No. 02-322

IN THE
Supreme Court of the United States

DEPARTMENT OF THE TREASURY, BUREAU OF ALCOHOL, TOBACCO AND FIREARMS,
Petitioner,
v.
CITY OF CHICAGO, ILLINOIS,
Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT

BRIEF OF AMICI CURIAE ELECTRONIC PRIVACY INFORMATION CENTER, AND 16 LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF RESPONDENT

DAVID L. SOBEL
Counsel of Record
MARC ROTENBERG
MIKAL J. CONDON
CHRIS JAY HOOFNAGLE
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICI CURIAE

Amicus the Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[1] EPIC has participated as *amicus curiae* in numerous privacy cases, including most recently *Watchtower Bible and Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150 (2002). EPIC frequently requests records under the Freedom of Information Act ("FOIA") concerning government activities that affect privacy interests. EPIC also publishes LITIGATION UNDER THE FEDERAL OPEN GOVERNMENT LAWS (Harry A. Hammitt et al. eds., 2002).

EPIC believes that it was the intent of Congress to maximize both the public's access to government information and to safeguard personal privacy to the greatest extent feasible. This intent is reflected in the original language of the Freedom of Information Act, the subsequent amendments, and regulations issued by agencies pursuant to the Act. In those cases where the Court is asked to consider how to reconcile competing privacy and open government claims, EPIC urges the adoption of policies and techniques that safeguard both interests.

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. Pursuant to Rule 37.6, *amici* state that counsel for *amici* authored the brief with the assistance of EPIC IPIOP Science Policy Fellow Ruchika Agrawal, and that no monetary contributions were made for the preparation or submission of the brief.

LEGAL SCHOLARS

Anita L. Allen, Professor of Law and Philosophy, University of Pennsylvania

James Boyle, William Neal Reynolds Professor of Law, Duke University Law School

Oscar H. Gandy, Jr., Herbert I. Schiller Information and Society Professor, Annenberg School for Communication, University of Pennsylvania

Justin Hughes, Assistant Professor of Law, Cardozo Law School

Peter Jaszi, Professor of Law and Director Glushko-Samuelson Intellectual Property Law Clinic, Washington College of Law

Jerry Kang, Professor of Law, UCLA School of Law

Ian R. Kerr, Canada Research Chair in Ethics, Law & Technology, Faculty of Law, Common Law Section, University of Ottawa

Malla Pollack, Visiting Associate Professor, University of Memphis Law School

Joel R. Reidenberg, Professor of Law, Fordham University School of Law

Daniel J. Solove, Assistant Professor of Law, Seton Hall Law School

David E. Sorkin, Associate Professor of Law, The John Marshall Law School

Peter L. Strauss, Betts Professor of Law, Columbia Law School

Richard C. Turkington, Professor, Villanova University School of Law

TECHNICAL EXPERTS

Dr. Barbara Simons, Past President, Association for Computing Machinery

Dr. Peter G. Neumann, Principal Scientist, SRI International Computer Science Laboratory

Dr. Bruce Schneier, Chief Technical Officer, Counterpane Internet Security

SUMMARY OF THE ARGUMENT

Even if portions of the records responsive to the City of Chicago's request are properly exempt from disclosure under the FOIA, petitioner Bureau of Alcohol, Tobacco and Firearms ("ATF") can provide the City with the requested information by encoding the exempt information. An interpretation of redaction limited to marking out words with a black pen on a hard copy of text is outdated in the modern day world of computer technology, and fails to comply with the Congressional intent underlying recent FOIA amendments. Such an interpretation makes even less sense where it is inconsistent with the agency's own system of information distribution and management. Requiring encoding that conceals personally identifiable information would serve to promote the underlying purpose of the FOIA, while ensuring that the privacy interests of citizens exercising their constitutional rights are not infringed.

ARGUMENT

I. Black Marker Redaction is Inappropriate in an Age of Electronic Record Keeping

Even if ATF demonstrates that disclosure of certain information would interfere with investigative activities or constitute an invasion of personal privacy, ATF can, as the district court found, provide the City with the requested information by "easily 'delet[ing]' the portion which it avers is sensitive, which here is limited to the identity of persons and weapons found in the database, while maintaining the integrity of the remainder of the requested information." *City of Chicago v. United States Dep't of the Treasury,* No. 00-C-3417, 2001 U.S. Dist. LEXIS 24495 at *13 (N.D. Ill. Mar. 6, 2001).

The Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, requires that, "any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." 5 U.S.C. § 552(b). As a result of this requirement, "an agency cannot justify withholding an entire document simply by showing it contains some exempt material." *Krikorian v. Dep't of State*, 984 F.2d 461, 467 (D.C. Cir. 1993). There is a presumption of segregability. *See Mead Data Central, Inc. v. United States Dep't of Air Force*, 566 F.2d 242, 261 (D.C. Cir. 1977); *see generally* LITIGATION UNDER THE FEDERAL OPEN GOVERNMENT LAWS 219-22 (Harry A. Hammitt et al. eds., 2002).

After encoding,[2] the ATF's records would still provide the City with the necessary information to pursue its litigation:

> In order to track the relationship between guns recovered in connection with crime, gun purchasers and gun manufacturers, the City needs to know that a particular individual purchased the recovered weapon, not the identity of that individual. Similarly, the City seeks to analyze the relationship between a particular weapon, and the events and manufacturer related to that weapon, but does not need the exact identifying serial number. In both instances a unique identifier code would serve to separate the sensitive information, from the information regarding trafficking patterns.

City of Chicago, 2001 U.S. Dist. LEXIS 24495 at *14. Although the FOIA does not require the agency to create new records in response to a request, *see NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 161-62 (1975), encoding the segregable information would not constitute the creation of a new record, but rather the retrieval of "information already stored within ATF's databases, in a redacted manner." *City of Chicago*, 2001 U.S. Dist. LEXIS 24495 at *15. Traditional black marker redaction of names and addresses is routinely required under similar circumstances because the remaining information is "reasonably segregable." *See Long v. IRS*, 596 F.2d 362, 366 (9th Cir. 1979), *cert. denied*, 446 U.S. 917

[2] The district court referred to "encryption" of data. *City of Chicago*, 2001 U.S. Dist. LEXIS 24495 at *15. *Amici* here use the word "encoding," which we believe is a more accurate description of the process the district court envisioned.

(1980) (deleting names and addresses did not constitute the production of a new record because the remaining information was "reasonably segregable"); *Walters v. Breaux*, 200 F.R.D. 271, 274 (E.D. La. 2001) (federal employee addresses and Social Security numbers were legitimately exempted under Exemption 7(a); the requested investigative files and reports were therefore ordered redacted and released); *Senate of Puerto Rico v. United States Dep't of Justice*, 1993 U.S. Dist. LEXIS 12162, at *19-36 (D.D.C. Aug. 24, 1993) (requiring agency to redact the name and identifying information of the addressee of a routing slip, which was exempt under Exemption 7(c), and to release the redacted document); *McCullough v. FDIC*, 1980 U.S. Dist. LEXIS 17685 at *9 (D.D.C. July 28, 1980) (In ordering the release of redacted examination reports prepared by state banking commissions, the court ordered that "[t]he FDIC should delete the names and reasonable identifying information and release the portions that it has withheld.").

The Court has not addressed the question of whether the encoding of information deemed to be exempt would constitute the creation of a new document. *Cf. McDonnell v. United States*, 4 F.3d 1227, 1244 (3d Cir. 1993) (court "not persuaded that translation of existing documents would be tantamount to imposing on the Government the burden of creating records").

The district court noted that "[e]ncryption is a modern form of computer deletion for redaction purposes. Encryption deletes sensitive information, such as exact identity, by obscuring it, while retaining useful information." *City of Chicago*, 2001 U.S. Dist. LEXIS 24495 at *15. This Court should follow that reasoning to find that in the digital age, a definition of redaction that requires application of pen to paper no longer complies with the statutory right of the public to receive information, nor does it take into account new methods used by federal agencies in the management of their information systems.

II. Recent Amendments to the FOIA Illustrate Congressional Intent to bring the FOIA into the Digital Age

The passage of the Electronic Freedom of Information Act Amendments of 1996 ("EFOIA"), Pub. L. No. 104-231, 110 Stat. 3048, reinforces the conclusion that traditional methods of redaction are no longer appropriate in an era where government records are routinely stored in electronic formats. Originally enacted in 1966, the FOIA has evolved from a mechanism to accommodate access to agency records maintained in paper form to one where access to agency records is promoted through the use of many different formats. The legislative history of the EFOIA Amendments clearly demonstrates Congress' intent to encourage agencies to make use of new technologies to facilitate public access to government records. The findings contained in the Act expressly encourage innovation in support of open government: "Government agencies should use new technology to enhance public access to agency records and information." Pub. L. No. 104-231 § 2(a)(6).

The 1996 Amendments to the FOIA also demonstrate Congress' desire for agencies to innovate and use new technologies to bring citizens closer to their government. The EFOIA broadened the definition of "record" to include any information maintained by an agency "in any format, including an electronic format." P.L. 104-231 § 3. The House Report accompanying the EFOIA recognized the evolution of records from paper to electronic files, and urged agencies to take advantage of technology to make these records more accessible:

> When the FOIA was enacted agency records were primarily produced on paper. The FOIA's efficient operation requires that its provisions make clear that the form or format of an agency record constitute no impediment public accessibility. Furthermore, the information technology currently being used by executive departments and agencies should be used in promoting greater efficiency in responding to FOIA requests. This objective includes using technology to let requestors obtain information in the form most useful to them.

H.R. Rep. No. 104-795, at 11 (1996).

Additionally, the EFOIA requires agencies to provide information where possible in the format specified by the requester. This provision allows the requestor to receive information "in any form or format" as long as the record is "readily reproducible" in the specified format. P.L. 104-231 § 5. Statements delivered by Members of Congress on the legislation also clearly express an intent to provide information in new formats, and also to use technology to improve access to information. Thus, Rep. Randy Tate, the sponsor of the legislation in the House, argued that new "technological marvels" are bringing the public into the information age, and that "it is only fitting that we now work to use modern-day technology to deliver common-sense efficiency and Government accountability to the American people." 142 Cong. Rec. H10449 (daily ed. Sept. 17, 1996) (statement of Rep. Tate). Similarly, the House Report accompanying the EFOIA noted that the government was increasingly using computers, and that Congress "encourages agencies to use new technology to enhance public access to

Government information." H.R. Rep. No. 104-795, at 19 (1996).

The legislative history demonstrates that the encoding of information to facilitate its disclosure does not constitute the creation of a new record. The Senate report states that the legislation "makes it clear that a search of computerized records that requires application of codes or some form of programming to retrieve information would not amount to the creation of a new record." S. Rep. No. 104-272, at 19 (1996). The use of encoding should thus be viewed, as the district court recognized, as a means of producing the records in a format that retains the links between data without releasing personal identifiers. The FOIA imposes a duty to accommodate a request for such a format as long as the programming and coding necessary to produce such a format is reasonable.

Both the findings and the purpose of the legislation indicate a congressional recognition that traditional definitions were no longer applicable to agency records, since most records are now stored in electronic format. Where, as in this case, segregable information is available upon application of a "readily producible" encoding process, the agency should be required to encode and disclose the information that the agency has withheld. Encoding a document containing segregable data furthers the goal of the EFOIA, that "[a]gencies need to fulfill their responsibilities under the FOIA in a manner that keeps pace with these new technological developments." H.R. Rep. No. 104-795, §12(I)(C)(1996).

III. The Encoding Technique Suggested by the District Court Is Both Technologically Feasible and Easy to Implement

The following technical overview demonstrates that the records responsive to the FOIA request made by the City could be easily encoded to provide the requested information without invading the privacy interests of gun owners or impeding ongoing law enforcement investigations.[3] An illustration of the technical concepts detailed below is provided in Appendix A.

A. Database Basics

A database is a collection of information, or data, organized especially for efficient access. *See* Jeff Ullman & Jennifer Widom, A FIRST COURSE IN DATABASE SYSTEMS 1-2 (2nd ed. 2001). For example, the Yellow Pages is a database organized by category and then alphabetically. A database management system is software that enables persistent storage of data, and allows users to store and manage data efficiently and easily. *Id.* at 1.[4] Petitioner ATF uses an Oracle database management system, R. 76-1 at 98;[5] the

[3] The analysis does not take ATF's exact database schemas into account, since this information is unavailable. However, the conceptual information provided in this analysis does not depend on any particular database schema.

[4] Here, when discussing database management systems, we are focusing on relational database management systems. Relational database management systems present the user with a view of data organized as "tables" or "relations." *See* Ullman & Widom at 4.

[5] The Oracle database management system supports all the features of a relational database management system. *See* Kevin Loney & George Koch, ORACLE 9I: THE COMPLETE REFERENCES 5 (2002)

agency previously used IBM's DB2 database management system, J.A. at 181. Database management systems enable the creation of tables, insertion of data, retrieval of data (via queries, for example), and modification of data. *See* Ullman & Widom at 2.

At a basic conceptual level, data is stored in tables, and a table consists of fields, also referred to as "attributes," along with what type of data is expected to populate each field. *See* Appendix A.

Database management systems also provide support for queries, which serve to retrieve information from the database. Executing queries on a database is analogous to asking questions and receiving responses. Users can also write queries to retrieve only pieces of information. The user can also decide how to label the output to enhance readability. *Id.*

It is important to note that executing queries to retrieve information leaves the database and the data intact; executing queries does not add new data or records, does not delete any data or records, nor modify any data or records. *See* Ullman and Widom at 2-5.

Structured Query Language ("SQL") is the language that many database management systems utilize to interpret user commands for controlling and interacting with the database. *See* James Groff and Paul Weinberg, SQL: THE COMPLETE REFERENCE, SECOND EDITION 4-6 (2002). SQL allows the creation of tables, insertion of data, data modification, deletion of data, retrieval of data, and much more. *Id*. at 5. Here, SQL will be discussed as a data retrieval mechanism.

SQL is vendor independent; leading database management system vendors, including Oracle, IBM (*e.g.*, IBM's DB2) and Microsoft, offer SQL. *Id.* at 8-10. In other words, SQL-based programs, including queries, can be moved from one database management system to another vendor's database management system with minimal conversion effort and little retraining of personnel. *Id.*

B. Redaction in Electronic Databases

Redaction is a very simple matter in the context of information retrieval from database management systems. Here, redaction does not involve actually "blackening out" or "whiting out" information by hand, nor does it involve the actual deletion of information. Instead, redaction is a matter of simply not selecting information. For example, if a user wanted the data contained in a so-called Individuals table but without first names and last names, the user would simply not specify the retrieval of first names and last names. *See* Appendix A.

In this respect, redaction in the electronic record-keeping environment may be thought of as a *logical* deletion, or logically "whiting out" information. *See* Appendix A. However, the actual data contained in the Individuals table remains intact.

C. Concealing Data

"Scrambling data" means to disarrange the data elements in order to make it unintelligible to interception. Microsoft ENCARTA COLLEGE DICTIONARY 1298 (2001). "Encoding data" means to convert it from one system of communication into another, while "decoding" means to convert an encoded message back into intelligible form. *Id*. at 373, 471. There are a number of ways to encode or scramble data. For example, to scramble data outputted from the Individuals table, an SQL query could be written to convert FirstName and LastName into numbers, concatenating year of birth, and then applying some mathematical function to the resulting number (*e.g.*, adding 100). A number of built-in functions are available to format or scramble output data. Some database management systems even provide built-in functions for the specific purpose of encoding and decoding information.

Encryption is the process of disguising content in such a way as to hide or conceal its substance.[6] Similarly, some database management systems also provide built-in functions that can be utilized to encrypt information.[7]

D. Encoding the Data Requested by City of Chicago

The City of Chicago requested information that would reveal that an unnamed individual purchased a known quantity of guns, which were recovered in Chicago. *City of Chicago*, 2001 U.S. Dist. LEXIS 24495 at *13-14. A query can be easily written to retrieve this information without revealing any personally identifiable information at all. *See* Appendix A. Therefore, consistent with the Congressional intent underlying recent amendments to the FOIA, the Court should find that petitioner ATF is required under the FOIA to encode the requested data to remove any information that would be properly exempt from disclosure, and to release the encoded records to the City.

[6] *See generally* Bruce Schneier, APPLIED CRYPTOGRAPHY (2nd ed., 1996); and Whitfield Diffie & Susan Landau, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION (1998) for an extensive discussion of the development and use of encryption.

[7] Oracle is very advanced in this respect, offering special functions (such as DESEncrypt, DES3Encrypt, etc.) to encrypt data. Peter Wayner, TRANSLUCENT DATABASES 23 (2002). Decryption functions are also available, and decryption is possible when the decryption key is available.

CONCLUSION

Even if portions of the City of Chicago's request are properly exempt from disclosure under the FOIA, ATF can provide the City with the requested information by encoding the exempt portions while retaining the integrity of the remainder of the requested information. In interpreting the FOIA in this way so as to encourage access to information while preserving privacy, the Court would be faithful to the language of the Act and the intent of Congress in the new context of pervasively used electronic databases. The definition of redaction propounded by petitioner ATF is outdated in the modern day world of computer technology and is inconsistent with ATF's own system of information distribution and management. We believe that the solution discussed here, a technologically simple process, hews closely to the purpose of the Act and the legislative intent. The Court should thus require the encoding suggested by the district court and the release of the information requested by the City of Chicago.

Respectfully submitted,

DAVID L. SOBEL
Counsel of Record
MARC ROTENBERG
MIKAL J. CONDON
CHRIS JAY HOOFNAGLE
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140

COUNSEL FOR *AMICI CURIAE*

February 5, 2003

APPENDIX A

I. Database Basics

This Appendix illustrates the technical concepts described in the Brief of *Amici*, Section III, pp. 10-13. [8]

A. Data Storage in Tables

As an illustrative and intuitive example, a database could have an "Individuals" table,[9] which could be depicted as:

FirstName (text)	**LastName (text)**	**DateOfBirth (date)**	**CityOfBirth (text)**	**…**
Jane	Doe	12-January-1965	Newark	…
John	Smith	25-August-1974	Menlo Park	…
Sally	Smith	3-November-1955	Skokie	…
…	...	…	…	…

In this example, the Individuals table has the following fields: FirstName, LastName, DateOfBirth, CityOfBirth, etc. The

[8] The information contained within this Appendix is discussed at length in the following reference materials: Jeff Ullman & Jennifer Widom, A FIRST COURSE IN DATABASE SYSTEMS (2nd ed., 2001); James Groff & Paul Weinberg, SQL: THE COMPLETE REFERENCE, SECOND EDITION (2002); Peter Wayner, TRANSLUCENT DATABASES (2002); and Kevin Loney & George Koch, ORACLE9I: THE COMPLETE REFERENCE (2002).

[9] The transcript of the district court proceedings, J.A. at 181, describes an Individuals table. Although the testimony was given by plaintiff's expert witness, Gerald A. Nunziato, who worked on ATF's DB2 database, the Individuals table may still be implemented in the Oracle system. However, the specific table is irrelevant as the concepts illustrated are interchangeable.

FirstName field accepts data in text format and interprets any data entered for this field as text; so if a user were to enter the number five, the database management system would interpret it as the text "5" as opposed to the number five (so, a user would not be able to apply mathematical operations on it). As another example, the DateOfBirth field accepts dates only; so if a user were to attempt to enter "cat" for the DateOfBirth field for a particular person, the database management system would not be able to interpret "cat" as a date, report an error, and not accept the entry.

A row in the Individual database represents a data instance, referred to as a "record." For example, the second row represents an individual named "Jane Doe" who was born on 12-January-1965 in Newark. The third row represents an individual named "John Smith" who was born on 25-August-1974 in Menlo Park.

II. Queries

A. Basic Queries

For the example of the Individuals table, a user could query the database to see if an individual with the last name "Smith" exists in the Individuals table; the query would respond with all individuals with the last name of "Smith." In this case, it would respond with Sally Smith and John Smith.

The SQL query might look like the following:

```
SELECT FirstName, LastName
FROM Individuals
WHERE LastName='Smith'
```

This query command tells the database management system to retrieve a list containing first names and last names of all people in the Individuals database with the last name of Smith. In other words, this query command may be understood as asking the database if there are any individuals in the Individuals table who have the last name of "Smith"; if so, return all such individuals' first names and last names. The output would look like:

```
FirstName      LastName
------------   ------------
John           Smith
Sally          Smith
```

By contrast, a user could query the database to see if an individual with the last name "Osbourne" exists in the Individuals table by executing the following query:

```
SELECT FirstName, LastName
FROM Individuals
WHERE LastName='Osbourne'
```

The output would look like:

```
FirstName      LastName
------------   ------------
```

Such an empty list indicates that there are no individuals with the last name "Osbourne" in the Individuals table.

B. Selecting Output Data and Formatting Output

Users can also write queries to retrieve only pieces of information. At one level, users can query for certain fields, *e.g.*, FirstName and LastName. At another level, users can query for pieces of information within a field, *e.g.*, the first letters of an individuals FirstName and LastName.

The user can also decide how to label the output to enhance readability, *e.g.*, the user can label the output columns as "FirstNameInitial" and "LastNameInitial" as opposed to "Column 1" and "Column 2".

As an example, if a user wanted to get a list of initials of all individuals in the Individuals table, the user could use the following query:

```
SELECT
SUBSTRING(FirstName, 1, 1)
AS FirstNameInitial,
SUBSTRING(LastName, 1, 1)
AS LastNameInitial
FROM Individuals
```

Some database management systems, including Oracle, support the SUBSTRING function (Oracle refers to the function as "SUBSTR", abbreviated for "substring") that a user can easily utilize. As a brief explanation, SUBSTRING (FirstName, 1, 1) says, "For each name listed under the FirstName column, output the letters located from the first position of the name continuing for one character," which thereby outputs the first letter of the name. By contrast, SUBSTRING (FirstName, 1, 2) says, "For each name listed under the FirstName column, output the letters located from the first position of the name continuing on for two characters," which thereby outputs the first two letters of the name.

The "AS FirstNameInitial" part of the query says, "Call or label this output column 'FirstNameInitial'". The query would output:

```
FirstNameInitial      LastNameInitial
--------------------  -------------------
J                     D
J                     S
S                     S
```

III. Concealing Data

A. Scrambling Data

There are a number of ways to scramble data. Here, this topic may be considered an advanced topic of formatting output, since the queries discussed below will scramble output data, while leaving the database data intact.

For example, to scramble data outputted from the Individuals table, a SQL query could be written to convert FirstName and LastName into numbers, concatenating (that is, attaching) year of birth, and then applying some mathematical function to the resulting number (*e.g.*, adding 100). A number of functions are available to scramble output data.

As a simple example, Oracle offers the TRANSLATE function. For example, to scramble first names outputted from the Individuals table, one could write the following query:

```
SELECT
TRANSLATE(FirstName,
'abcdefghijklmnopqrstuvwxyz',
'somearbitrarystringofsamel')
FROM Individuals
```

This query says, "For each name listed under the FirstName column, and then for each letter in the name, if the letter appears in 'abcdefghijklmnopqrstuvwxyz', replace that letter with the letter in the same position as in 'somearbitrarystringofsamel'". For example, for the name "jane", the letter 'j' appears in 'abcdefghijklmnopqrstuvwxyz' in the 10th position. The corresponding letter in the 10th position of 'somearbitrarystringofsamel' happens to be 'r'. Applying this logic for 'a', 'n' and finally 'e', "jane" becomes scrambled as "rssa".

B. Encrypting Data

Some database management systems provide functions for the specific purpose of encoding and decoding data. Reverting to the Individuals table example, a user could write the following query:

```
SELECT
ENCODE(FirstName, "password"),
ENCODE(LastName, "password"),
DateOfBirth, CityOfBirth
FROM Individuals
```

This query would output the FirstName and LastName of all individuals in the Individuals table as encoded with the supplied password. The data could be decoded, given that the decoder has access to the password used to originally encode the data.

Some database management systems also provide functions that can be utilized to encrypt data. Oracle is very advanced in this respect, offering special functions (*e.g.*, DESEncrypt, DES3Encrypt, etc.) to encrypt data.

Reverting to the Individuals table example, a user could write the following query:

```
SELECT
DESENCRYPT(FirstName, somekey),
DESENCRYPT (LastName, somekey),
DateOfBirth, CityOfBirth
FROM Individuals
```

This query would output the FirstName and LastName of all individuals in the Individuals table in encrypted form.

Please note that decryption functions are also available, and decryption is possible only when the decryption key is available.

C. An Example of Redaction Applied to City of Chicago's Request

Suppose that the Trace Database has a "RecoveryLocation" table,[10] which could be depicted as the following:

RecoveredWeaponID	**StreetName**	**City**	**State**	**…**
1	StreetName1	Chicago	IL	…
2	StreetName2	Newark	NJ	…
3	StreetName3	Chicago	IL	…
4	StreetName4	Chicago	IL	…
5	StreetName5	Baltimore	MD	…
…	…	…	…	…

[10] Datatypes have not been included to facilitate a simple discussion.

Also, suppose the database has a "Trace" table that lists which individuals purchased which weapons. The table could be depicted as the following:

Individual	**WeaponID**	**…**
X	1	…
Y	2	…
X	3	…
Y	4	…
Y	5	…
…	…	...

The built-in data summary COUNT function may be used to count the number of elements in a group. For example, the following query would answer the question that particular individuals purchased some number of guns, which were recovered in Chicago:

```
SELECT COUNT(Trace.Individual) AS
NumberOfPurchasesByAnIndividual,
RecoveryLocation.City
FROM RecoveryLocation, Trace
WHERE
Trace.WeaponID=RecoveryLocation.Recov
eredWeaponID
AND RecoveryLocation.City='Chicago'
GROUP BY Trace.Individual,
RecoveryLocation.City
```

An intermediate, though not displayed, step may look like:

```
Trace.Individual WeaponID RecoveryCity
-------------------- ------------- -----------------
X                    1            Chicago
X                    3            Chicago
Y                    4            Chicago
```

Then for each element under Trace.Individual, the COUNT function counts how many times the element appears. For example, X appears twice while Y appears once. The output might look like:

```
NumberOfPurchasesByAnIndividual  RecoveryCity
---------------------------------------------  -----------------
2                                               Chicago
1                                               Chicago
```

In other words, one particular individual purchased 2 guns, which were recovered in Chicago. Another individual purchased 1 gun, which was recovered in Chicago.

Note that the information was retrieved without disclosing any personally identifiable information.