SmartData:
Make the data “think” for itself

Privacy and security in a virtual web-world

George J. Tomko, Ph.D.
Expert-In-Residence
Identity, Privacy and Security Institute (IPSI)
University of Toronto, Canada

Presentation Outline

1. *Why SmartData? Background and context*
2. *Why on-line PETs may not be rolled out*
3. *The concept and goals of SmartData*
4. *The structure*
5. *EHR application example*
6. *The R & D strategy*
7. *Conclusions and discussion*

Virtual Worlds and the Future of Cyberspace

- *Original internet (text) ---- One dimensional.*
- *World Wide Web (images) --- Two dimensional.*
- *Virtual worlds --- Three dimensional.*
- *Humans familiar with 3-D world – social ways of exchanging information.*
- *Demands for privacy and security will escalate dramatically.*

PETs – A Hard Sell!

- ***Governments and corporation want greater access to personal data – not less.***

- ***Why would the rabbits who are in charge of the lettuce finance fences to restrict unfettered access?***

Why SmartData?

- ***The individual and his personal information has been separated.***

- ***Need to re-embody personal information.***

The Goal of SmartData

- *Better privacy is not more security and regulations around an expanding perimeter of collective personal information.*

- *Better privacy is shrinking that perimeter down to one individual's personal information such that the person and his information are inseparable.*

- *And the person via his/her proxy is always in control.*

Our Approach

Virtual Simulation

+

Evolutionary Embodied Cognition within a dynamical systems framework

Three principles guiding the design

- ***Individual consent within a context***
- ***Security***
- ***Use limitation based on primary purpose***

What is SmartData?

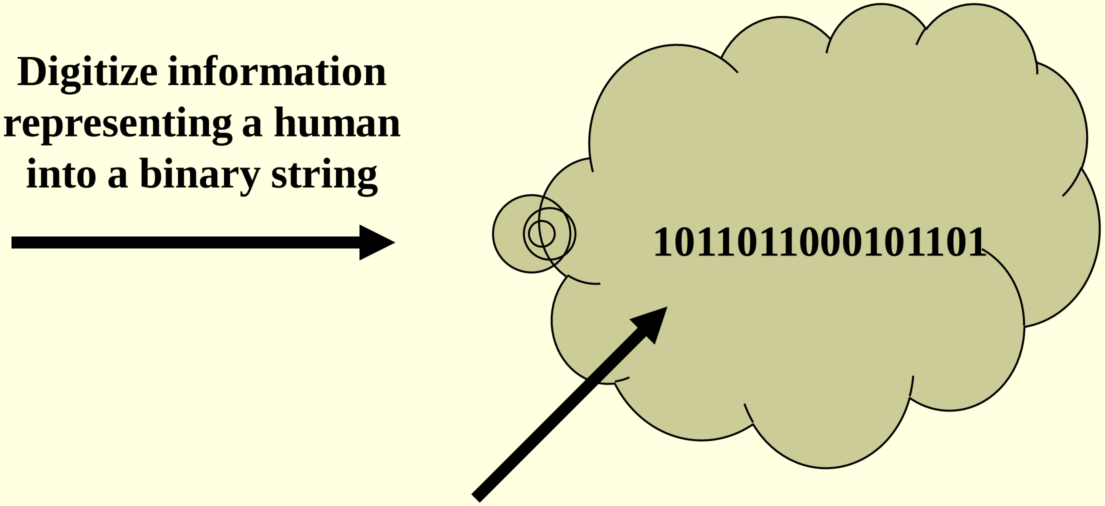
A Thought Experiment

Human SmartData

My Personal Information

The Digital Human SmartData

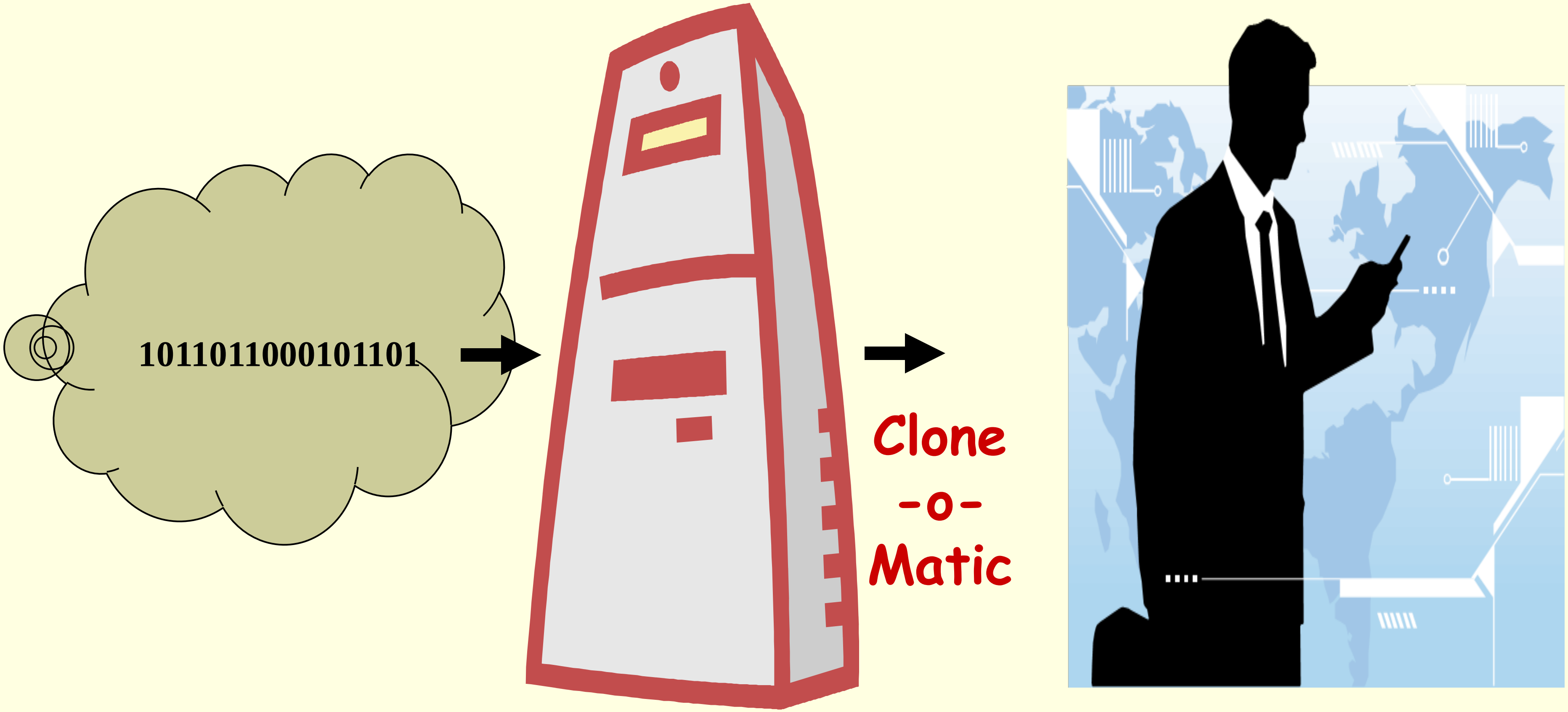
Digitize information representing a human into a binary string



1011011000101101

Stored in the "cloud"

What if we reconstruct the human?



1011011000101101

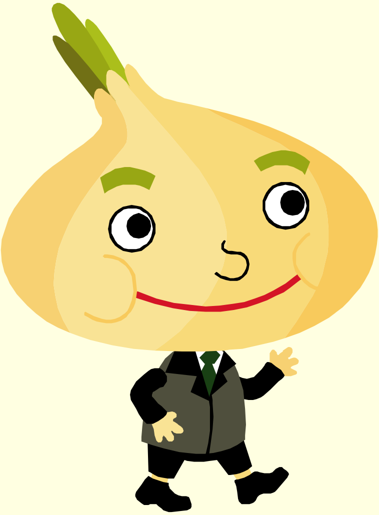
Clone
-o-
Matic

Clone serves as your proxy on the web

Features of SmartData

- *discloses information only when your personal criteria have been met;*
- *Protects and secures your personal information;*
- *Information can be released in a non-digital form;*
- *Make decisions about whether or not to disclose information based on context.*

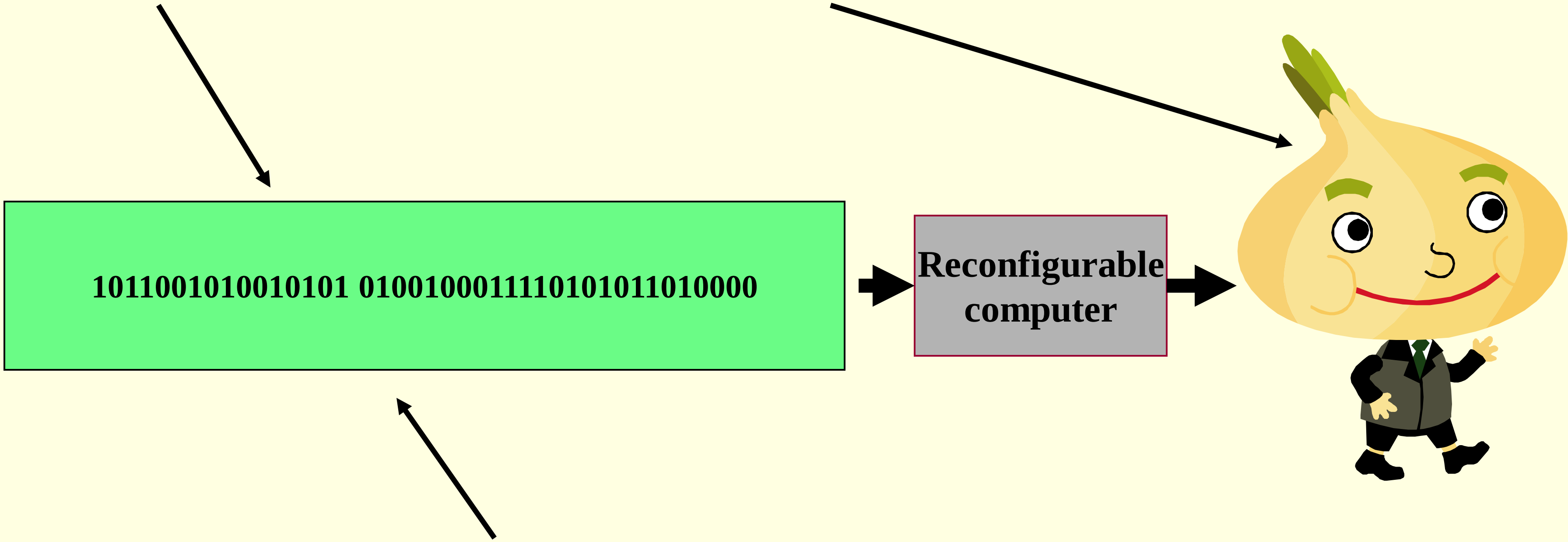
Substitute clone with an intelligent agent



SmartData

Structure of SmartData

Binary String represents the structure of the SmartData agent

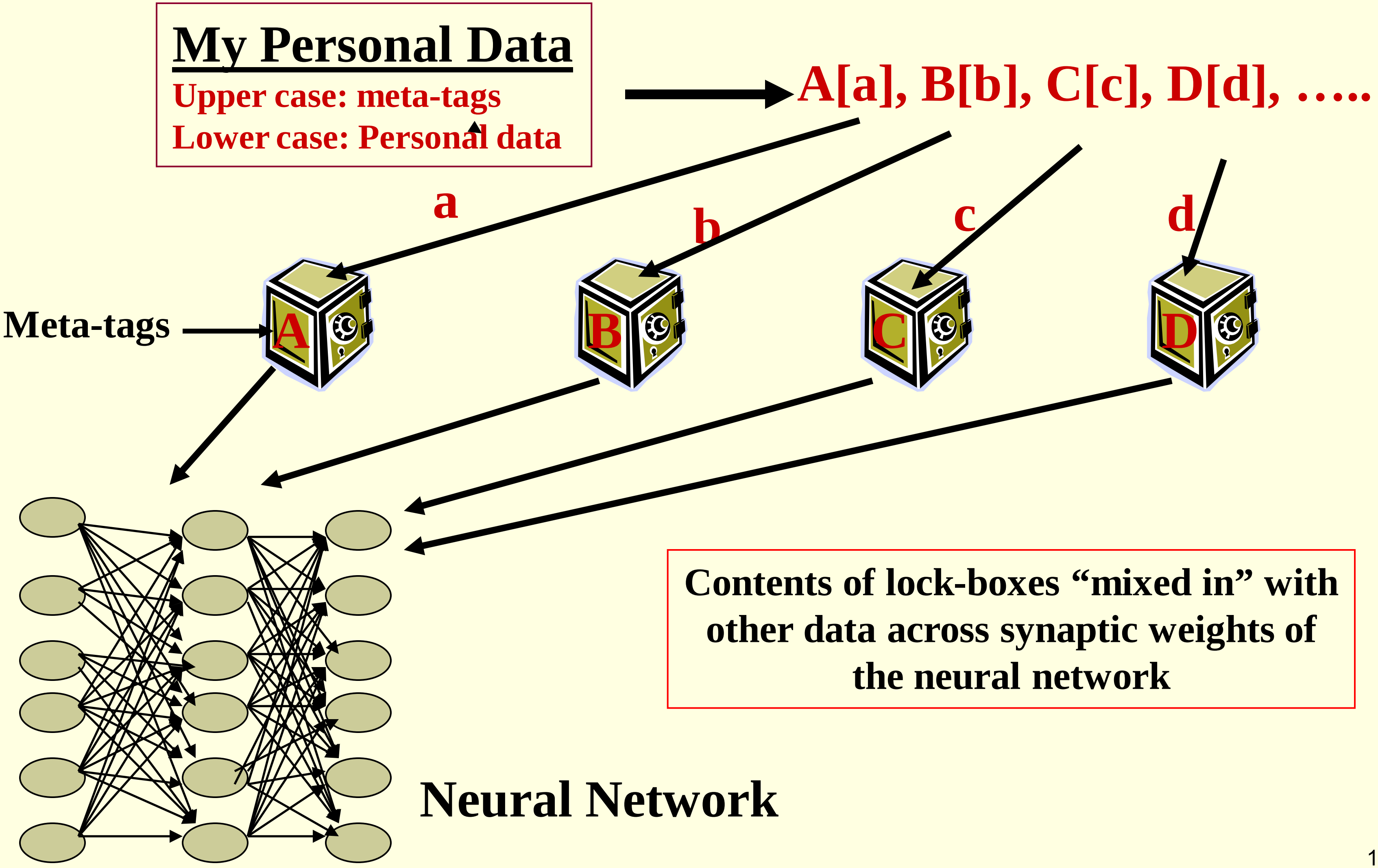


1011001010010101 0100100011110101011010000

Reconfigurable computer

Personal data “mixed in” with other information

SmartData Security Structure



My Personal Data

Upper case: meta-tags

Lower case: Personal data

A[a], B[b], C[c], D[d], …..

Contents of lock-boxes “mixed in” with other data across synaptic weights of the neural network

Neural Network

Authenticating

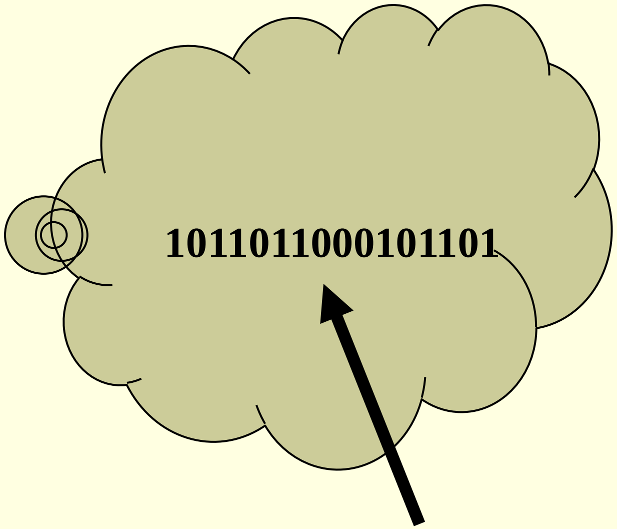
- ***SmartData: authenticate credentials of requestors***
- ***Requestors: authenticate credentials of SmartData***
  - ***Digital signatures and biometrics***

Analog output option

- ***Digital-to-analog or digital-to-image within SmartData***

No Personal information in the cloud: Just SmartData

- **Only SD binary string is transmitted**

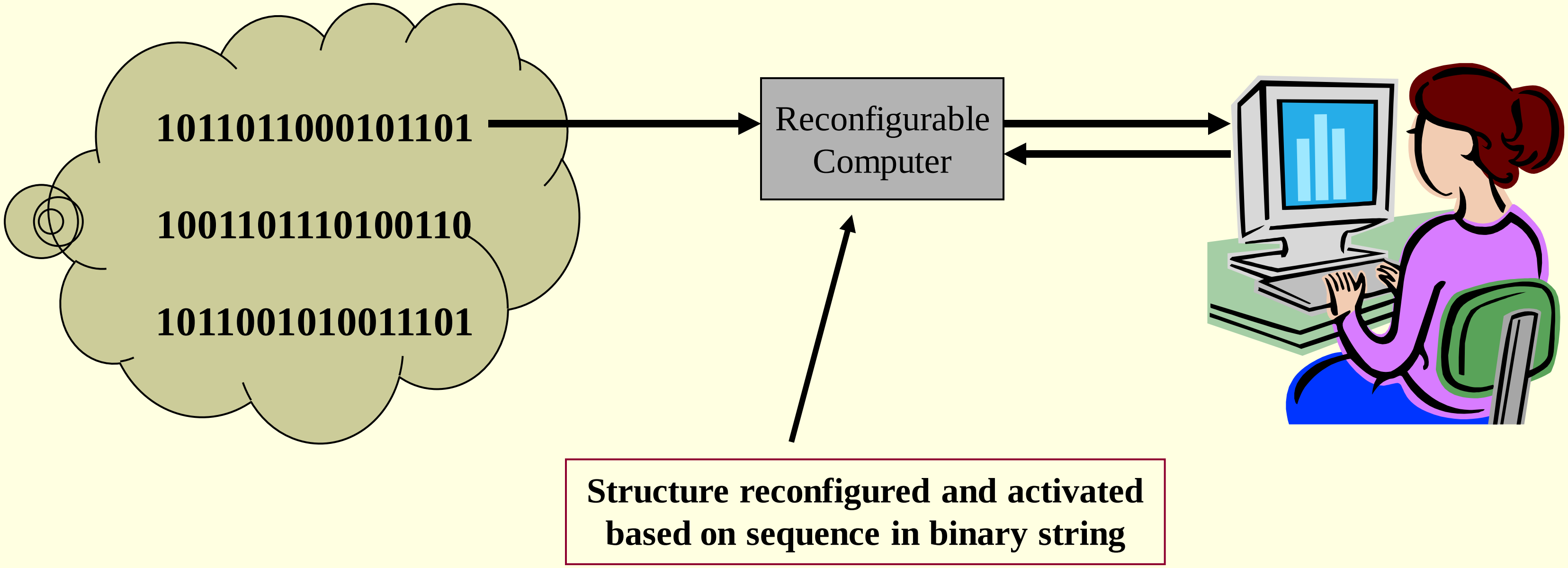


SmartData binary string – personal information locked inside

- There would be no personal or proprietary “raw” data out in the open.

- It would instead be housed “within” a SmartData agent

SmartData as an Electronic Health Record



1011011000101101

1001101110100110

1011001010011101

Reconfigurable Computer

Structure reconfigured and activated based on sequence in binary string

Houston, we have a problem!

- ***Details of brain’s algorithm is far too complex.***
- ***Brains may not use algorithms at all, but heuristics tailored to each individual.***
- ***Solution: Copy nature – evolution and natural selection.***

Embodied Cognition

- *Contents and operations of cognition are determined by the whole body and the environment in which the body is situated.*
  - *Not just the brain alone.*
  - *Physical, “organismic”, and conceptual embodiment.*
- *The body is the active interface to the world.*
  - *transforms physical variables in the environment via the sensors into neural control system parameters.*
  - *converts neural variables via motor action into environmental parameters.*

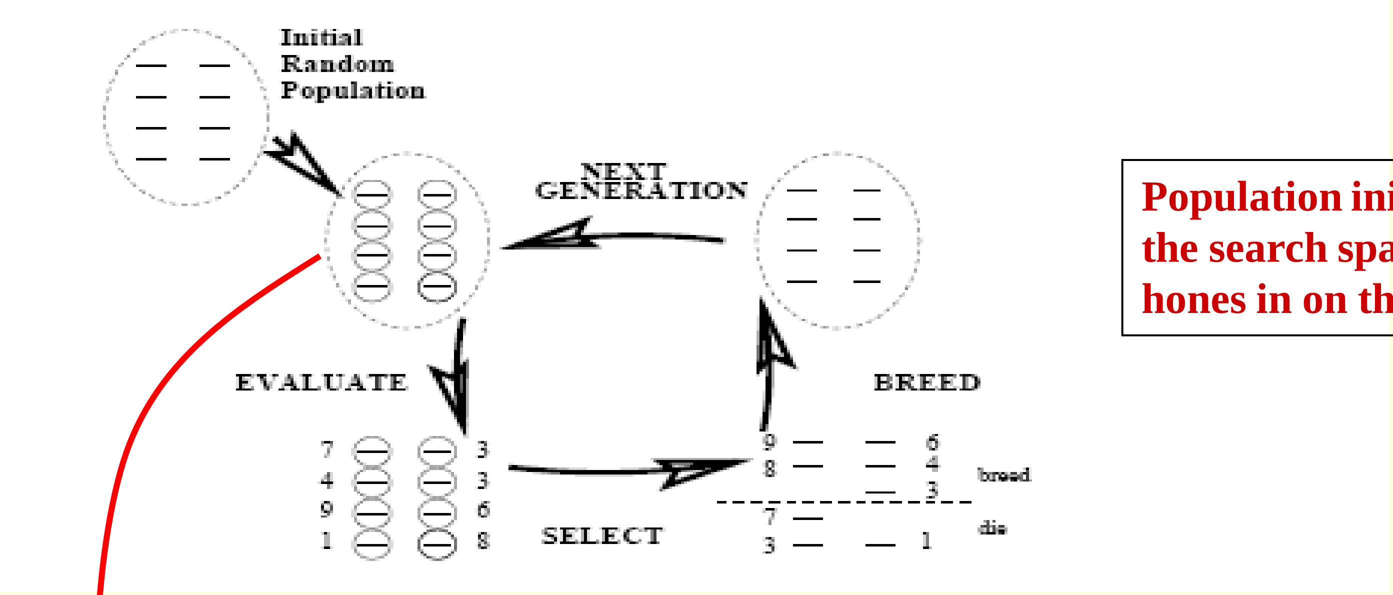
Evolutionary Robotics

- ***Uses principles of natural evolution to create artificial agents.***

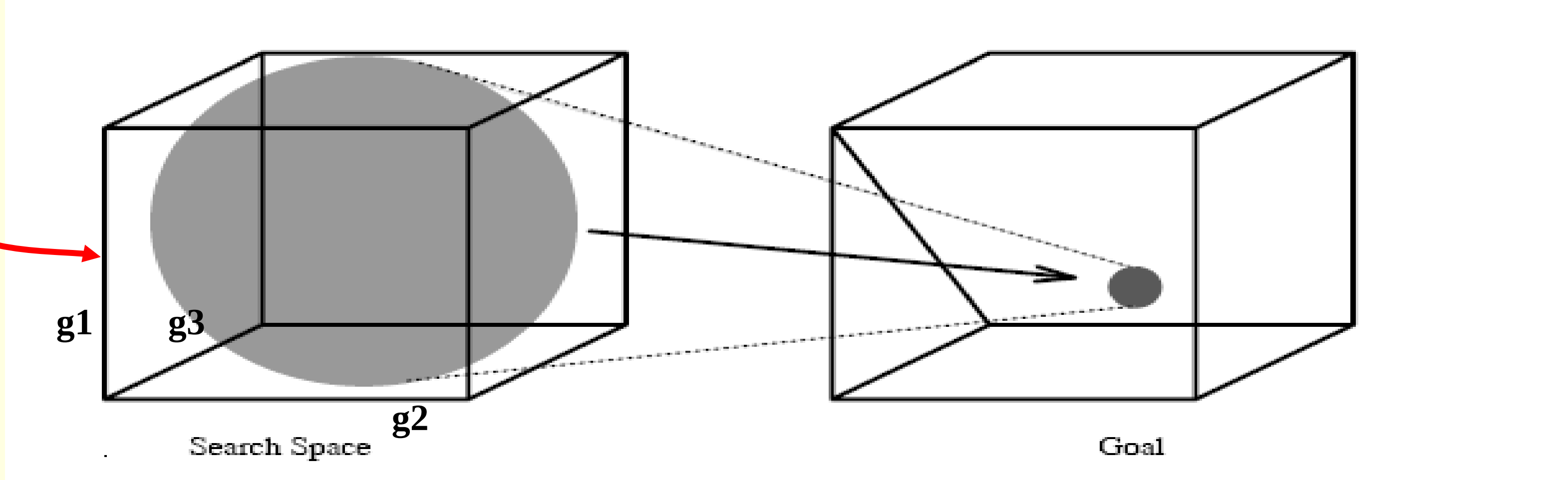
- ***Bottom-up methodology versus top-down as in the field of Artificial Intelligence.***

- ***No initial design – only an initial design objective.***

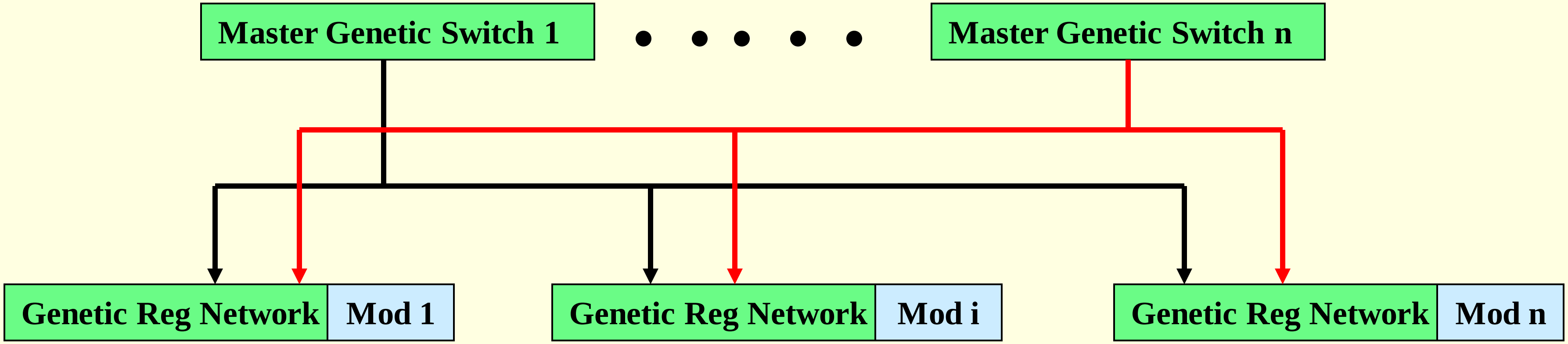
The Genetic Algorithm Cycle



Population initially spans the search space and progressively hones in on the optimum



Evolution by Modifying Design



Master Genetic Switch 1 • • • • • Master Genetic Switch n

Genetic Reg Network | Mod 1

Genetic Reg Network | Mod i

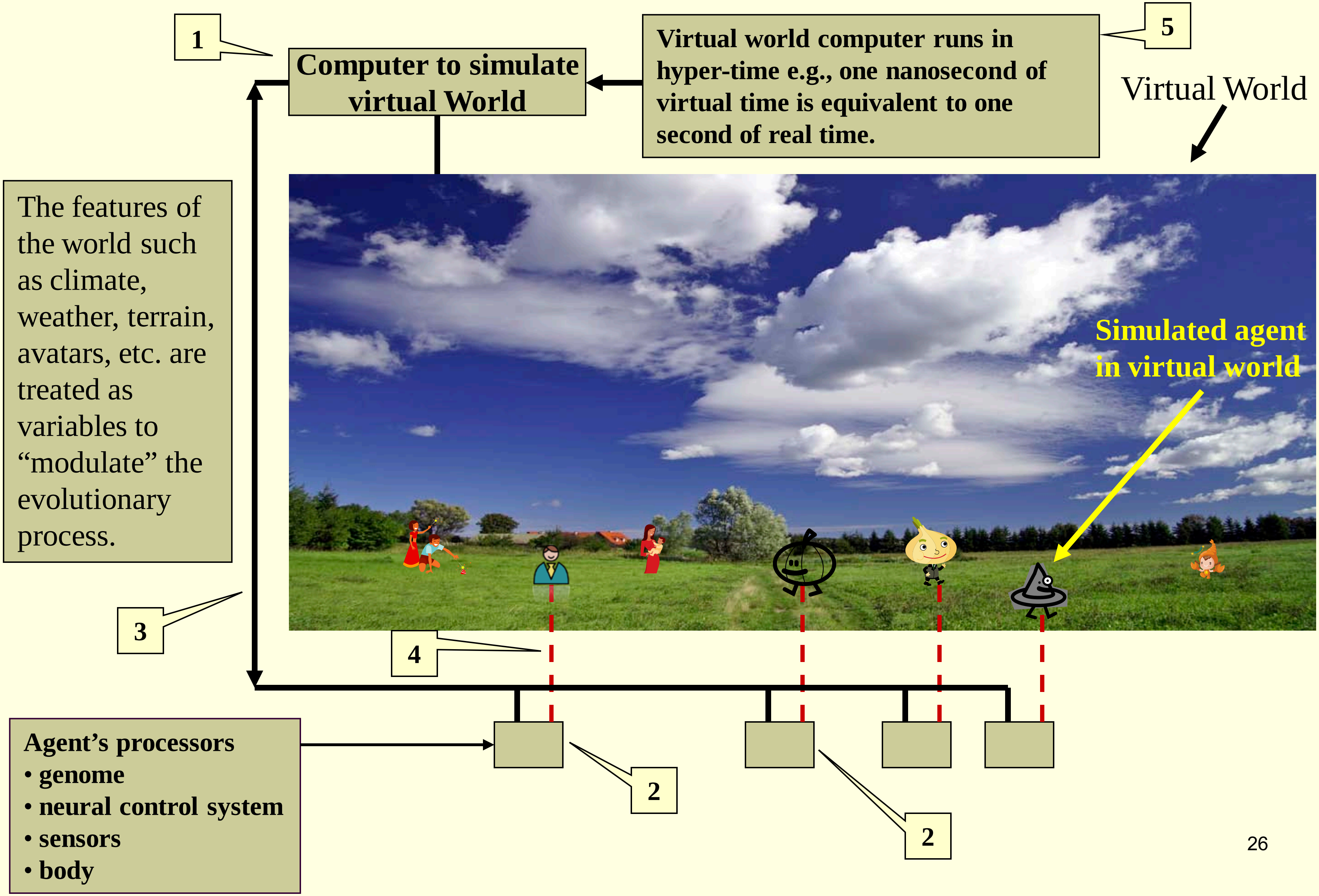
Genetic Reg Network | Mod n

Mod 1 = neuron (w,x,y,z…)
Where:
w = type of neuron;
x = number of neurons;
y = transfer function;
z = rules for LTP;

Mod i = sensor (x,y,x,z…)
Where:
w = type of sensor;
x = number of sensors;
y = location of sensors;
z = resolution;

Modules conserved;
GRN controls variables (,w,x,y,z);
GRN and MGS will undergo mutation

The Matrix of Virtual Evolution



Computer to simulate virtual World

Virtual world computer runs in hyper-time e.g., one nanosecond of virtual time is equivalent to one second of real time.

The features of the world such as climate, weather, terrain, avatars, etc. are treated as variables to “modulate” the evolutionary process.

Agent’s processors

- **genome**
- **neural control system**
- **sensors**
- **body**

Evolution is a knowledge-gaining process of the world

- ***The world “selects” the cognitive structures.***

- ***Therefore, must “build-into” and organize the virtual world such that it will select the necessary structure for SmartData.***

Embodied Dynamical Systems Framework

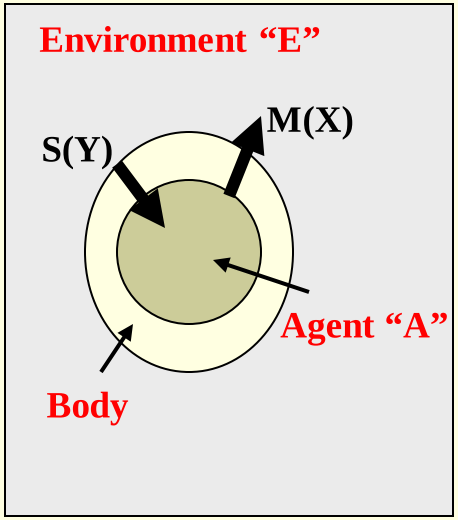
Simulate E

Evolve A

$$\frac{dX}{dt} = A\left(X; S\left(Y\right); U\right)$$

$$\frac{dY}{dt} = E\left(Y; M\left(X\right); V\right)$$

Coupling Parameters



Where:

A = Agent's transition map;

E = Environment's transition map;

X = Output variable of Agent's neurons;

Y = Output variables of environment;

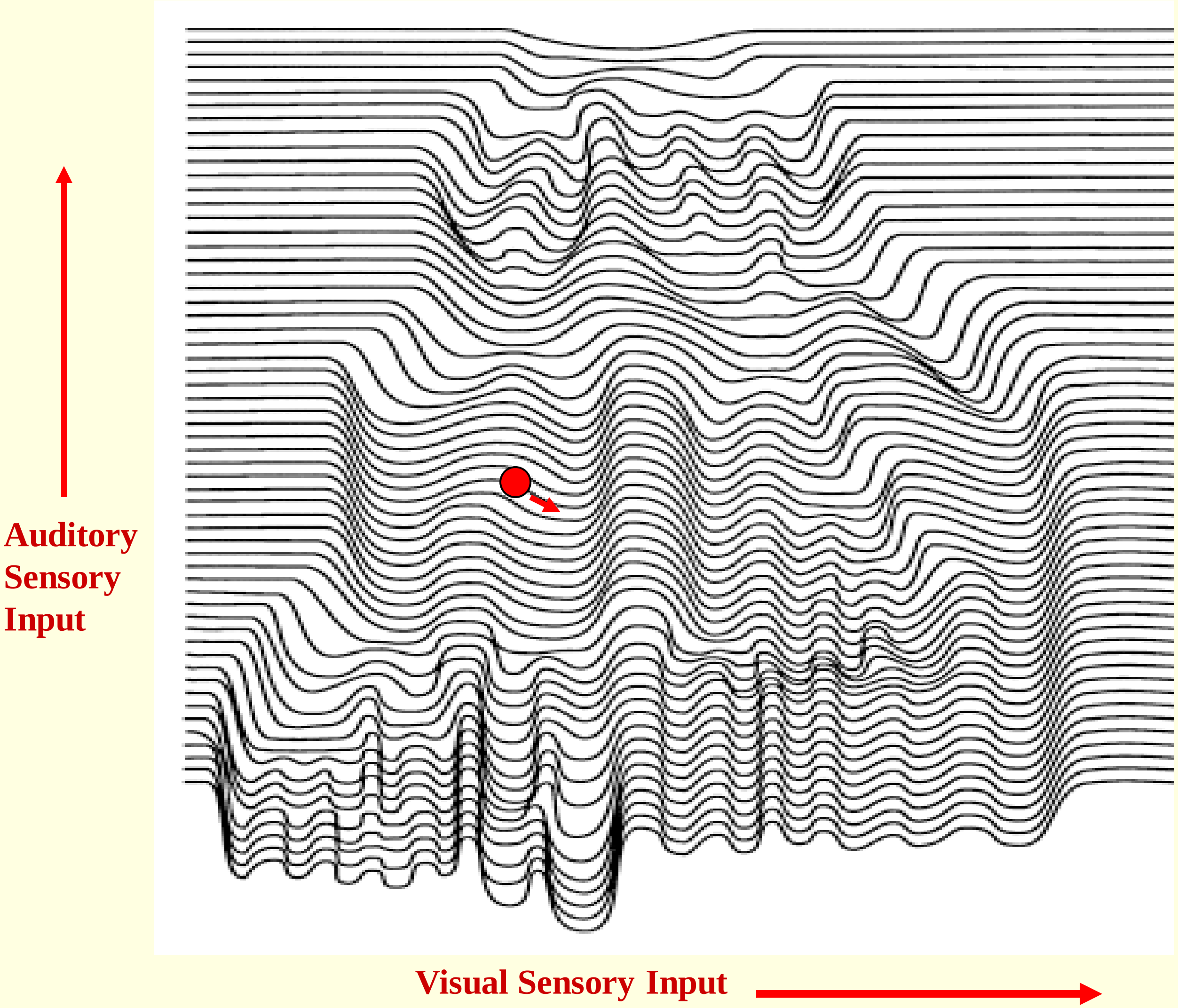
S(Y) = transformation of environment's variables into sensory parameters;

M(X) = transformation of Agent's variables into motor parameters that affect the environment;

U = Agent's internal parameters;

V = Environment's parameters

Dynamical System as a Dancing Landscape



Auditory Sensory Input

Visual Sensory Input

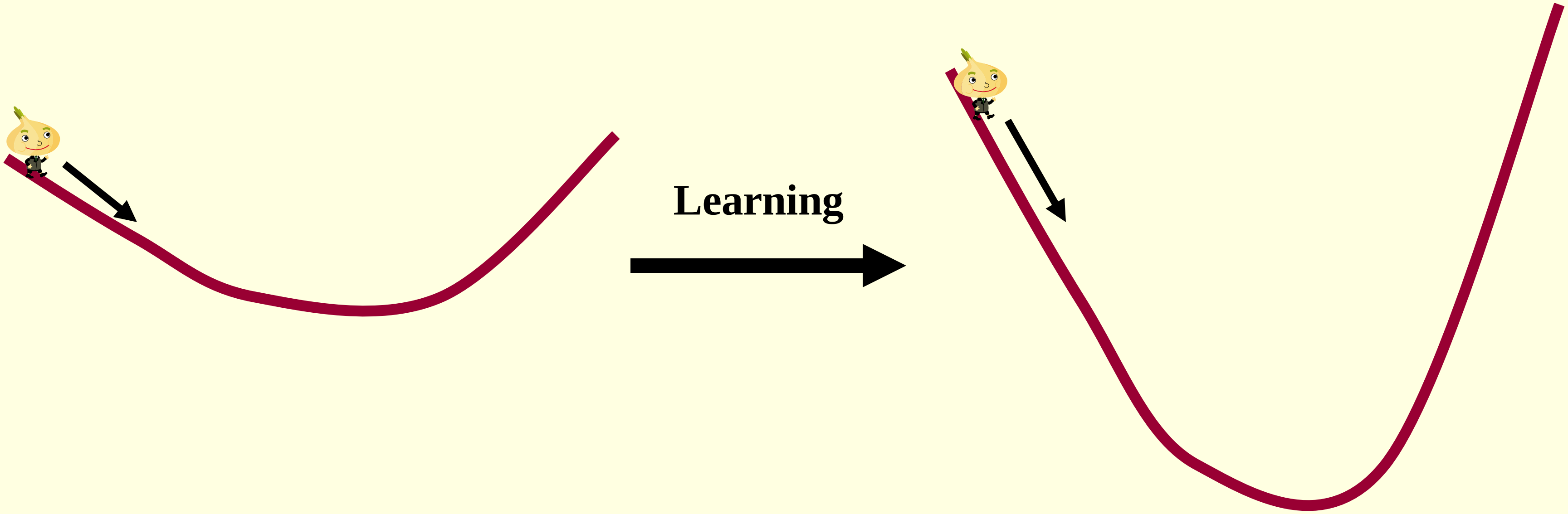
Life is Just a Journey

- *In the dynamical systems framework, all behaviours – perception, motor, language, thinking, reasoning, and memories – are one and the same.*

- *They are trajectories in an appropriate basin of attraction.*

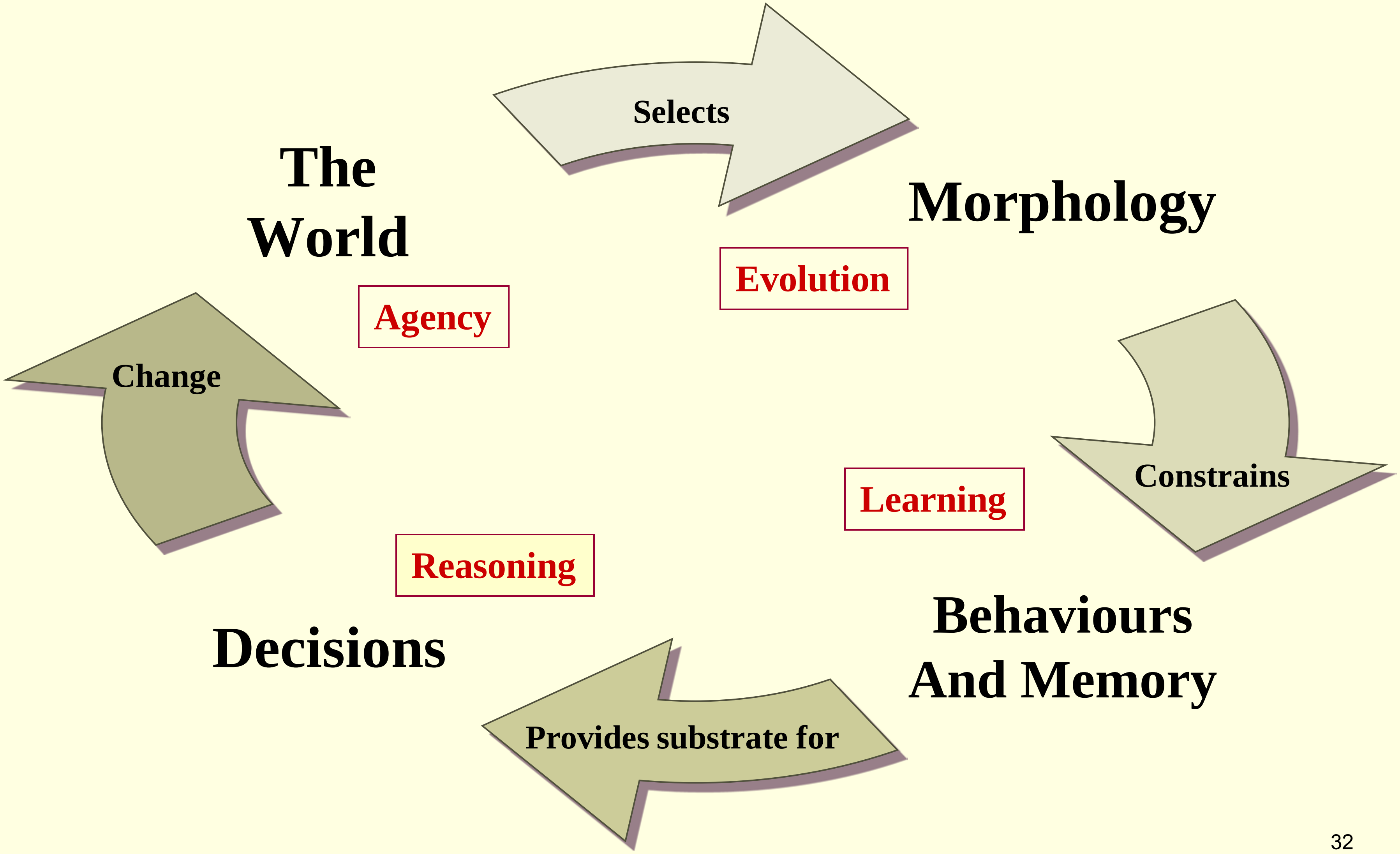
And Learning is …

- about changing shallow basins of attraction into deep basins that are more stable to change



Learning

The Nested Loops of Artificial Agency



Conclusions

- ***Current-day protections are largely ineffective – reactive.***
- ***Empower virtual, cognitive agents to act on our behalf to protect the data entrusted to them – proactive.***
- ***The ultimate embodiment of Privacy by Design.***
- ***SmartData – an innovative approach to protecting privacy and security.***