

# Exploring Best Practices for Protecting Sensitive Data using Oracle Data Redaction

**Ami Aharonovich**  
Oracle ACE Director   
[Ami@DBAces.com](mailto:Ami@DBAces.com)

# About Me

- Oracle ACE Director  
- Oracle Certified Professional DBA (OCP) 
- Founder and CEO, DBAces
- President, Israel Oracle User Group 
- Ambassador, EMEA Oracle User Group Community 
- Oracle DBA consultant and instructor, specializing in Oracle database core technologies
- Frequent speaker at Oracle events and user group conferences around the globe

# ORAWORLD

e-Magazine for Oracle Users published by the EOUC

E-magazine

**for Oracle users around the world**

Published

**by the EMEA Oracle Usergroup  
Community (EOUC)**

Comes with

**exciting stories and  
interesting infographics from  
the Oracle cosmos**

And the best thing:

**it's free!**

As a member of the EOUC,  
we take part in ORAWORLD.  
Join us!

EOUC  
EMEA  
ORACLE  
USERGROUP  
COMMUNITY



Subscribe now for free to receive the next issue via e-mail!

Share your story and submit your own articles, ideas and events.



# Previous Highlights





# Oracle Database 18c XE

## "Free Oracle Database for Everyone"

- Same powerful Oracle Database with a full-featured experience
- Use in any environment, plus the ability to embed and redistribute – free!
- What is included:
  - Multitenant (multiple Pluggable Databases inside your Multitenant Container Database)
  - In-Memory (to support real-time analytics using In-Memory column store)
  - Partitioning
  - Advanced Analytics (Data Mining SQL, R programming and the Oracle Data Miner UI)
  - Advanced Security (TDE and Data Redaction)
- Resources – up to: 12GB of user data, 2GB DB RAM, 2 CPU threads, 3 PDBs

<https://www.oracle.com/database/technologies/appdev/xe.html>

# Agenda

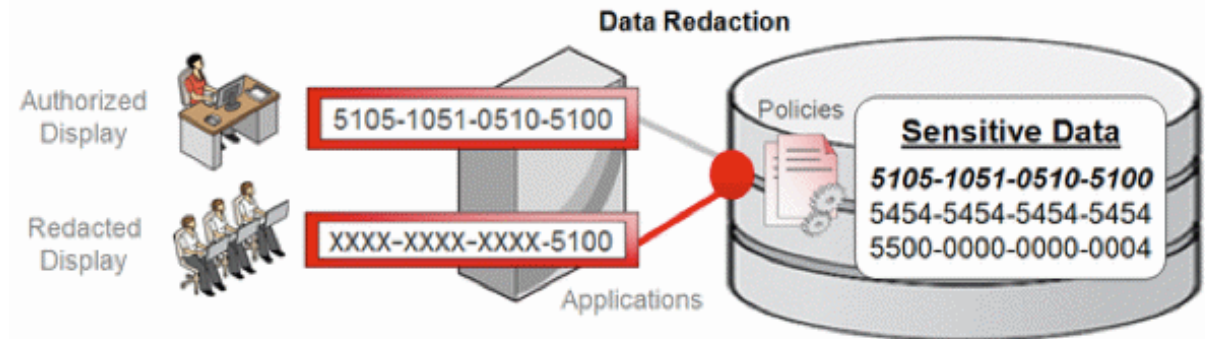
- Oracle Data Redaction – What? Why? When?
- Redaction Policy
- Redaction Methods:
  - Full Redaction
  - Partial Redaction
  - Random Redaction
  - Regular Expression
- Guidelines
- Live Demo

# What is Oracle Data Redaction?

- Oracle Data Redaction enables you to mask (redact) data that is returned from queries issued by applications
- Database applies the redaction at runtime
- Works well in a production system
- Helps you to comply with industry regulations such as GDPR and Payment Card Industry Data Security Standard (PCI DSS)
- Introduced in Oracle Database 12c R1

# When to Use Oracle Data Redaction?

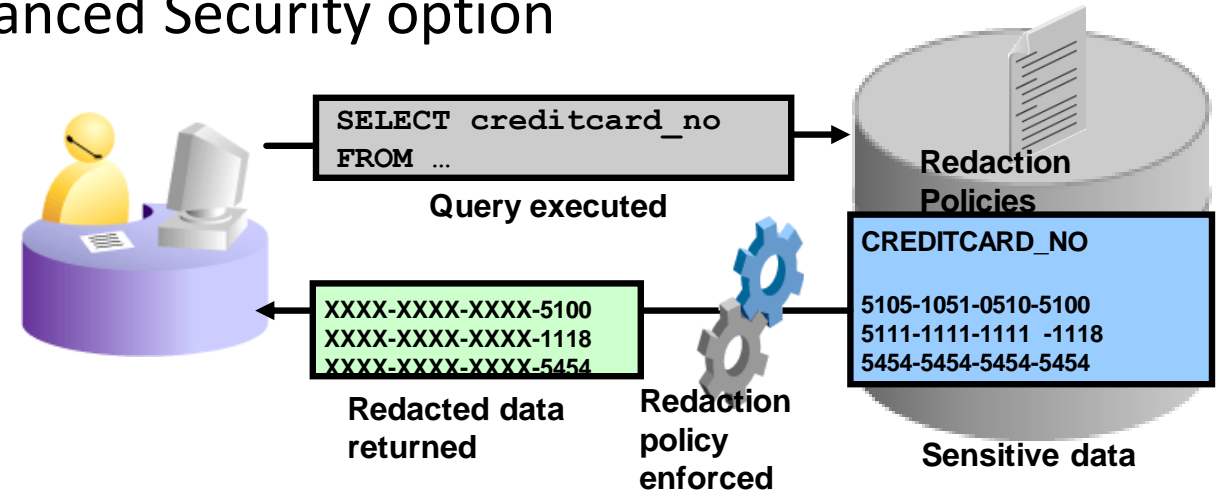
- Ideal for situations in which you must redact specific characters out of the result set of queries of personally identifiable information returned to certain application users
- Particularly suited for call center/other types of applications that are read-only
- Oracle Data Redaction is **NOT** designed to prevent data exposure to database users who run ad hoc queries directly against the database





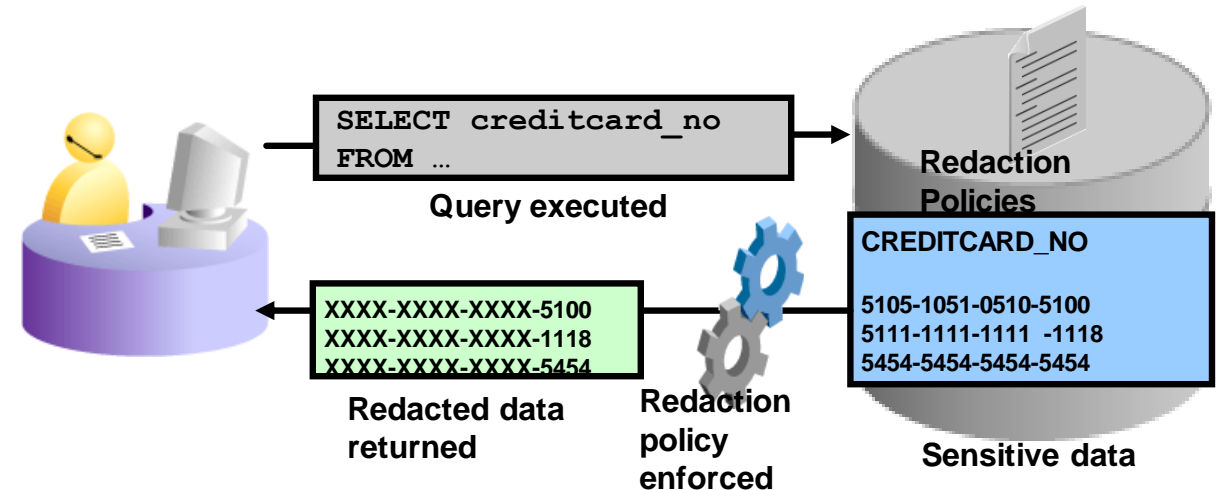
# Oracle Data Redaction: Overview

- Prevent display of sensitive data to end users
- Transparent, flexible and simple solution
- Modifies sensitive data columns contained in SQL query results dynamically before results returned to applications
- Redaction preserves returned column data type and format
- Enterprise Edition, requires Oracle Advanced Security option



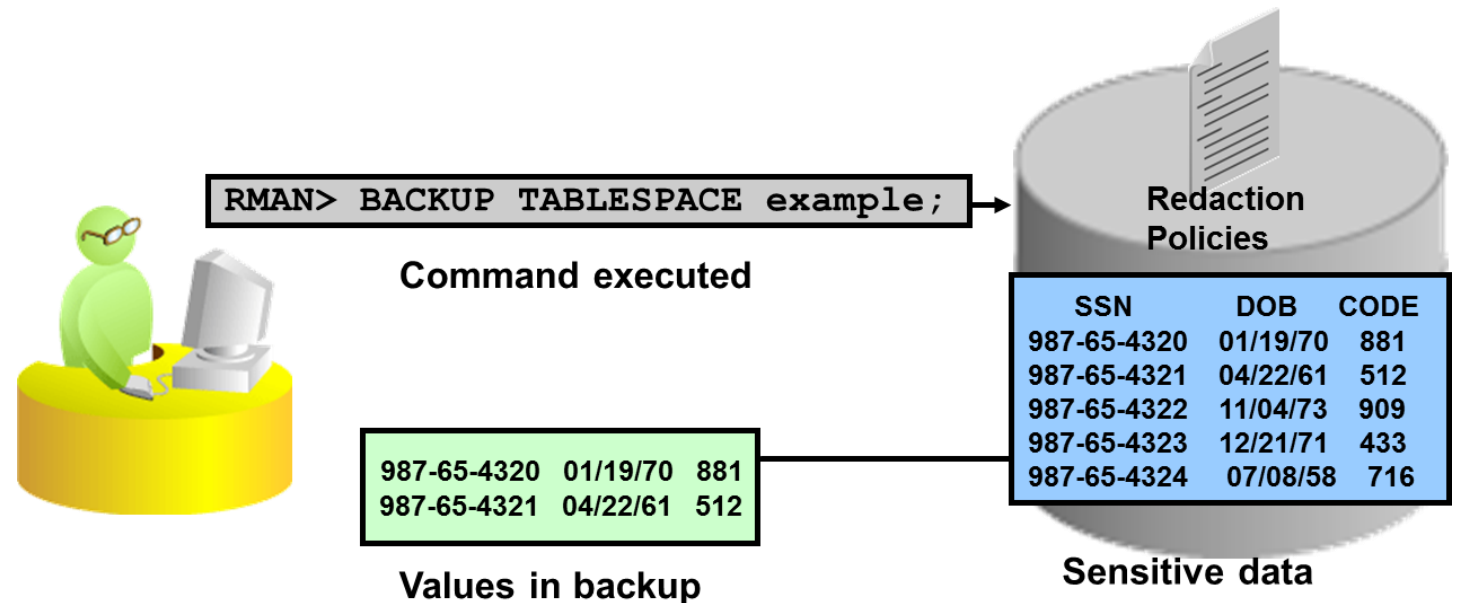
# Oracle Data Redaction: Overview

- Data is redacted according to flexible policies that provide conditional redaction
- Policies are managed directly within the database
- Does not alter underlying data blocks on disk or in cache
- No measurable impact on production workloads
- Embedded in the database system



# Data Redaction and Operational Activities

- SYS user is always exempted from redaction policies
- Operational activities that are not subject to redaction:
  - Backup and restore
  - Import and export
  - Patching and upgrades
  - Replication



## Available Redaction Methods

Type	Description
None	No redaction is performed
Full	Columns are redacted to constant values based on the column data type
Partial	User-specified positions are replaced by a user-specified character
Random	Data type is preserved and different values are output each time
Regular Expression	A “match and replace” based on parameters is performed



# Available Redaction Methods: Examples

Data in the Database > Redacted Values		
Full Redaction	05/24/75 11 Rock Bluff Drive	→ 01/01/01 → xxxxxxxxxx
Partial Redaction	068-35-2299 D1L86YZV8K	→ ***-**-2299 → D1*****8K
Regular Expression Redaction	94025-2450 Tom.Lee@acme.com	→ 94025-[hidden] → [redacted]@acme.com
Random Redaction	6011111111111117 09/30/73	→ 4222222222222226 → 11/30/85

# Redaction Policy – What, How and When?

- What = schema name, object name, column name
- How = function type, function parameters (or regular expression parameters)
- When = policy expression
- Restrictions:
  - Cannot redact SYS or SYSTEM schema objects
  - Cannot redact virtual columns
  - Cannot redact columns of specific data types

# Managing Redaction Policies

Use DBMS\_REDACT package to manage redaction policies  
(must be granted the EXECUTE privilege for the package):

- ADD\_POLICY = add redaction policy to a table
- DROP\_POLICY = remove redaction policy from a table
- ALTER\_POLICY = change redaction policy
- DISABLE\_POLICY = disable redaction policy
- ENABLE\_POLICY = enable redaction policy after it is disabled

## Full Redaction: Example

Use full redaction (default) to redact the returned data to a fixed value:

- Characters = single black space
- Numbers = single zero
- Datetime = first of January 2001

Find current values in: REDACTION\_VALUES\_FOR\_TYPE\_FULL

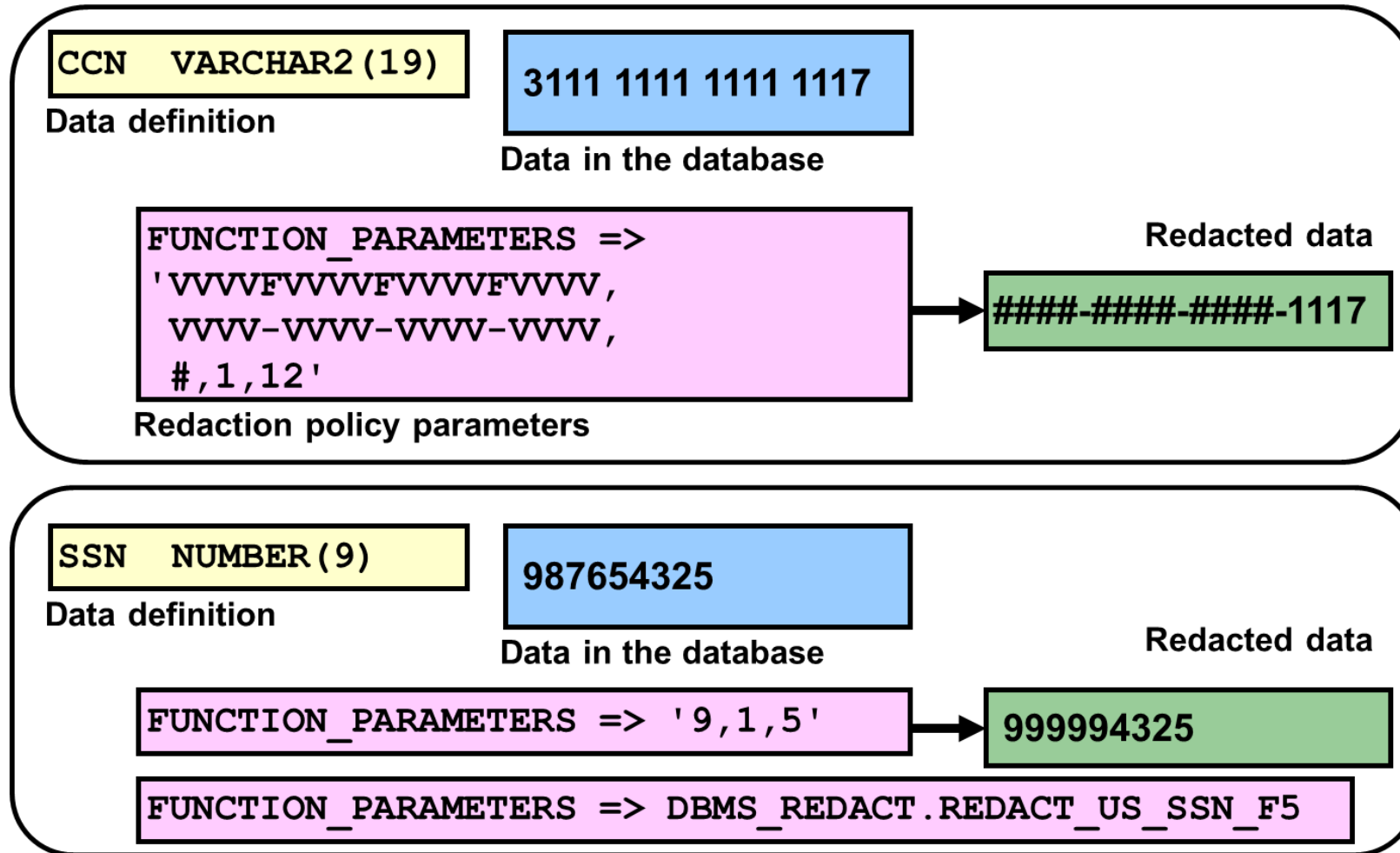
Data definition	Data in the database	Redacted data
SSN VARCHAR2 (11)	987-65-4320 987-65-4321	' ' ' '
SSN NUMBER (9)	987654322 987654323	0 0
HIREDATE DATE	12-AUG-02 19-NOV-02	01-JAN-01 01-JAN-01



## Partial Redaction: Example

- Use function\_type => DBMS\_REDACT.PARTIAL
- Specify parameters so that a portion of the data is redacted and part of the original data is preserved
- F = format characters, where to insert formatting characters
- V = values, redaction character that should be used and the values that should be redacted
- For numbers = specify only numbers 0 through 9
- For dates = lowercase letters indicate month, day, year, hour, minute and second, uppercase letters indicates no redaction should be performed

# Partial Redaction: Example



## Partial Redaction: Fixed Character Shortcuts

- You can use parameter shortcuts for commonly redacted Social Security Numbers, postal codes, and credit cards that use either the VARCHAR2 or NUMBER data types

Shortcut	Description
DBMS_REDACT.REDACT_US_SSN_F5	Redacts the first 5 numbers of Social Security numbers when the column is a VARCHAR2 data type
DBMS_REDACT.REDACT_US_SSN_L4	Redacts the last 4 numbers of Social Security numbers when the column is a VARCHAR2 data type
DBMS_REDACT.REDACT_US_SSN_ENTIRE	Redacts the entire Social Security number when the column is a VARCHAR2 data type
DBMS_REDACT.REDACT_NUM_US_SSN_ENTIRE	Redacts the entire Social Security number when the column is a NUMBER data type
DBMS_REDACT.REDACT_ZIP_CODE	Redacts a 5-digit postal code when the column is a VARCHAR2 data type
DBMS_REDACT.REDACT_NUM_ZIP_CODE	Redacts a 5-digit postal code when the column is a NUMBER data type
DBMS_REDACT.REDACT_DATE_MILLENNIUM	Redacts dates that are in the DD-MON-YY format to 01-JAN-00
DBMS_REDACT.REDACT_CCN16_F12	Redacts a 16-digit credit card number, leaving the last 4 digits displayed

## Regular Expression: Example

- Use function\_type => DBMS\_REDACT.REGEXP
- REGEXP\_PATTERN = regular expression that represents column data that will be redacted and describes the pattern of data that must be matched
- REGEXP\_REPLACE\_STRING = define how data should be replaced
- REGEXP\_POSITION = indicate the starting position for the string search
- REGEXP\_OCCURENCE = specify how the search and replace operation is to be performed
- REGEXP\_MATCH\_PARAMETER = specify text literal to change the default matching behavior of the function



# Regular Expression: Example

**SSN VARCHAR2(11)**

Data definition

987-65-4325  
987-65-4326

Data in the database

```
REGEXP_PATTERN=  
' (\d\d\d) - (\d\d) - (\d\d\d\d) ',  
REGEXP_REPLACE_STRING=  
' XXX-XX-\3 ',  
REGEXP_POSITION=1,  
REGEXP_OCCURRENCE=0,  
REGEXP_MATCH_PARAMETER=' i '
```

Redaction policy parameters

XXX-XX-4325  
XXX-XX-4326

Redacted data

## Regular Expression: Example

- You can use shortcuts for both the REGEXP\_PATTERN and REGEXP\_REPLACE\_STRING parameters in the DBMS\_REDACT.ADD\_POLICY procedure:

REGEXP_PATTERN	REGEXP_REPLACE_STRING
DBMS_REDACT.RE_PATTERN_ANY_DIGIT	DBMS_REDACT.RE_REDACT_WITH_SINGLE_X
DBMS_REDACT.RE_PATTERN_US_PHONE	DBMS_REDACT.RE_REDACT_US_PHONE_L7
DBMS_REDACT.RE_PATTERN_EMAIL_ADDRESS	RE_REDACT_EMAIL_NAME RE_REDACT_EMAIL_DOMAIN RE_REDACT_EMAIL_ENTIRE
DBMS_REDACT.RE_PATTERN_IP_ADDRESS	RE_REDACT_IP_L3

# Data Redaction General Usage Guidelines

- Choose the columns to redact selectively, redact only what is needed
- Keep the policy expression logic as simple as possible
- When you are defining regular expression policies, keep the regular expressions simple
- Partial and full redaction policies generally provide better performance than regular expression policies that must be compiled each time they are used
- You can apply only one policy on a table or view

# Data Redaction General Usage Guidelines

- CREATE TABLE AS SELECT and INSERT AS SELECT are blocked by default. You can grant EXEMPT REDACTION POLICY to disable this behavior
- Oracle Data Redaction is not intended to protect against:
  - Attacks by regular and privileged database users who run ad hoc queries directly against the database
  - Users who run ad hoc SQL queries that attempt to determine the actual values by inference
- Redaction is not enforced for users who are logged in using the SYSDBA administrative privilege

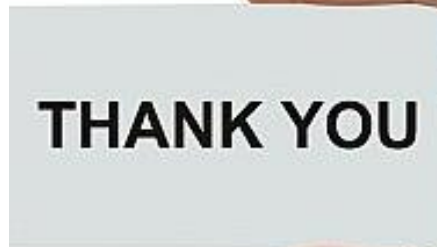


# Static Data Masking

## Oracle Data Masking and Subsetting Pack

- Helps database customers improve security and accelerate compliance by sanitizing copies of production data for testing, development, and other activities
- Enables entire copies or subsets of application data to be extracted from the database, obfuscated, and shared with partners inside/outside of the business
- The integrity of the database is preserved assuring continuity of the applications





THANK YOU

# Exploring Best Practices for Protecting Sensitive Data using Oracle Data Redaction

**Ami Aharonovich**  
Oracle ACE Director   
[Ami@DBAces.com](mailto:Ami@DBAces.com)