What exactly does US6370629 control?

US6370629 or CONTROLLING ACCESS TO STORED INFORMATION BASED ON TIME AND LOCATION is a US Patent which today may be the single most infringed patent on Earth. The Enforcement Losses are significant enough to impact the US GDP and any covering up of the Fraud Loss would be a Crime against the Public it seems.

How so? Simple… The US6370629 patent controls a trifecta of current use models in digital systems. They are all based on the use of a COMPLEX TIMESTAMP WHICH MAY ALSO HAVE LOCATION INFORMATION INSIDE THE STAMP ITSELF'; Those already identified infringements based on our analysis are as follows:

COMPLEX TIMESTAMPS IN ORACLE AND OTHER DATABASES

The Timestamps inside ORACLE DATABASES AND VIRTUALLY ALL OTHER DATABASE SYSTEMS [INCLUDING SPREAD SHEET SYSTEMS] use a secured timestamp form which infringes on Claims 1-32 of the US6370629patent. Additionally Database Systems have INFORMATION INTEGRITY PRACTICES which involve creating signed or secured hashes or other cryptographically enhanced service models.

So in an ORACLE FINANCIAL package there would be numerous TIMESTAMPS which infringe created by the CONTENT CREATION PROCESSES of the Application - i.e. when it works on data it creates output with TIMESTAMPS which Infringe directly in a number of places in the infrastructure (the APP, the CONCURRENT MANAGER, and the BACK-END DBMS Server itself).

This is also true for MySql, PeopleSoft and many other DBMS systems and their applications. The same Infringement will of course follow as true for CUSTOM APPLICATIONS BASED AROUND MICROSOFT ACCESS AS WELL.

COMPLEX TIMESTAMPS IN DOCUMENT METADATA

The Timestamps inside Electronic Document METADATA in all commercial uses today including but not limited to Adobe PDF Files, Microsoft Office Files, all of the GRAPHICAL INTERCHANGE Technology Formats standardized and globally accepted today.

They all use the same conceptual METADATA timestamping as the basis of their Revision and Policy Engine Controls and as such they use a secured or hashed timetsamp with location or network addressing as the location information which infringes on Claims 1-32 of the US6370629 patent.

So for instance there are TWO TYPES OF TIMESTAMPS in MICROSOFT OFFICE OR ADOBE PDF FILES, the first is inside the FILE CONTENT itself, these are used inside

the PROGRAM READING OR WRITING THE FILE TO PROVIDE POLICY CONTROLS, and then there is the OPERATING SYSTEM TIMESTAMP for each and every FILE ACCESS. Both of these are direct infringements into US6370629;

One key and new use is GEOTAGGING of information; The concept of digitally signing or embossing the LOCATION AND TIME data so that this Image can be sorted or processed based on constraints therein is a key infringing use today.

COMPLEX TIMESTAMPS IN POLICY CONTROL MODELS IN MOBILE AND EMBEDDED OR SECURE CONTROL SYSTEMS

The Timestamps inside OPERATING SYSTEM FILE SYSTEMS have already been noted but there are others including SECURE SYSLOG INSTANCES OR LIKE LOGGING SYSTEMS WHICH CAPTURE KEY EVIDENCE OF OPERATIONS; Additionally virtually anything using an x.509 Certificate for anything will directly infringe as will most PKI Models using a timestamp or location context (GeoTagging) to put controls into Operating System Infrastructures.

Network Interfaces as an Infringement

These areas of Infringement include the actual NETWORK SOFTWARES used to connect the computers together today as well meaning the network which links most systems will operating with one or more infringing practices directly.

As to how this happened a number of the actual NETWORK PROTOCOL STANDARDS from IETF and others integrate COMPLEX TIMESTAMPS WHICH ARE SECURED OVER ENCRYPTED NETWORKS INTO THE ACTUAL NETWORK PROCESS meaning just turning the machine on and connecting it to anything will in most instances provide several OS Level Network Infringements therein.

Electronic Metadata (including GEOTAGGING) which contains Infringing Timestamps

As noted above in the comment about GeoTagging of images, another key area of Infringement is in Electronic Document METADATA in all commercial uses today including but not limited to Adobe PDF Files, Microsoft Office Files, all of the GRAPHICAL INTERCHANGE Technology Formats standardized and globally accepted today.

Additionally DOCUMENT CONTROL SYSTEMS WHICH RELY ON ISO-32000-1 WILL ALL INFRINGE because they rely on the TIMESTAMPS INSIDE PDF DOCUMENTS TO PROVIDE THEIR DOCUMENT CONTROL SERVICES used in concert with OS and Access Control Paradigms.

KEY INFRINGING APPLICATIONS INCLUDE:

1) Document Control and Processing Systems in Public and Private Operations; Timestamping IN THE OPERATING INITATION CODE - Meaning the code which certifies the OS instance is properly licensed and can start up. 2) Microsoft and the other OS Vendors have developed a number of control practices in the OS which require this SECURED COMPLEX TIMESTAMP service to function at all. 3) PATCH AND CHANGE MANAGEMENT SYSTEMS;

KEY INFRINGING APPLICATION SYSTEMS

Voting is the first one to list, the Data Capture Models all rely on COMPLEX TIMSTAMPS including from the SCANNING of PAPER BALLOTS INTO THE VOTE CAPTURE SYSTEM and all the VOTING TABULATION CODE;

Another Key one is Federal, State and Private Document Control systems, including the Court ECF, the FBI's National Crime Information Center and its total services as well as those TIMESTAMPING APPLICATIONS IN THE US SECURITIES FRAMEWORK;

Finally it controls the GEOSPATIAL INTELLIGENCE AND GLOBAL SURVEILLANCE SYSTEM TOTALLY as well as ALL TIME ON TARGET WEAPON AND WEAPON-REPORTING SYSTEMS AND SERVICES; all of which infringe both in their COMPONENT OPERATIONS (the actual running of the systems) and in their DATA PRODUCTS, i.e. in the content data they produce which is DIGITALLY TIMESTAMPED AND RECORED IN THAT CONTEXT AS ADMISSIBLE COURT EVIDENCE.

In Summary - One Planet - One Patent…

Today, whether ANY Government likes it or not US6370629 controls the planet Earth in whole. Any Intel or Government Agency wishing to refute this Statement please do so…