lacks key anonymity, so an attacker can determine which records belong to the same principal, but this is not fundamental [7].

5.2 Reveal Credentials

Edna supports two forms of reveal credentials: (i) private keys; or (ii) principals’ passwords, and recovery tokens in case they forget their passwords. If an application chooses to use the latter, it provides the principal’s password to Edna upon user registration. Edna uses a variant of Shamir’s Secret Sharing [64] to generate three shares from the private key, any two of which can reconstruct the private key. Shares are $(x, f(x) \bmod p)$ tuples, where $f(x) = \text{privkey} + \text{rand} \cdot x$ and $p > \text{privkey}$ is a known prime. One share derives x from the user’s password using a Password-Based Key Derivation Function (PBKDF) [38]. Edna stores the resulting $f(x)$ half of the share, allowing Edna to derive one full share from the password. Edna returns the second full share as a recovery token and stores the third full share. Edna can combine this third share with the recovery token or a full share derived from the password to recover the private key.

The PBKDF ensures that Edna cannot guess the password-derived value with dictionary and rainbow table attacks [76], and that Edna cannot brute force the recovery token.

Password-based secret-sharing is only one possible implementation for backup secrets; Edna could also support password-based backup secrets by, for example, storing a version of the private key encrypted with the user’s password.

5.3 Application Updates Replay Log

Edna’s prototype accepts application update specifications as Rust functions from database objects (`<table, row>` pairs) to a new set of database objects. Edna stores the log as a vector of updates function pointers with timestamps, and persists the pointers to disk. This approach requires recompiling Edna to add new update functions; an alternative approach could put the functions into separate executables (and Edna would store executable names instead of function pointers). In this alternative, Edna would invoke these executables upon reveal with serialized input rows, and deserialize the output.

5.4 Batching

For efficiency, Edna batches the deletion of rows from the same table, updates to rows of the same table from modifications and decorrelation, and the creation of pseudoprincipals upon disguise. Edna also batches the deletion of pseudoprincipals during reveal, and the reveal of same-table diff records. This allows, for example, all updates for database management operations to be applied to all diff record rows of the same table at the same time; and for all rows of the same table to be inserted, updated, or removed from the database in a single query.

5.5 Concurrency

Edna runs disguising and revealing transformations in transactions, providing serializable isolation to application users. If a query within a transformation fails, the entire transformation aborts (returning an error to the application). Edna provides an option to run long-running transformations that touch large amounts of data (e.g., anonymization of all users’ posts) without a transaction, at the expense of clients potentially observing intermediate states.

Chapter 6

Case Studies

This section evaluates Edna’s ability to add new disguising features to several applications; §7 evaluates the effort needed to do so and the resulting performance.

We add disguising and revealing transformations based on the motivating examples in §1 to three applications—Lobsters [1], WebSubmit [62], and HotCRP [39].

6.1 Lobsters

Lobsters is a Ruby-on-Rails application backed by a MySQL database. Beyond the previously-mentioned stories, tags, etc., Lobsters also contains moderations that mark inappropriate content as removed. We added three disguising transformations: account deletion with return; account decay (i.e., automatic dissociation and protection of old data); and topic-specific throw-away accounts.

GDPR-compliant account deletion (i) removes the user account; (ii) removes information that’s only relevant to the individual user, such as their saved stories; (iii) modifies story and comment content to “[deleted content]”; (iv) decorrelates private messages; and (v) decorrelates votes, stories, comments, and moderations on the user’s data. This preserves application semantics for other users—e.g., vote counts remain consistent even after account deletion, and other users’ comments remain visible—while protecting the privacy of removed users. Important information such as moderations on user content remains in the database, and Edna recorrelates it if the user restores their account. After Edna applies the disguising transformation, Lobsters emails the user a URL that embeds the disguise ID. The user can visit this URL and provide their credentials to restore their account.

The **account decay** transformation protects user data after a period of user inactivity. We added a cron job that applies account decay to user accounts that have been inactive for over a year. This (i) removes the user’s account; (ii) removes information only relevant to the user, such as saved stories; (iii) and decorrelates votes, stories, comments, and moderations on the user’s data by associating them with pseudoprincipals. Lobsters sends the user an email which

informs them that their data has decayed, and includes a URL with an embedded disguise ID that can reactivate or completely remove the account if credentials are provided.

Finally, topic-based throwaway accounts via **topic-based anonymization** enable users to decorrelate their content relating to a particular topic. As per §3.1, this disguises contributions associated with the specified tag by (i) decorrelating tagged stories and comments associated with tagged stories, and (ii) removing votes for tagged stories. Again, Lobsters sends the user an email with links that allow reclaiming or editing these contributions.

With Edna’s support for composing disguising transformations, users can delete accounts that have been decayed or dissociated into throwaways, and can later reveal them.

Application Updates and Schema Migrations. We implemented three examples of recent application updates and schema migrations applied by the Lobsters developers in 2023-2024. The first is an application update and schema migration which performs URL normalization [8] on the `url` column of all rows in the `stories` table, and then stores the normalized URL text in a new `normalized_url` column. The second changes the schema by adding a `show_email` attribute to the `users` table automatically set to `false`. The third creates a new `story_texts` table that stores the `title`, `description`, and `story_cache` attributes of rows from `stories`. This enables search over story content. The `story_cache` column is then removed from `stories`.

6.2 WebSubmit

We integrated Edna as a Rust library with WebSubmit [62]. WebSubmit is a homework submission application used at Brown University, and its schema consists of tables for lectures, questions, answers, and user accounts. Clients create an account, submit homework answers, and view their submissions; course staff can also view submissions, and add/edit questions and lectures. The original WebSubmit retains all user data forever. We added support for two disguising transformations: GDPR-compliant user account removal with return, and instructor-initiated answer anonymization, which protects data of prior years’ students by decorrelating student answers for a given course. These transformations allow instructors to retain FERPA-compliant [71] answers after the class has finished. With Edna, students can delete their accounts or access and view their answers even after class anonymization, and can always restore their deleted accounts, including restoring them to anonymized state.

6.3 HotCRP

HotCRP is a conference management application whose users can be reviewers and/or authors. HotCRP’s schema contains papers, reviews, comments, tags, and per-user data such as watched papers and review ratings [39]. HotCRP currently retains past conference data forever and requires manual requests for account removal [40]. We wrote two disguise specifications for

HotCRP: conference anonymization to protect old conference reviews, and GDPR account removal with return.

Conference anonymization is invoked by PC chairs after the conference and decorrelates users from their submissions, reviews, comments, and per-user data such as watched papers. User accounts remain in the database with no associated data. Conference anonymization protects users' data after the conference; with Edna, users can come back to view or edit their anonymized reviews and comments.

Account removal (i) removes the user's account; (ii) removes information only relevant to the user, such as their review preferences; (iii) removes their author relationships to papers; and (iv) decorrelates the remainder of their data, such as reviews. Decorrelating a review removes its association with the reviewing user, but importantly keeps the review itself around to preserve utility for others (e.g., the PC and the authors of the reviewed paper). With Edna, users can remove their accounts even after conference anonymization has taken place, and can always restore their accounts.

Chapter 7

Evaluation

Update with numbers from Google Cloud Fix figures

Our evaluation seeks to answer six questions:

1. How much developer effort and application modification does Edna require? (§7.1)
2. How expensive are common application operations, as well as disguising, revealing, and operations over disguised data with Edna? (§7.2)
3. What overheads does Edna impose, and where do they come from? (§7.3)
4. How does the effort required to implement Edna’s functionality in a related system (Qapla [47]), and its performance, compare with using Edna? (§7.4)
5. What is the performance impact of composing Edna’s guarantees with those of encrypted databases? (§7.5)
6. Which categories of application updates and schema migrations can Edna support, and with what overheads? (§7.6)

We compare Edna to three alternative settings: (i) a manual version of each disguising transformation that directly modifies the database (e.g., via SQL queries that remove data), which lacks support for revealing and does not support composition of multiple transformations; (ii) an implementation of disguising and revealing in Qapla [47] using Qapla’s query rewriting and access control policies; and (iii) an integration of Edna with CryptDB [55], an encrypted database.

All benchmarks run on a Google Cloud `n1-standard-16` instance with 16 CPUs and 60 GB RAM, running Ubuntu 20.04.5 LTS. Benchmarks run in a closed-loop setting, so throughput and latency are inverses. We use MariaDB 10.5 with the InnoDB storage engine atop a local SSD.

7.1 Edna Developer Effort

We evaluate the developer effort required to use Edna by measuring the difficulty of implementing the disguising and revealing transformations in our three case studies. This took one person-day per case study for a developer familiar with Edna but unfamiliar with the applications.

A developer supporting these transformations must first add application infrastructure to allow users to invoke them and notify users when they happen. This is required even if the developer were to implement transformations manually without Edna. These changes add 179 LoC of Ruby to Lobsters (160k LoC), and 312 LoC of Rust to the original WebSubmit (908 LoC). They implement HTTP endpoints, authorization of anonymous users, and email notifications.

A developer using Edna also writes disguise specifications and invokes Edna. Lobsters' disguise specifications are written in 518 LoC, WebSubmit's in 75 LoC, and HotCRP's in 357 LoC (all in JSON). The specification size is proportional to schema size and what data each application disguises. Writing the corresponding updates for the three Lobsters bulk management operations required an additional 81 LoC on top of the 89 LoC the application developer wrote for the bulk database management operations themselves.

Thus, the developer effort required to use Edna—writing Edna specifications, and invoking Edna—is small, even though these applications were not written with Edna in mind.

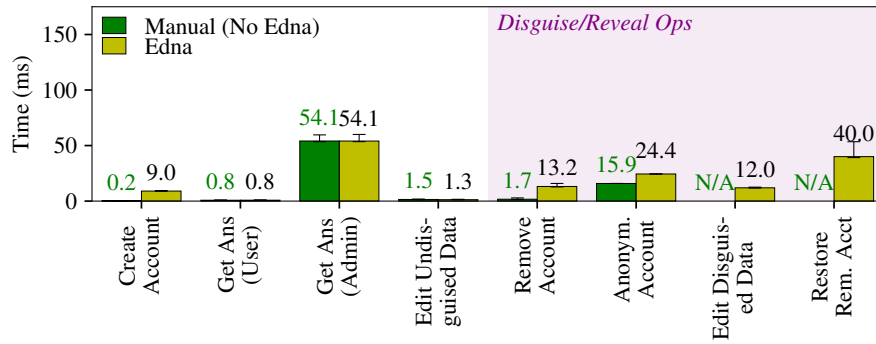
7.2 Performance of Edna Operations

We now evaluate Edna's performance using WebSubmit, HotCRP, and Lobsters (Ch. 6). We measure the latency of common operations, disguising transformations, and operations over disguised data enabled by Edna (e.g., account restoration and editing disguised data). The three applications do not create new data that references pseudoprincipals, but to fully capture any overheads we configure Edna to nevertheless run the checks for lingering pseudoprincipal references on revealing. A good result for Edna would show no overhead on common operations, competitive performance with manual disguising, and reasonable latencies for revealing operations only supported by Edna (e.g., a few seconds for account restoration)

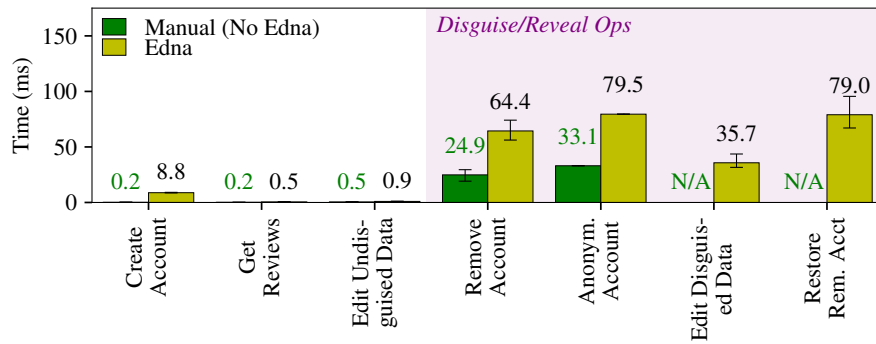
WebSubmit. We run WebSubmit with a database of 2k users, 20 lectures with four questions each, and an answer for each question for each user (160k total answers). We measure end-to-end latency to perform common application operations (which each issue multiple SQL queries), as well as disguising and revealing operations when possible (revealing operations are impossible in the baseline). Figure 7-1a shows that common operations have comparable latencies with and without Edna. Edna adds 9ms to account creation; and disguising and revealing operations take longer in Edna (13.2–40.0ms), but allow users to reveal their data and take less developer effort.

HotCRP. We measure server-side HotCRP operation latencies for PC members on a database seeded with 3,080 total users (80 PC members) and 550 papers with eight reviews, three comments, and four conflicts each (distributed evenly among the PC). HotCRP supports the same disguising transformations as WebSubmit, but PC users have more data (200–300 records each), and HotCRP's disguising transformations mix deletions and decorrelations across 12 tables.

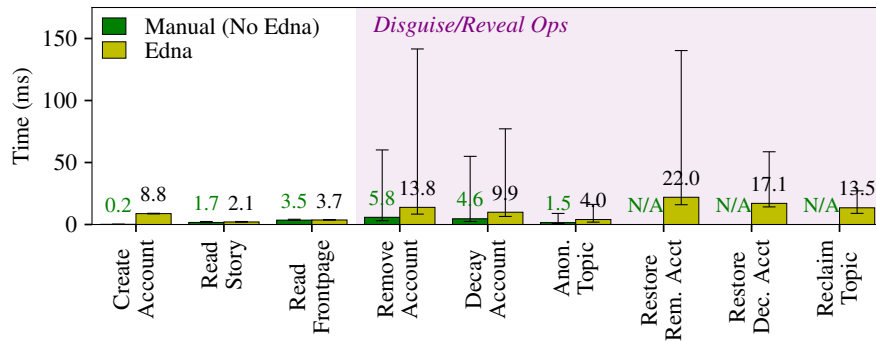
Figure 7-1b shows higher latencies in general, even for the manual baseline, which reflects the more complex disguising transformations. Edna takes 64.4–79.5ms to disguise and reveal



(a) WebSubmit (2k users, 80 answers/user).



(b) HotCRP (80 reviewers, 3k total users, 200–300 records/reviewer).



(c) Lobsters (16k users, Zipf-distributed data/user).

Figure 7-1: Edna adds no latency overhead to common application operations and modestly increases the latencies of disguising operations compared to a manual implementation that lacks support for revealing or composition. Bars show medians, error bars are 5th/95th percentile latencies.

a PC member’s data, again owing to the extra cryptographic operations necessary. HotCRP’s account anonymization is admin-applied and runs for all PC members, so its total latency is proportional to the PC size. With 80 PC members, this transformation takes 6.4s, which is acceptable for a one-off operation. As before, Edna adds small latency to common application operations, and 9ms to account creation.

Lobsters. We run Lobsters benchmarks on a database seeded with 16k users, and 120k stories and 300k comments with votes, comparable to the late-2022 size of production Lobsters [1]. Content is distributed among users in a Zipf-like distribution according to statistics from the actual Lobsters deployment [34], and 20% of each user’s contributions are associated with the topic to anonymize. The benchmark measures server-side latency of common operations and disguising/revealing transformations.

The results are in Figure 7-1c. The median latencies for entire-account removal or decay are small (9.9–13.8ms for Edna, and 4.6–5.8ms for the baseline), since the median Lobsters user has little data. Revealing disguised accounts takes 17.1–22.0ms in the median. Highly active users with lots of data raise the 95th percentile latency to ≈ 150 ms for account removal and 150ms for account restoration. Topic anonymization touches less data and is faster than whole-account transformations, taking 4.0ms and 13.5ms for the median user to respectively disguise and reveal.

Summary. Edna necessarily adds some latency compared to manual, irreversible data removal, since it encrypts and stores disguised data. However, most disguising transformations are fast enough to run interactively as part of a web request. Some global disguising transformations—e.g., HotCRP’s conference anonymization over many users—take several seconds, but an application can apply these incrementally in the background, as in Lobsters account decay.

7.2.1 Edna Performance Drill-Down

We next break down the cost of Edna’s operations into the cost of database operations and the cost of cryptographic operations. Edna’s database operations are fast; in our prototype, they generally take 0.2–0.3ms but vary depending on the amount of data touched. Edna’s cryptographic operations are comparatively expensive. PBKDF2 hashing for private key management incurs a 8ms cost and affects account registration and operations on disguised data that reconstruct a user’s private key; this accounts for up to 79% of these operations’ cost when the operation issues only a few database queries.

Encryption and decryption incur baseline costs of 0.1ms and 0.02ms respectively; their cost grows linearly with data size. In the common case, disguising or revealing data performs two cryptographic operations: one to encrypt/decrypt the diff and speaks-for records, and one to encrypt/decrypt the ID at which they are stored.

Edna also generates a new key for each pseudoprincipal created, which takes 0.2ms. Edna’s cryptography accounts for up to 35% of the cost of disguising/revealing operations such as account removal or anonymization; this proportion decreases as the number of database modi-

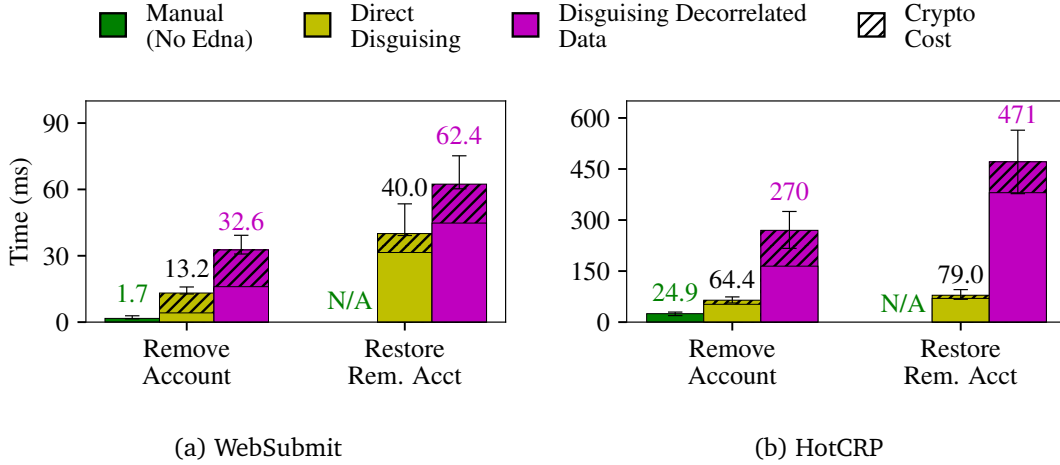


Figure 7-2: Applying disguising transformations to previously-decorrelated accounts increases latency linear in the number of pseudoprincipals involved. Hatched lines indicate the proportion of cost attributed to cryptographic operations.

fications made by a transformation increases. When the application applies multiple disguising transformations and disguises the data of pseudoprincipals, doing so may require several encryptions/decryptions. We evaluate this cost next.

7.2.2 Composing Disguising Transformations.

To understand the overhead of composing transformations in Edna, we measure the cost of composing account removal on top of a prior disguising transformation to anonymize and decorrelate all users' data. We consider WebSubmit and HotCRP, and compare three setups: (i) manual account removal (as before); (ii) account removal and restoration *without* a prior anonymization disguising transformation; and (iii) account removal and restoration *with* a prior anonymization disguising transformation. With prior anonymization, a subset of the user's data has already been decorrelated when removal occurs, and removal therefore performs per-pseudoprincipal encryptions of disguised data with pseudoprincipals' public keys. Restoring the removed, anonymized account must then individually decrypt pseudoprincipal records and restore them. Hence, disguising and revealing in the third setup should take time proportional to the number of pseudoprincipals created by anonymization.

Figure 7-2 shows the resulting latencies. WebSubmit account removal and restoration latencies increase by ≈ 1 ms per pseudoprincipal (19.4ms and 22.4ms respectively); 50% of this increased cost comes from the additional, per-pseudoprincipal encryption and decryption of records, the rest comes from database operations.

HotCRP removal latencies also increase by ≈ 1 ms per pseudoprincipal (205.6ms) and restoration latencies increase by ≈ 2 ms per pseudoprincipal (392.0ms). Again, cryptographic operations add ≈ 0.5 ms per pseudoprincipal, and the remaining cost increase comes from per-pseudoprincipal database queries and updates. Restoration requires more per-pseudoprincipal queries

to e.g., perform consistency checks, resulting in a greater latency increase than in removal. Compared to accounts in WebSubmit, accounts in HotCRP have more data and 14–15× more pseudoprincipals after anonymization, which accounts for the larger relative slowdown and the increased effect of per-pseudoprincipal reveals.

WebSubmit and HotCRP do not create new references to pseudoprincipals after data gets disguised, but if they did, Edna would need to issue additional per-pseudoprincipal queries to rewrite or remove these references (if configured to do so).

Importantly, disguising latencies stabilize when Edna composes further disguising transformations: since cost is proportional to the number of pseudoprincipals affected, latency does not grow once the application has maximally decorrelated data (to one pseudoprincipal per record), as done by HotCRP anonymization.

7.3 Edna Overheads

Edna adds both space and compute overheads to the application; we measure the impact of these next.

7.3.1 Space Used By Edna.

To understand Edna’s space footprint, we measure the size of all data stored on disk by Edna before and after 10% of users in Lobsters (1.6k users) remove their accounts. Cryptographic material adds overhead and each generated pseudoprincipal adds an additional user to the application database; Edna also stores data for each registered principal (a public key and a list of opaque indexes) as well as encrypted records.

Edna’s record storage uses 12 MB, which grows to 58.5 MB after the users remove their accounts, and the application database size increases from 261 MB to 290 MB (+11%). (Edna also caches some of this data in memory.) The space used is primarily proportional to the number of pseudoprincipals produced: each pseudoprincipal requires storing an application database record, a speaks-for record, and row in the principal table. In this experiment, Lobsters produces 78.1k pseudoprincipals. Edna removes the public keys and database data for the 1.6k removed principals, but stores encrypted diff records with their information, which uses another 2.2 MB.

7.3.2 Impact On Concurrent Application Use.

For Edna to be practical, the throughput and latency of normal application requests by other users must be largely unaffected by Edna’s disguising and revealing operations.

We thus measure the impact of Edna’s operations on other concurrent requests in Lobsters. In the experiment, a set of users make continuous requests to the application that simulate normal use, while another distinct set of users continuously remove and restore their accounts.

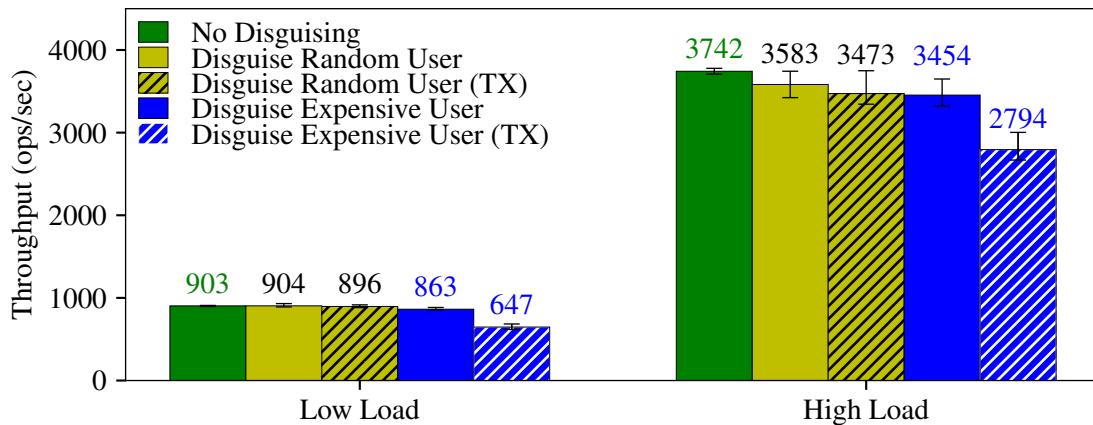


Figure 7-3: Continuous disguising/revealing operations in Lobsters have $<7\%$ impact on application request throughput when disguising a random user; an extreme case of a heavy-hitter user with lots of data repeatedly disguising and revealing causes up to 8% drop in throughput without transactions, and up to 28.3% drop in throughput with transactions.

Edna applies disguising transformations sequentially, so only one transformation happens at a time. We measure the throughput of “normal” users’ application operations, both without Edna operations (the baseline) and with the application continuously invoking Edna. The Lobsters workload is based on request distributions in the real Lobsters deployment [34].

Since users’ disguising/revealing costs vary in Lobsters, we measure the impact of (i) randomly chosen users invoking account removal/restoration, and (ii) the user with the most data continuously removing and restoring their account (a worst-case scenario). We show throughput in a low load scenario ($\approx 20\%$ CPU load), and a high load scenario ($\approx 95\%$ CPU load). Finally, we measure settings with and without a transaction for Edna transformations. A good result for Edna would show little impact on normal operation throughput when concurrent disguising transformations occur.

Figure 7-3 shows the results. If a random user disguises and reveals their data (the common case), normal operations are mostly unaffected by concurrent disguising and revealing: throughput drops $\leq 4.2\%$ without transactions and $\leq 7.2\%$ with transactions (at high load). This shows that Edna’s disguising and revealing transformations have acceptable impact on other users’ application experience in the common case.

Constantly disguising and revealing the user with the most data (the worst-case scenario) has a larger effect, with throughput reduced by up to 7.7% without transactions and up to 28.3% with transactions at both low and high load. This worst-case scenario disguises and reveals a user owning 1% of all the data in a database of 16k users, and demonstrates the upper bound on Edna’s performance impacts when Edna runs large disguising and revealing transactions continuously. Because the queries within disguise and reveal transactions touch 16 tables, all which are commonly read by normal application operations, this impact is expected:

transactions lock any written tables, preventing application operations from reading them until the transaction has completed.

The latency of disguising operations depends on load: on average, disguising and revealing transformations take <100ms. The expensive user’s account removal and revealing take 2.7 and 5.4 seconds under high load. This is acceptable: 50% of data deletions at Facebook take five minutes or longer to complete [17].

7.4 Comparison to Qapla

We compare Edna’s performance and the effort to use Edna to an implementation of the same disguising and revealing functionality for WebSubmit in Qapla.

Effort. Specifying disguising transformations as Qapla policies requires far more explicit reasoning about transformations’ implementations and their compositions. In Qapla, a developer would realize disguising transformations via metadata flags that they add to the schema (e.g., `is_deleted` for removed data) and toggles in application code. They then provision Qapla with a predicate that checks if this metadata flag is `true` before returning a row. Developers must carefully craft Qapla’s predicates, which grow in complexity with the number of disguising transformations that can compose. For example, an application supporting both account removal and account anonymization must combine predicates such that removal always takes precedence. Each additional transformation increases the number of predicates whose combinations the developer must reason about. Developers must also optimize Qapla predicates (e.g., reducing joins, adding schema indexes and index hints) to achieve reasonable performance.

To modify data, the application developer can use Qapla’s “cell blinding” mode, which dynamically changes column values (to fixed values) based on a predicate before returning query results. The developer must manually implement more complex modifications and decorrelation (i.e., creating pseudoprincipals and rewriting foreign keys).

Realizing WebSubmit transformations in Qapla required 576 lines of C/C++, and 110 lines of Rust to add pseudoprincipal, modification, and decorrelation support.

Overall, Qapla requires more developer effort than Edna, particularly in writing composable and performant predicates, and manually implementing modifications and decorrelations. However, Qapla’s approach does make some things easier. Because data remains in the database, revealing simply requires toggling metadata flags, and data to reveal can adapt to database changes (e.g., schema updates). But keeping the data in the database also means that developers cannot use Qapla to achieve GDPR-compliant data removal.

Performance. We measure Qapla’s performance (Figure 7-4) on the same WebSubmit operations (Figure 7-1a). Qapla performs well on operations that require only writes, since Qapla does not rewrite write queries. Removing and restoring accounts requires only a single metadata flag update in Qapla, whereas Edna encrypts/decrypts user data and actually deletes it from the database. However, Qapla rewrites all read queries, so Qapla performs poorly on operations

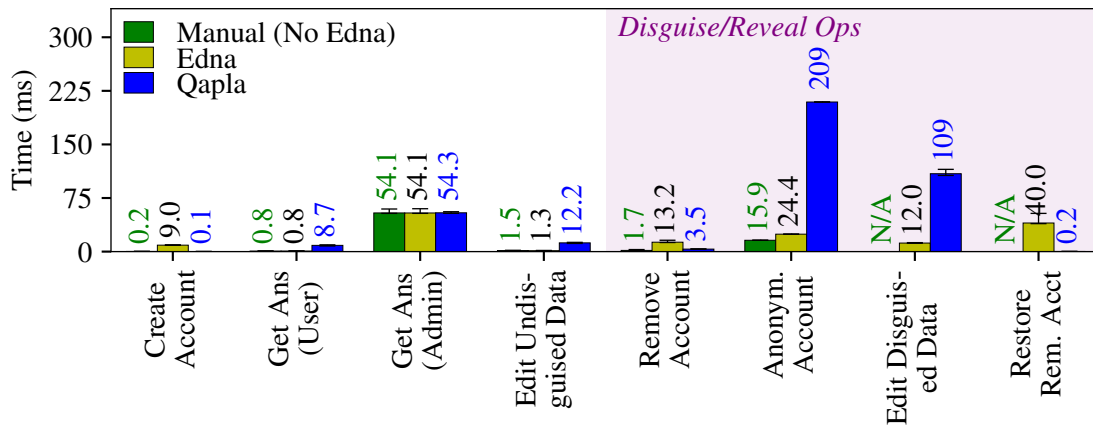


Figure 7-4: Edna achieves competitive performance with a manual baseline and outperforms Qapla on nearly all common WebSubmit operations (2k users, 80 answers/user). Bars show medians, error bars are 5th/95th percentile latencies.

that require reads, such as listing answers and editing (disguised or undisguised) data. Qapla’s query rewriting takes ≈ 1 ms, and rewrites SELECT queries in ways that affect performance (e.g., adding joins to evaluate predicates). Overall, Edna achieves better performance on common operations.

7.5 Edna+CryptDB

We combine Edna with CryptDB to evaluate the cost of composing Edna’s guarantees with those of encrypted databases. CryptDB protects undisguised database contents against attackers who compromise the database server itself (with some limitations [33]), in addition to Edna’s existing protections for disguised data.

Edna+CryptDB operates in CryptDB’s threat model 2 (database server and proxy can be compromised). A developer using Edna+CryptDB deploys the application (and Edna) atop a proxy that encrypts and decrypts database rows. Queries from Edna and the application operate unchanged atop the proxy, but to ensure proper access to user data, the application and Edna must handle user sessions. Edna+CryptDB exposes an API to log users in and out using their credentials. Prior to applying transformations to a user’s data, Edna performs a login to ensure that Edna has legitimate access to their data (e.g., the user, an admin, or someone sharing the data is logged in).

Edna+CryptDB handles keys in the same way as CryptDB: Edna+CryptDB encrypts database rows with per-object keys, and object keys are themselves encrypted with the public keys of the users who can access the object. After a user logs in, the application gives the proxy their private key, thus allowing decryption of their accessible objects.

Our prototype only supports the CryptDB deterministic encryption scheme (AES-CMC en-

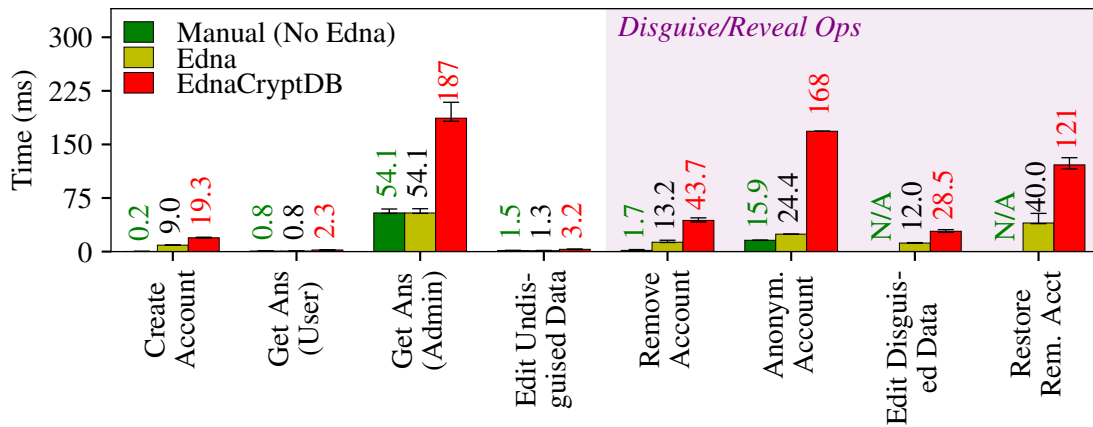


Figure 7-5: Latencies of WebSubmit (2k users, 80 answers/user) operations when implemented with Edna+CryptDB (adding encrypted database support). Bars show median latency; error bars are 5th/95th percentile latencies.

ryption), which limits it to equality comparison predicates. It also does not support joins, a limitation shared with multi-principal CryptDB.

Performance. We measure the latency of WebSubmit operations like before, and compare a manual baseline, Edna, and Edna+CryptDB. Edna+CryptDB is necessarily more expensive than Edna, and a good result for Edna+CryptDB would therefore show moderate overheads over Edna, and acceptable absolute latencies.

Figure 7-5 shows the results. Normal application operations are 2–3× slower with Edna+CryptDB than in Edna, with the largest overheads on operations that access many rows, such as the admin viewing all answers. Disguising and revealing operations are also 2–6× slower than Edna.

These overheads result from the cryptographic operations and additional indirection in Edna+CryptDB. Edna+CryptDB relies on a MySQL proxy, which adds latency: a no-op version of our proxy makes operations 1.03–1.5× slower. Cryptographic operations themselves are cheap (< 0.2ms), but every object inserted, updated, or read also requires lookups to find out which keys to use, query rewriting to fetch the right encrypted rows, and execution of more complex queries.

This is particularly expensive when the user owns many keys (e.g., the WebSubmit admin). Admin-applied anonymization incurs the highest overhead (+143.6ms) as it issues many queries to read user data and execute decorrelations. Among the common operations, an admin getting all the answers for a lecture suffers similar overheads (+132.9ms).

Like CryptDB, Edna+CryptDB increases the database size (4–5× for our WebSubmit prototype). Edna+CryptDB also stores an encrypted object key and its metadata (1KB per key) for each user with access to that object.

Attribute	Normalize URL	Add Story Texts	Add Show Email
Impl Bulk Op	68 LoC	19 LoC	2 LoC
Impl Update	Ø	54 LoC	27 LoC

Figure 7-6: Schema migrations that affect entire tables require writing separate update function for Edna. Applying these updates adds greater overheads per story than per user or per other table row, as more updates apply to the stories table.

7.6 Database Management Operations

If developers perform database management operations, this both increases developer effort and affects Edna’s performance. Here, we answer the following two questions:

1. What categories of bulk management operation can Edna support, and how easily?
2. What are the performance impacts of invoking Edna’s API to record an update, and applying updates during reveal?

7.6.1 Supporting Updates

Developers must already write their management operations today (e.g., Lobsters implements these updates as Ruby Active Record Migrations [59]). However, depending on the type of operation, developers may need to additionally write an update specification for Edna to capture that operation. Operations that execute by affecting entire tables (e.g., via an `ALTER TABLE` command) require writing separate updates which take as input a set of rows instead of an entire table. However, bulk management operations may already operate on a row-level, and thus can be reused as an update specification to Edna.

Our Lobsters implementation implements the selected three bulk operations in Rust instead of Ruby Active Record Migration. Table 7-8 shows the amount of code required per operation, as well as the additional code required to add a corresponding update to give Edna. We reuse the bulk URL normalization operation for the update to Edna; the update requires no additional code. However, we implement the other two schema migrations as bulk table updates, and thus write separate updates that operate on individual rows, taking 54 and 27 LoC respectively. Invoking Edna with the three different application updates and schema migrations for Lobsters required adding one line of code per update that the application calls when performing the bulk operation.

In addition to the updates described and implemented in §6.1, we inspected the 20 most recent management operations in Lobsters from the past three years, and classified them as:

1. a row operation (which can be reused as an update to Edna), such as URL normalization;
2. a table operation (which requires writing a new update for Edna), such as generating tables from other tables (e.g., `textttstory_texts` from `stories`) or altering columns; or
3. an unsupported operation (which cannot be supported as an update with Edna), such as updating the `vote_count` of comments based on the number of votes).

Figure 7-7 shows the distribution of 20 bulk operations among these three categories. Edna can

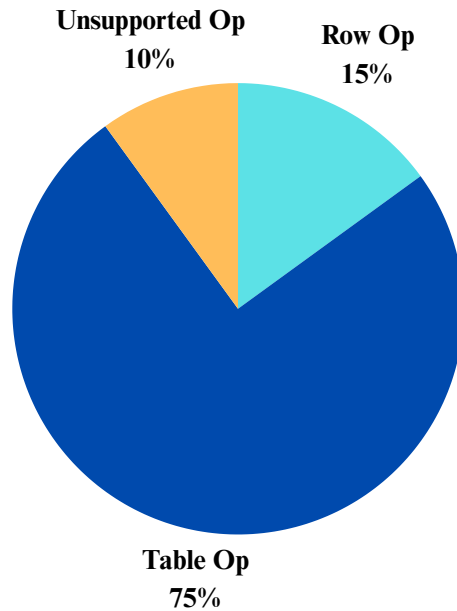


Figure 7-7: Out of the most recent 20 Lobsters database management operations, the majority (75%) are table operations which require developers to write separate update specifications for Edna, 15% are row operations which can be reused as updates without additional effort, and 10% are unsupported because they denormalize the schema in order to cache aggregate results.

Attribute	Normalize URL	Add Story Texts	Add Show Email
Bulk Op	5.63s	5.10s	0.095s
Update 1 story row	0.22ms	0.01ms	0.01ms
Update 1 user row	<0.01ms	0.01ms	0.01ms

Figure 7-8: Schema migrations that affect entire tables require writing separate update function for Edna. Applying these updates adds greater overheads per story than per user or per other table row, as more updates apply to the stories table.

support all operations other than updating rows based on current external database state, unless the update's output is correct no matter the state of other database tables. This represents 2 of the 20 inspected updates. These types of operations might occur in applications that optimize for performance by denormalizing their database schema; we hypothesize that this category of update would not exist with a normalized schema. However, these particular operations also happen to be idempotent for any rows affected, and thus could be reapplied via e.g., a cron job regularly to update revealed data.

For the large majority of database management operations, users can still reveal their data disguised prior to these migrations, as if the migration had occurred with their data present in the database.

7.6.2 Performance of Reveals with Updates

We next look at how bulk operations and updates affect application performance, and how updates affect Edna’s reveal performance. Table 7-8 shows the results.

Bulk Operation Performance. First, as a baseline, we look at the cost of performing bulk operations, which applications incur without Edna.

The URL normalization application update takes 5.63s, the longest of all updates. This matches the optimized bulk operation execution time of 6s in the deployed Lobsters application, which batch updates all stories with the normalized URL. The unoptimized version first implemented by the Lobsters developers updates stories one-by-one, and takes 1789s, requiring them to reimplement via batching. URL normalization modifies all 120k stories.

Adding the `show_email` attribute to the `users` table takes 82ms, as it performs only one query to change the database schema.

Finally, creating and populating the `story_texts` table and removing a column from the `stories` table takes 5.24s. This modifies all 120k stories, and changes the database schema by adding tables and removing columns.

Record Update. Invoking Edna’s hook to insert a new application update in Edna’s replay log takes on average 0.58ms, a negligible amount compared to the time to perform the update/migration. This includes the time to persist the update (one database insert query) and add it to Edna’s in-memory update replay log.

Reveal with Updates. We next evaluate the latency of reveal operations in Lobsters when updates corresponding to the implemented three bulk operations have been applied after reveal.

Apply Update to Diff Record. First, we measure the cost to apply the various updates to diff record rows. Updating stories diff records is the most costly, as both URL normalization and the `story_texts` updates apply: this takes 0.2–0.3ms per story. Diff records for modified or decorrelated stories have both placeholder and original rows. Edna applies updates to both placeholder and original rows, and thus updates take 0.5–0.6ms per stories modify or decorrelate diff record. Initializing a URL normalizer object during the update takes a one-time cost of 0.2ms. Because Edna applies updates to batches of rows of the same table (§5.4), Edna amortizes the cost of URL normalizer initialization by creating a URL normalizer object only once per reveal (when Edna reveals all stories).

Applying all three updates to `users` diff records incurs < 0.1ms per user: the `show_email` update appends a single column to user rows.

The three implemented updates do not affect other row types. However, the implementation of Lobsters’ updates does iterate through all rows to check whether to update them, and each

row iteration takes $\approx 1\mu$. At scale (e.g., for a user with thousands of comments), this cost can add up to a couple milliseconds over the entire reveal.

Restore Updated Diff Record Rows. Next, we measure the cost to restore updated rows to the database compared to the cost to restore rows without updates.¹ Updates do not affect the cost of restoring rows for all tables other than `stories`, since the queries to restore the rows are the same. However, restoring a story now requires additional queries to perform consistency checks for and insert `story_texts` table rows, adding $\approx 0.6\text{ms}$ per story.

Conclusion. As expected, the effects of performing updates increases with the amount of disguised data a user wants to reveal. Users with little data (e.g., less than 5 stories) experience no visible increase in reveal latency with updates, but users with lots of data can experience a small effect (e.g., revealing a user with 673 stories, 1971 comments, and 2000 messages takes on average 4.67s instead of 4.50s, an increase of 3.8%).

7.7 Summary

In our evaluation, we used Edna to add seven disguising transformations to three web applications. We found that the effort required was reasonable, that Edna’s disguising and revealing operations are fast enough to be practical, and that they impose little to moderate overheads on normal application operation depending on the amount of data being disguised or revealed.

check

¹Although restoring updated rows is more expensive than restoring the original rows, the application’s bulk operation would have incurred the cost of updating these rows had the rows not been disguised at the time. Thus, Edna moves the cost of updating these rows to reveal time, rather than bulk operation time (although the cost may be higher because the update is not batched over all table rows).

Chapter 8

Conclusion

This thesis envisions a world in which web services routinely protect, store, and reveal disguised user data with user permission. To move towards this goal, this thesis presents Edna, a system that gives users back flexible privacy controls over their data via data disguising. With Edna, developers can provide data disguising and revealing transformations that give users control over their data in web applications. This thesis illustrates how these transformations help users protect inactive accounts, selectively dissociate personal data from public profiles, and remove a web service's access to their data without permanently losing their accounts; and demonstrates that Edna can support disguised data in real-world applications with reasonable performance. However, Edna is just the beginning. To truly achieve a world in which web applications meet the desired flexible privacy standards, several challenges remain unsolved, which we describe here as future opportunities for research.

8.1 Deploying Disguised Data

Supporting disguised data in web applications that have millions or more users, operate with low cost margins, and/or distribute their compute and storage across multiple regions requires addressing several issues.

Disguised Data Storage. If many (e.g., millions) of users disguise their data over time, disguised data may become too much for applications to store. Even though storage is historically cheap, and applications today willingly store and retain user data nearly indefinitely, eventually disguised data (particularly since it cannot be sold or processed) may burden the application. Edna currently retains disguised data in its disguised table until a user reveals their disguised data, which could be forever if users choose to never reveal data. Instead, Edna could allow applications to put reasonable, coarse-grained time limits (e.g., 10 years) on disguised data to eventually clean it up, without leaking fine-grained information about which data was disguised at the same time.

Deriving Value from Disguised Data. Edna enables an application to keep as much data as possible if users exercise their data protection rights, and to allow users to return to the application. For many applications, this provides a better solution than handling user data deletion requests via permanent user deletion, or decentralized approaches that move all user data out of the application.

However, with Edna, applications store disguised data, but cannot derive value from the now-confidential data. Potentially some clever cryptography such as additive homomorphic secret sharing as done in Zeph [10], may allow Edna to support limited computation such as aggregations over disguised data from which an application can derive value. However, such cryptographic approaches require some initial setup to determine whose data can be aggregated with whose (in order to split the secrets appropriately) and who should be able to reveal the result. Furthermore, defining groups of users whose data can be combined requires more thought into what these groups may reveal about their constituents.

Edna in Large-Scale Applications. Many web services, particularly those at scale, run on machines in various regions and datacenters, and replicate and shard their database. While distributed databases used by these applications (e.g., Spanner [19]) already implement parallel, distributed, and large-scale transactions, Edna’s disguising and revealing transactions may potentially impose high burdens on distributed databases due to the size and frequency of these transactions. For example, Edna may need to handle thousands or more disguising (or revealing) requests per second, and a disguise could touch all database tables.

Today, many applications will already break down large transactions into smaller pieces (at the cost of transactional consistency) or run large transactions in batches overnight to reduce their impact on database performance. Similarly, we can imagine Edna breaking down large disguise and reveal transactions into multiple, per-table transactions, so as to not lock all tables at once; or delaying their execution until night and notifying the user once their disguise or reveal has completed.

8.2 Disguising Beyond Edna: Flexible Access Control

Disguising and revealing in Edna protects disguised data from any external party other than the user themselves. However, disguising and revealing can also apply in more nuanced settings, such as disguising data in different ways to protect from different parties. In these settings, disguising and revealing can offer potential opportunities for more flexible access control to control user data exposure to web application insiders.

As part of a collaboration with Hannah Gross [32], we investigated using disguising abstractions to allow the application to control user data exposure to insiders. Our work draws on the key observation that company employees do not *always* need the user information that they can typically access. Just as Edna allows users to expose their data only while using the application,

perhaps the application can use disguising and revealing to only expose user data to employees when they actually need and use it.

To achieve this goal, we envision a world where every employee operates atop a personalized disguised database that contains the minimum amount of data they need continuously. For example, a hotel customer service representative might only need to be able to look at room occupancy and see free rooms when not actively helping a customer. However, disguised databases would present only the minimal amount of data the employee needs; if, for example, a particular customer needs assistance, the employee currently helping the customer should be able to temporarily reveal parts of their disguised database to dynamically expose that user's data. Different employees simultaneously helping different customers can reveal different disguises to get a partially disguised view of the database individualized for that employee. As soon as the employee no longer needs the user's data, the employee's access returns back to its original, maximally disguised state.

To achieve this flexible access control, we need a database system that applies disguises and dynamically reveals them at a per-employee granularity. A strawman solution might attempt to do so with personalized database views (similar to the proposal in Multiverse DB [44]), but this would require an enormous number of views (potentially one for each employee, and for each reveal the employee requests). Furthermore, just as with Edna, disguises cannot break the database: they would need to handle referential integrity, work even in the presence of indexes and database views, and work with existing query optimizations without overly affecting performance. Employees must also have the ability to flexibly perform fine-grained reveals of their disguised views without compromising security. While Edna's disguising and revealing abstractions can help address some of these challenges (e.g., handling referential integrity with decorrelation), achieving a database system for flexible access control requires solving many new challenges.

8.3 Final Thoughts

Today, user data increasingly lands in the hands of web services, which reduce or remove users' ability to control the privacy of their data as they wish. While Edna represents just one step forward in improving user data privacy on the web, this thesis and Edna thus demonstrate that with disguised data, applications can support flexible privacy features beyond what they offer users today.

Edna provides proof to both web services and regulators that flexible privacy features can be supported with reasonable efforts, and thus can and should be widely implemented and enforced.

Bibliography

- [1] Lobsters. URL <https://lobste.rs>.
- [2] Archita Agarwal, Marilyn George, Aaron Jeyaraj, and Malte Schwarzkopf. Retrofitting gdpr compliance onto legacy databases. *Proc. VLDB Endow.*, 15(4):958–970, dec 2021. ISSN 2150-8097. doi: 10.14778/3503585.3503603. URL <https://doi.org/10.14778/3503585.3503603>.
- [3] Muneeb Ali, Jude Nelson, Ryan Shea, and Michael J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, pages 181–194, Denver, Colorado, USA, June 2016. ISBN 978-1-931971-30-0. URL <https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali>.
- [4] Apple. Apple platform security, April 2023. URL https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.
- [5] Daniel Arkin. Celebrities are starting to leave twitter. here’s a running list. URL <https://www.nbcnews.com/pop-culture/celebrity/twitter-celebrities-leaving-elon-musk-rcna54831>.
- [6] Daniel Augus. Thinking of quitting twitter? here’s the right way to do it. URL <https://economictimes.indiatimes.com/news/how-to/thinking-of-quitting-twitter-heres-the-right-way-to-do-it/articleshow/95696874.cms>.
- [7] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In Colin Boyd, editor, *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, pages 566–582, November 2001.
- [8] T. Berners-Lee, R. Fielding, and L. Masinter. Rfc2396: Uniform resource identifiers (uri): Generic syntax, 1998.
- [9] Kristy Browder and Mary Ann Davidson. The virtual private database in oracle9ir2. *Oracle Technical White Paper, Oracle Corporation*, 500(280), 2002.
- [10] Lukas Burkhalter, Nicolas Küchler, Alexander Viand, Hossein Shafagh, and Anwar Hithnawi. Zeph: Cryptographic enforcement of end-to-end data privacy. In *Proceedings of the 15th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 387–404, July 2021. ISBN 978-1-939133-22-9. URL <https://www.usenix.org/conference/osdi21/presentation/burkhalter>.

- [11] California Legislature. The California Consumer Privacy Act of 2018, June 2018. URL https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.
- [12] Michelle Caruthers. World password day: How to improve your passwords, April 2023. URL <https://blog.dashlane.com/world-password-day/>.
- [13] Tej Chajed, Jon Gjengset, Jelle van den Hooff, M. Frans Kaashoek, James Mickens, Robert Morris, and Nikolai Zeldovich. Amber: Decoupling user data from web applications. In *Proceedings of the 15th Workshop on Hot Topics in Operating Systems (HotOS)*, Kartause Ittingen, Switzerland, May 2015. URL <https://www.usenix.org/conference/hotos15/workshop-program/presentation/chajed>.
- [14] Tej Chajed, Jon Gjengset, M. Frans Kaashoek, James Mickens, Robert Morris, and Nikolai Zeldovich. Oort: User-centric cloud storage with global queries. Technical Report MIT-CSAIL-TR-2016-015, MIT CSAIL, 2016. URL <https://people.csail.mit.edu/nickolai/papers/chajed-oort.pdf>.
- [15] Ramesh Chandra, Priya Gupta, and Nikolai Zeldovich. Separating web applications from user data storage with bstore. In *Proceedings of the 2010 USENIX Conference on Web Application Development (WebApps)*, USA, 2010.
- [16] Adam Chlipala. Static checking of dynamically-varying security policies in database-backed applications. In *Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 105–118, 01 2010.
- [17] Katriel Cohn-Gordon, Georgios Damaskinos, Divino Neto, Joshi Cordova, Benoît Reitz, Benjamin Strahs, Daniel Obenshain, Paul Pearce, and Ioannis Papagiannis. DELF: Safeguarding deletion correctness in online social networks. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security)*, August 2020. URL <https://www.usenix.org/conference/usenixsecurity20/presentation/cohn-gordon>.
- [18] Kate Conger and Lauren Hirsch. Elon musk completes \$44 billion deal to own twitter. URL <https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html>.
- [19] James C. Corbett, Jeffrey Dean, Michael Epstein, Andrew Fikes, Christopher Frost, J. J. Furman, Sanjay Ghemawat, Andrey Gubarev, Christopher Heiser, Peter Hochschild, Wilson Hsieh, Sebastian Kanthak, Eugene Kogan, Hongyi Li, Alexander Lloyd, Sergey Melnik, David Mwaura, David Nagle, Sean Quinlan, Rajesh Rao, Lindsay Rolig, Yasushi Saito, Michal Szymaniak, Christopher Taylor, Ruth Wang, and Dale Woodford. Spanner: Google’s globally distributed database. *ACM Trans. Comput. Syst.*, 31(3), aug 2013. ISSN 0734-2071. doi: 10.1145/2491245. URL <https://doi.org/10.1145/2491245>.
- [20] Kinan Dak Albab, Ishan Sharma, Justus Adam, Benjamin Kilimnik, Aaron Jeyaraj, Raj Paul, Artem Agvastian, Leonhard Spiegelberg, and Malte Schwarzkopf. K9db: Privacy-compliant storage for web applications by construction. In *Proceedings of the 17th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, July 2023.
- [21] Emma Dauterman, Eric Feng, Ellen Luo, Raluca Ada Popa, and Ion Stoica. DORY: An encrypted search system with distributed trust. In *Proceedings of the 14th USENIX Symposium*

- on *Operating Systems Design and Implementation (OSDI)*, pages 1101–1119, November 2020. ISBN 978-1-939133-19-9. URL <https://www.usenix.org/conference/osdi20/presentation/dauterman-dory>.
- [22] Emma Dauterman, Vivian Fang, Ioannis Demertzis, Natacha Crooks, and Raluca Ada Popa. Snoopy: Surpassing the scalability bottleneck of oblivious storage. In *Proceedings of the 28th ACM SIGOPS Symposium on Operating Systems Principles (SOSP)*, page 655–671, 2021. ISBN 9781450387095. URL <https://doi.org/10.1145/3477132.3483562>.
 - [23] Vincent De Beer. Heartbreak and hacking: Dating apps in the pandemic, April 2021. URL <https://securityboulevard.com/2021/04/heartbreak-and-hacking-dating-apps-in-the-pandemic/>.
 - [24] Amol Deshpande. Sypse: Privacy-first data management through pseudonymization and partitioning. In *Proceedings of the 11th Conference on Innovative Data Systems Research (CIDR)*, Chaminade, California, USA, January 2021.
 - [25] Katie Doptis. Podcast: How AWS KMS could help customers meet encryption and deletion requirements, including GDPR, June 2018. URL <https://aws.amazon.com/blogs/security/podcast-how-aws-kms-could-help-customers-meet-encryption-and-deletion-requirements-inc>
 - [26] Dmitry Duplyakin, Robert Ricci, Aleksander Maricq, Gary Wong, Jonathon Duerig, Eric Eide, Leigh Stoller, Mike Hibler, David Johnson, Kirk Webb, Aditya Akella, Kuangching Wang, Glenn Ricart, Larry Landweber, Chip Elliott, Michael Zink, Emmanuel Cecchet, Snigdha aswin Kar, and Prabodh Mishra. The design and operation of CloudLab. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, pages 1–14, July 2019. URL <https://www.flux.utah.edu/paper/duplyakin-atc19>.
 - [27] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L119:1–88, May 2016. URL <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC>.
 - [28] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web (WWW)*, page 657–666, New York, NY, USA, 2007. ISBN 9781595936547. doi: 10.1145/1242572.1242661. URL <https://doi.org/10.1145/1242572.1242661>.
 - [29] Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy, and Henry M. Levy. Vanish: Increasing data privacy with self-destructing data. In *Proceedings of the 18th USENIX Security Symposium (USENIX Security)*, pages 299–316, 2009. URL <http://dl.acm.org/citation.cfm?id=1855768.1855787>.
 - [30] Daniel B. Giffin, Amit Levy, Deian Stefan, David Terei, David Mazières, John C. Mitchell, and Alejandro Russo. Hails: Protecting data privacy in untrusted web applications. In *Proceedings of the 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 47–60, Hollywood, California, USA, October 2012. ISBN 978-1-931971-96-6. URL <https://www.usenix.org/conference/osdi12/technical-sessions/presentation/giffin>.

- [31] GlobalData Thematic Research. Crypto-shredding the best solution for cloud system data erasure, January 2022. URL <https://www.verdict.co.uk/crypto-shredding-gdpr-cloud-systems/>.
- [32] Hannah Gross. Funhouse: A Hall of Mirrors Database, May 2023.
- [33] Paul Grubbs, Thomas Ristenpart, and Vitaly Shmatikov. Why your encrypted database is not secure. In *Proceedings of the 16th Workshop on Hot Topics in Operating Systems (HotOS)*, page 162–168, 2017. ISBN 9781450350686. doi: 10.1145/3102980.3103007. URL <https://doi.org/10.1145/3102980.3103007>.
- [34] Peter Bhat Harkins. Lobste.rs access pattern statistics for research purposes, March 2018. URL https://lobste.rs/s/cqnzl5/lobste_rs_access_pattern_statistics_for#c_hj0r1b.
- [35] Katia Hayati and Martín Abadi. Language-based enforcement of privacy policies. In *Proceedings of the International Workshop on Privacy Enhancing Technologies*, pages 302–313. Springer, 2004.
- [36] Tyler Hunt, Zhiting Zhu, Yuanzhong Xu, Simon Peter, and Emmett Witchel. Ryoan: A distributed sandbox for untrusted computation on secret data. In *Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation (OSDI)*, pages 533–549, 2016. ISBN 978-1-931971-33-1. URL <http://dl.acm.org/citation.cfm?id=3026877.3026919>.
- [37] Zsolt István, Soujanya Ponnappalli, and Vijay Chidambaram. Software-defined data protection: low overhead policy compliance at the storage layer is within reach! *Proc. VLDB Endow.*, 14(7):1167–1174, mar 2021. ISSN 2150-8097. doi: 10.14778/3450980.3450986. URL <https://doi.org/10.14778/3450980.3450986>.
- [38] Burt Kaliski. Pkcs# 5: Password-based cryptography specification version 2.0. Technical report, 2000.
- [39] Eddie Kohler. Hotcrp.com. URL <https://hotcrp.com>.
- [40] Eddie Kohler. Hotcrp.com privacy policy. HotCRP.com, August 2020. URL <https://hotcrp.com/privacy>.
- [41] Robert Krahn, Bohdan Trach, Anjo Vahldiek-Oberwagner, Thomas Knauth, Pramod Bhatotia, and Christof Fetzer. Pesos: policy enhanced secure object store. In *Proceedings of the Thirteenth EuroSys Conference*, EuroSys ’18, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450355841. doi: 10.1145/3190508.3190518. URL <https://doi.org/10.1145/3190508.3190518>.
- [42] Tim Kraska, Michael Stonebraker, Michael Brodie, Sacha Servan-Schreiber, and Daniel Weitzner. Schengendb: A data protection database proposal. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, pages 24–38. Springer, 2019. ISBN 978-3-030-33752-0.
- [43] Maxwell Krohn, Alex Yip, Micah Brodsky, Robert Morris, and Michael Walfish. A World Wide Web Without Walls. In *Proceedings of the 6th ACM Workshop on Hot Topics in Networking (HotNets)*, Atlanta, Georgia, USA, November 2007.

- [44] Alana Marzoev, Lara Timbó Araújo, Malte Schwarzkopf, Samyukta Yagati, Eddie Kohler, Robert Morris, M. Frans Kaashoek, and Sam Madden. Towards multiverse databases. In *Proceedings of the 17th Workshop on Hot Topics in Operating Systems (HotOS)*, pages 88–95, 2019.
- [45] Mastadon gGmbH. Social networking that’s not for sale., 2023. URL <https://joinmastodon.org/>.
- [46] Cecily Mauran. So you want to leave twitter: A wellness plan. URL <https://mashable.com/article/how-to-leave-twitter-guide-elon-musk>.
- [47] Aastha Mehta, Eslam Elnikety, Katura Harvey, Deepak Garg, and Peter Druschel. Qapla: Policy compliance for database-backed systems. In *Proceedings of the 26th USENIX Security Symposium (USENIX Security)*, pages 1463–1479, Vancouver, British Columbia, August 2017. ISBN 978-1-931971-40-9. URL <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/mehta>.
- [48] Richard Mortier, Jianxin Zhao, Jon Crowcroft, Liang Wang, Qi Li, Hamed Haddadi, Yousef Amar, Andy Crabtree, James Colley, Tom Lodge, et al. Personal data management with the databox: What’s inside the box? In *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*, pages 49–54, 2016.
- [49] Mozilla Foundation. Tinder (*privacy not included), March 2021. URL <https://foundation.mozilla.org/en/privacynotincluded/tinder/>.
- [50] Ken Olin. Hey all - i’m out of here. no judgement... URL <https://twitter.com/kenolin1/status/1586031904007954433>.
- [51] Shoumik Palkar and Matei Zaharia. Diy hosting for online privacy. In *Proceedings of the 16th ACM Workshop on Hot Topics in Networks (HotNets)*, pages 1–7, 2017.
- [52] Primal Pappachan, Roberto Yus, Sharad Mehrotra, and Johann-Christoph Freytag. Sieve: A middleware approach to scalable access control for database management systems. *arXiv preprint arXiv:2004.07498*, 2020.
- [53] Pranay Parab. How to make a burner account on reddit, even though they don’t want you to anymore. Lifehacker, January 2022. URL <https://lifehacker.com/how-to-make-a-burner-account-on-reddit-even-though-the-1848336857>.
- [54] Nicole Perlroth, Amie Tsang, and Addam Satariano. Marriott hacking exposes data of up to 500 million guests, November 2018. URL <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html>.
- [55] Raluca Ada Popa, Catherine M. S. Redfield, Nikolai Zeldovich, and Hari Balakrishnan. Cryptdb: Protecting confidentiality with encrypted query processing. In *Proceedings of the 23th ACM Symposium on Operating Systems Principles (SOSP)*, page 85–100, 2011. ISBN 9781450309776. doi: 10.1145/2043556.2043566. URL <https://doi.org/10.1145/2043556.2043566>.
- [56] Raluca Ada Popa, Emily Stark, Jonas Helfer, Steven Valdez, Nikolai Zeldovich, M. Frans Kaashoek, and Hari Balakrishnan. Building web applications on top of encrypted data using mylar. In *Proceedings of the 11th USENIX Conference on Networked Systems Design*

- and Implementation (NSDI), pages 157–172, 2014. ISBN 978-1-931971-09-6. URL <http://dl.acm.org/citation.cfm?id=2616448.2616464>.
- [57] Joel Reardon, Srdjan Capkun, and David Basin. Data node encrypted file system: Efficient secure deletion for flash memory. In *Proceedings of the 21st USENIX Security Symposium (USENIX Security)*, pages 333–348, Bellevue, Washington, USA, August 2012. ISBN 978-1-931971-95-9. URL <https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/reardon>.
 - [58] Shonda Rhimes. Not hanging around for whatever elon has planned. bye. URL <https://twitter.com/shondarhimes/status/1586399694896390147>.
 - [59] Ruby on Rails Guides. Active Record Migrations, 2024. URL https://guides.rubyonrails.org/active_record_migrations.html.
 - [60] Andrei Vlad Sambra, Essam Mansour, Sandro Hawke, Maged Zereba, Nicola Greco, Abdurrahman Ghanem, Dmitri Zagidulin, Ashraf Abounaga, and Tim Berners-Lee. Solid: a platform for decentralized social applications based on linked data. Technical report, MIT CSAIL & Qatar Computing Research Institute, 2016.
 - [61] David Schultz and Barbara Liskov. Ifdb: Decentralized information flow control for databases. In *Proceedings of the 8th ACM European Conference on Computer Systems (EuroSys)*, pages 43–56, April 2013.
 - [62] Malte Schwarzkopf. websubmit-rs: a simple class submission system. URL <https://github.com/ms705/websubmit-rs>.
 - [63] Malte Schwarzkopf, Eddie Kohler, M. Frans Kaashoek, and Robert Morris. Position: Gdpr compliance by construction. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, pages 39–53, Cham, 2019. Springer International Publishing. ISBN 978-3-030-33752-0.
 - [64] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979. ISSN 0001-0782. doi: 10.1145/359168.359176. URL <https://doi.org/10.1145/359168.359176>.
 - [65] Elizabeth Stobert and Robert Biddle. The password life cycle: User behaviour in managing passwords. In *Proceedings of the 10th USENIX Conference on Usable Privacy and Security (SOUPS)*, page 243–255, 2014. ISBN 9781931971133.
 - [66] Yang Tang, Phillip Ames, Sravan Bhamidipati, Ashish Bijlani, Roxana Geambasu, and Nikhil Sarda. CleanOS: Limiting mobile data exposure with idle eviction. In *Proceedings of the 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 77–91, Hollywood, California, USA, October 2012. ISBN 978-1-931971-96-6. URL <https://www.usenix.org/conference/osdi12/technical-sessions/presentation/tang>.
 - [67] The Office of the Privacy Commissioner. New zealand’s biggest data breach shows retention is the sleeping giant of data security, April 2023. URL <https://www.privacy.org.nz/publications/statements-media-releases/new-zealands-biggest-data-breach-shows-retention-is-the-sleeping-giant-of-data-security>

- [68] Patrick Townsend. GDPR, Right of Erasure (Right to be Forgotten), and Encryption Key Management, January 2028. URL <https://info.townsendsecurity.com/gdpr-right-erasure-encryption-key-management>.
- [69] Lillian Tsai, Hannah Gross, Eddie Kohler, Frans Kaashoek, and Malte Schwarzkopf. Edna: Disguising and revealing user data in web applications. In *Proceedings of the 29th Symposium on Operating Systems Principles, SOSP '23*, page 434–450, New York, NY, USA, 2023. Association for Computing Machinery. ISBN 9798400702297. doi: 10.1145/3600006.3613146. URL <https://doi.org/10.1145/3600006.3613146>.
- [70] Harshavardhan Unnibhavi, David Cerdeira, Antonio Barbalace, Nuno Santos, and Pramod Bhatotia. Secure and policy-compliant query processing on heterogeneous computational storage architectures. In *Proceedings of the 2022 International Conference on Management of Data, SIGMOD '22*, page 1462–1477, New York, NY, USA, 2022. Association for Computing Machinery. ISBN 9781450392495. doi: 10.1145/3514221.3517913. URL <https://doi.org/10.1145/3514221.3517913>.
- [71] U.S. Department of Education. Ferpa, August 1974. URL <https://studentprivacy.ed.gov/ferpa>.
- [72] Frank Wang, Ronny Ko, and James Mickens. Riverbed: Enforcing user-defined privacy constraints in distributed web services. In *Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, pages 615–630, Boston, Massachusetts, USA, February 2019. ISBN 978-1-931971-49-2. URL <https://www.usenix.org/conference/nsdi19/presentation/wang-frank>.
- [73] Caity Weaver and Danya Issawi. 'finsta,' explained. The New York Times, September 2021. URL <https://www.nytimes.com/2021/09/30/style/finsta-instagram-accounts-senate.html>.
- [74] Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmett Witchel. Defeating vanish with low-cost sybil attacks against large dhds. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, February 2010. URL <https://www.ndss-symposium.org/ndss2010/defeating-vanish-low-cost-sybil-attacks-against-large-dhds>.
- [75] Jean Yang, Kuat Yessenov, and Armando Solar-Lezama. A language for automatically enforcing privacy policies. *ACM SIGPLAN Notices*, 47(1):85–96, 2012.
- [76] Frances F Yao and Yiqun Lisa Yin. Design and analysis of password-based key derivation functions. In *Topics in Cryptology (CT-RSA): The Cryptographers' Track at the RSA Conference*, pages 245–261, San Francisco, California, USA, 2005. Springer.
- [77] Wen Zhang, Eric Sheng, Michael Chang, Aurojit Panda, Mooly Sagiv, and Scott Shenker. Blockaid: Data access policy enforcement for web applications. In *Proceedings of the 16th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 701–718, Carlsbad, California, USA, July 2022. ISBN 978-1-939133-28-1. URL <https://www.usenix.org/conference/osdi22/presentation/zhang>.