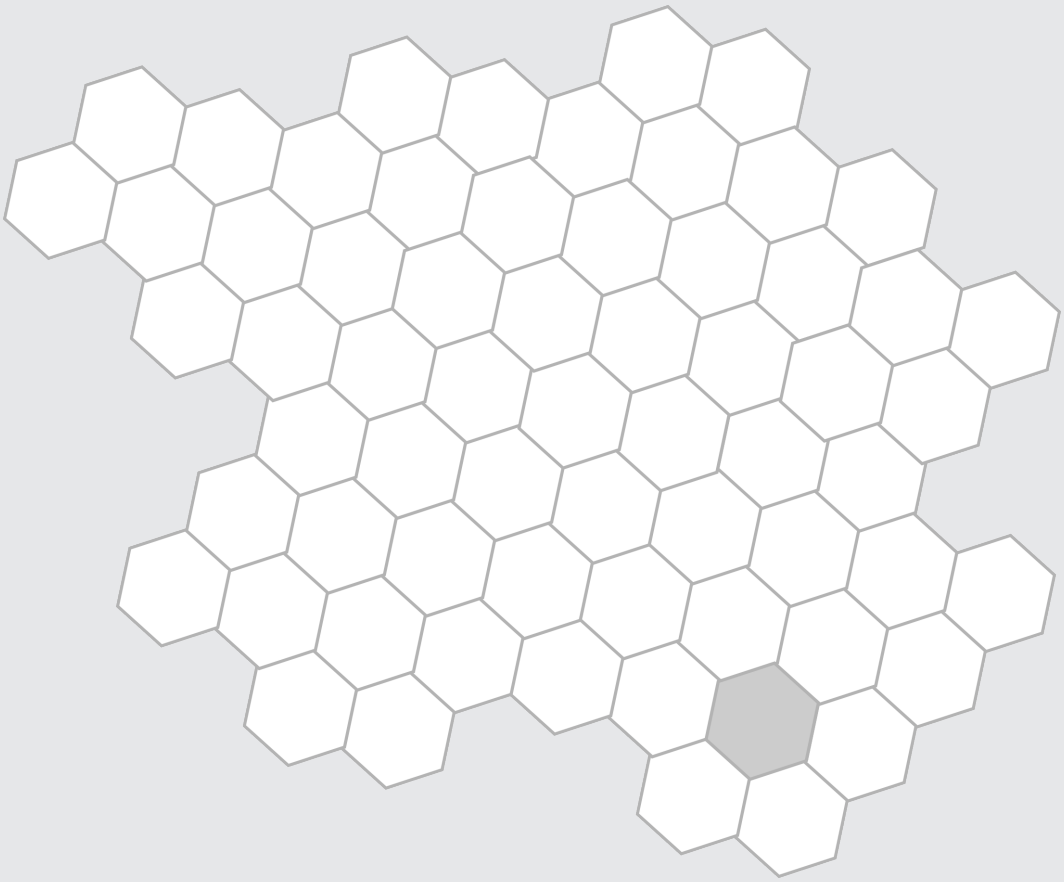
International Journal on

SOCIAL MEDIA

MMM: Monitoring, Measurement, and Mining



I, 2010, 1
ISSN 1804-5251

...OFFPRINT...

International Journal on SOCIAL MEDIA

MMM: Monitoring, Measurement, and Mining

I, 2010, 1

Editor-in-Chief: Jan Žižka

Publisher's website: www.konvoj.cz
E-mail: konvoj@konvoj.cz, SoNet.RC@gmail.com
ISSN 1804-5251

No part of this publication may be reproduced, stored or transmitted in any material form or by any means (including electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of the publisher, except in accordance with the Czech legal provisions.

Data Mining of Online Judicial Records of the Networked US Federal Courts

Joseph Zernik
Human Rights Alert (NGO), PO Box 526, 91750 La Verne, California, U.S.A.
e-mail: jz12345@earthlink.net

Abstract

The US federal courts have completed a decade-long project of networking coast to coast. Data mining was conducted through the online public access system to examine the validity and integrity of records and of the system as a whole. Many records were not verified at all. Moreover, records were universally missing their authentication counterparts, required by law to render them valid and effectual. The authentication counterparts—previously public records—were now excluded from public access. Records, which are today posted online in the public access system, included both valid and invalid, void records. However, the public was unable to discern the difference. The system as a whole was deemed invalid. Case management systems of the courts must be subjected to certified, functional logic verification. Mandated system transparency should permit ongoing data mining, and the computing/informatics community should lead the way in monitoring the integrity of the courts in the digital era.

Key words

relational databases; functional logic verification; Case Management Systems; United States Courts; human rights; Los Angeles; California; United States; justice system; law; fraud; corruption; judges

Biographical note

Professor Zernik served on the faculty of the University of Connecticut, University of Southern California, and University of California, Los Angeles.

In 2010 he founded Human Rights Alert (NGO), dedicated to discovering, archiving, and disseminating evidence of human rights violations by the justice systems of the State of California and the United States in Los Angeles, California, and beyond. Special emphasis is given to the unique role of computerized case management systems in the precipitous deterioration of the integrity of the justice system.

Paper v Digital Administration of the Courts[i]

The transition of the US courts to digital administration was executed over a comparatively short time through a large-scale project managed by the Administrative Office of the US Courts, an arm of the US judicial branch. Dual systems were established: PACER—for public access to court records, and CM/ECF—for case management/electronic court filing. The systems are effectively a series of relational databases.[ii] With it—a sea change was affected in court procedures. In contrast,

procedures for the paper administration of the English-speaking courts evolved over centuries, and formed the foundation of due process and fair hearings rights. Disambiguation of court procedures and court records was the cornerstone of such rights. Therefore the current report employed data mining to examine the newly established digital administration of the US courts for the following fundamentals of due process: a) valid, published rules of court, b) public access to judicial records—to inspect and to copy, and c) verification 1 and authentication of judicial records, including notice and service of judicial papers. Finally—validity of the systems as a whole as assessed.

Valid Published Rules of Court

Procedures of the US courts under paper administration evolved from the English legal system, and were established in the US Code of Civil/ Criminal Procedures[iii, iv] and published Local Rules of Court, which the courts were authorized to adopt, [v] subject to prior publication of such rules for public comment and challenge. The transition to digital administration of the US courts inevitably entailed a sea change in court procedures, which had to be established by law or by the publication of new local rules of courts. The current report documents the failure of the US courts to publish their new rules pertaining to the new digital procedures.

Public Access to Judicial Records—to Inspect and to Copy

The right to public access to judicial records—to inspect and to copy - was well established in both US and common law.[vi] Judicial paper records, which were maintained by the Clerk of the Court, included individual Court Files together with Books of Courts, including, but not limited to the Court Dockets—logs of all valid proceedings and all valid records pertaining to the respective court files by the clerk. The transition to digital administration of the courts entailed substantial changes, not by necessity, of the well-established set of judicial records. Moreover, through differential individual authorities, it became much easier to conceal digital judicial records. The current report documents the universal denial of public access to critical judicial records, that is the authentication counterparts of individual court records in all courts that were examined.

Verification and Authentication of Judicial Records

Verification by a judge, and authentication by a clerk, of court orders and judgments were a prerequisite for entry of court records as honest, valid, and effectual court papers in court files and dockets. These requirements were founded in the US Constitution, in early Acts of US Congress, and in the US Code of Civil/ Criminal Procedures.[vii, viii]. Notice and service of judicial records—court minutes, orders, and judgments were an integral part of the authentication procedures mandated on the clerks for all court minutes, orders, and judgments. The clerks would mail out to all parties in a case certified, authenticated copies of all judicial records, jointly satisfying both the authentication per se and the notice and service requirements. In the transition to digital administration of the courts, new procedures were devised for the digital verification by judges, for the purported certification of entry

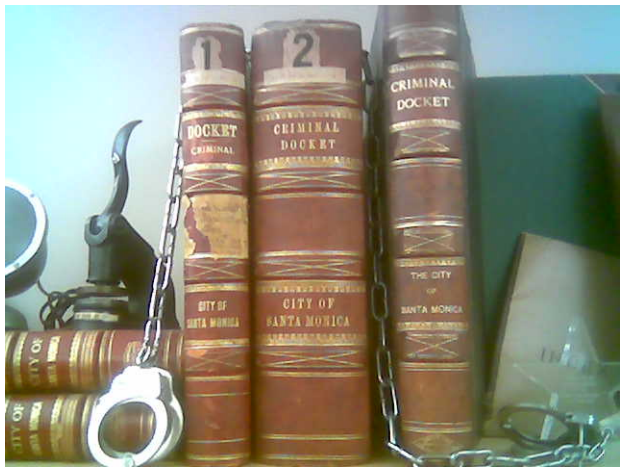


Figure 1:
Historic, paper-based Books of Court–Criminal Dockets; City of Santa Monica, California

of the records, and for the construction of dockets by the clerks. Additionally, service and notice were made possible through electronic mail. The current report documents deficient or invalid authentication of court records, effectively eliminating any valid certification by the clerk, and universal denial of public access to the authentication records.

Proposed Solutions

The current report documents the compromised integrity of the US courts, undermined through the installation of invalid, unverified digital administration systems. Solutions are readily available tha which could make digital administration of the courts honest and secure and far superior to paper administration of the courts. The relational databases,[ix] which form the foundation of digital administration of the US courts, must be subjected to certified, functional logic verification. Transparency should be required, to allow ongoing data mining by the public at large–for monitoring integrity of the courts. The computing/informatics community should assume a leading role in the safeguarding of human rights and the democratic nature of society in the digital era.

Objective

The current report investigated through data mining the online public records of the US courts and evaluated the safeguards for the fundamentals of due process and fair hearings in the transition from paper to digital administration of the courts. Moreover, the report examined the potential role of data mining of online public records of the courts as an essential civic duty–public monitoring of the integrity of the courts.

Figure 2:
CM/ECF—the Case Management/Electronic Case Filing system of the United States courts

The Systems

PACER,[x] the online system for Public Access to Court Electronic Records of the US Courts, permits public access on payment to records of the US district courts and some US courts of appeals, including the indices, dockets, calendars, and records of the various cases. CM/ECF[xi], the online system for Case Management/Electronic Court Filing of the US Courts, permits the courts themselves and attorneys, who are authorized by a given US court in a given case, to file records. Pro se litigants—those representing themselves in court, including most prisoners[xii] and others, who petition the US courts for protection of Human, Constitutional, and Civil Rights, are routinely denied access to CM/ECF, and are required to file records on paper. They are likewise permitted access to court records through PACER alone. CM/ECF also provides notice and service of records, only to those authorized, via email.

NEFs (Notices of Electronic Filing)[xiii]—at the US district courts, and NDAs (Notices of Docket Activity)—at the US courts of appeals, were established by the US courts as the counterparts for the purported digital authentication of court records.[xiv] Parties, who are unauthorized in CM/ECF are routinely excluded from notice and service of the NEFs and NDAs.

Methods—Data Mining and Record Examination

Data mining, which formed the basis for the current report, was conducted through public access to PACER, as permitted by law, in over 20 US district courts, US bankruptcy courts, and US courts of appeals.[xv] Some of the individual cases that were examined as part of the study were identified through methods which were developed for rapid screening of cases in the various courts to identify cases that were deemed at high risk of perversion and were therefore selected for further examination. Other cases were identified through direct alerts by individuals who were parties to the cases. Most of the cases involved litigations where individuals who were plaintiffs filed complaints for protection of civil rights, or complaints alleging wrongdoing by large financial institutions. Court records were examined in the individual cases to determine whether court minutes, orders, and judgments were verified and authenticated in a valid manner.[xvi] Since public access was found to be universally denied to the authentication counterparts, in some of the cases repeat attempts were made over months, as described below, to gain access to the authentication records, through written requests as well as repeat personal appearances at the offices of the clerks of some of the courts. In particular instances where

credible evidence was found that records provided through PACER were false and misleading, lacking verification and/or authentication, but displayed as "entered", written requests were filed with the clerks and presiding judges of the US district courts to investigate such records and initiate corrective actions.

Additionally, local rules of courts, general orders, and CM/ECF user's manuals were downloaded through routine web browsing of the web pages of the various courts. Court rules, general orders, and user's manuals were examined to determine whether the courts published clear and unambiguous rules establishing the courts' new digital procedures. When no clear and unambiguous published rules were found, requests were forwarded in some cases to the clerks and the chief judges to disclose the new rules of the courts.

Results

Data Mining

All data mining in the current report was manually performed. However, although not detailed in this report, methods were devised to scan large numbers of cases in any given US court, which could be automated. Although significant differences were found in implementation of PACER and CM/ECF in the various courts, the basic platforms were identical in all courts that were examined. The basic findings were likewise similar in all courts. Specific examples are provided below.

Published rules of court

Review of the local rules of court of the various US courts and US courts of appeals,[xvii, xviii] universally revealed no direct reference to PACER, CM/ECF, or new digital procedures pertaining to verification and authentication of, notice and service of, and public access to, court records. In some cases reference, albeit vague and ambiguous, was found in general orders of the courts. However, in the vast majority of the courts, which were examined, no reference was made anywhere in local rules of court, in general orders, or even in user's manuals, to the critical new procedures now established by the courts for purported authentication of records through a "Document Stamp" (an encrypted checksum string) as the equivalent of the former signature by the clerk of the court.

For example, upon inquiry, the office of the clerk, US District Court, Central District of California, claimed that the new rules were established in General Order 08-02.[xix, xx] In pertinent parts,[xxi] General Order 08-02 prohibited external hyperlinks in any court records, declared that acceptance of electronic filing constituted entry of a record in the case docket, established the NEF as the certification by clerk of court records, and the electronic "document stamp" as validating the authenticity and notice of the record. The order established that pro se litigants would be required to continue filing records on paper, and electronic filing of records, which were filed by pro se litigants on paper, would be executed by the clerk. However, the NEF itself was never defined in the General Order 08-02. Moreover, it should also be noted that General Order 08-02, in contrast to other general orders of the

US District Court, Central District of California, was published with no verification by a judge at all, and with no name of its author either. No significant information pertaining to electronic filing practices were found in the Local Rules of Court or General Orders of the US Court of Appeals, 9th Circuit.[xxii]

Additional critical information regarding the NEF and procedures of the US District Court, Central District of California was detailed in the Unofficial Anderson Manual.[xxiii] The CM/ECF User's Manual of the US Court of Appeals, 9th Circuit,[xxiv] likewise included detailed description of the NDAs—Notices of Docket Activity—as the purported authentication records of the Court.

Public Access to Judicial Records—to Inspect and to Copy

Public access to the purported authentication records—NEFs and NADs—was universally denied in PACER. Additional efforts were made to access the NEFs and NDAs in some of the courts, through repeated direct requests to the clerks of the courts. The courts routinely denied such access, with no reason at all. Limited access was eventually gained in two of the courts – the US District Court for the Central District of California, and the US Court of Appeals, 9th Circuit.[xxv]

It should further be noted that key records were removed from public access in the dockets of the various US district courts and US courts of appeals, with no reason at all. For example, in the Fine v Sheriff Appeal (09-56073) at the US Court of Appeals, 9th Circuit, records Dkt #28, 32, 36, 56, were removed from public access. These records were mostly related to response to the appeal by the Appellees. Such selective denial of public access to court records was of particular concern, since the Appellant in the case objected to some of the same response papers, claiming that they included as evidence records that were not admissible. PACER, as a public access system, if validated, should never permit such selective removal of records from the dockets, unless by authorized personnel, pursuant to sealing orders, docketed in the respective cases.

It should also be noted that the dockets of the US Court of Appeals, 9th Circuit, as a rule failed to explicitly state within the public dockets the date of entry of judgments of the US district courts from which the appeals were purported to originate. The dates of entry of judgments are critical data regarding the validity of the appeals as a whole, since the jurisdiction in appeals is limited by law to entered judgments, if notice of appeal is filed within the time frames permitted by law.

Table 1: Summary of information pertaining to electronic filing for the US District Court, Central District of California and the US Court of Appeals, 9th Circuit

Court	Rules of Court	General Orders	User's Manuals
Central District of California	None	General Order 08-02	Detailed description of electronic filing practices in an "unofficial" manual
Court of Appeals, 9th Circuit	None	None	Detailed description of electronic filing practices.

Verification, Authentication, and Notice of Judicial Records

The dockets of the US courts and courts of appeals were found to include records that were either not verified by a judge, or not adequately authenticated by a clerk. For example, two critical records—the Judgment and the Mandate, in the docket of Richard Fine v Sheriff of Los Angeles County (2:09-cv-01914) at the US District Court, Central District of California, were deficient. One was an unverified record, failing to include any signature by a judge, and both were unauthenticated records—missing the electronic "Document Stamp" in the respective NEFs:[xxvi] Similarly - orders of the US District Court, Vermont, in Huminski v Rutland Police Department (1:99-cv-160) were served with NEFs bearing no "Document Stamp" at all.[xxvii] Therefore such records could not possibly be deemed by the courts themselves as honest, valid, and effectual judicial records.[xxviii] Regardless, these records were listed in the dockets of the respective US district courts as "entered". However, pro se litigants and the public at large, who must rely on PACER access alone, would not be able to discern the difference between records where valid NEFs were issued, and ones where invalid NEFs were issued by the courts.[xxix]

Moreover, nowhere in court dockets of any of the courts was there any statement of certification invoking the authority of the clerk of the court, and in various cases it was found that unauthorized personnel executed transactions in the dockets. For example—some 15 key records[xxx] in the docket of Richard Fine v Sheriff of Los Angeles County (2:09-cv-01914) were found to have been 'entered' by a court employee who was not authorized as a Deputy Clerk. Moreover, the Clerk of the latter court refused to certify the docket of the latter case, or to state that the dockets in the latter case and other similar cases were dockets constructed pursuant to authority of the clerk in compliance with US law.[xxxi] Similar requests, which were forwarded to the Chief Judge of the respective court—to investigate the matter and initiate corrective actions, were never answered at all. The PACER dockets of the US courts of appeals, likewise, never named the individuals who constructed the dockets and their respective authority. Moreover, no records were stated as 'entered' in the dockets of the US Court of Appeals, 9th Circuit.

Numerous Orders of the US courts of appeals in various cases were served and posted in the dockets with no verification by any judge at all. Moreover, such orders of the US courts of appeals were served with no NDAs at all.[xxxii, xxxiii] Therefore, the dockets, orders, and judgments of the US courts of appeals were deemed inherently ambiguous[xxxiv, xxxv].

Discussion

The findings described in this study must raise serious concerns regarding substantial ambiguity introduced into the conduct of the US courts and US courts of appeals through the transition to digital administration of the courts. Such ambiguity, in and of itself, should be deemed as antithetical to due process and fair hearings, and undermining the integrity of the courts. The effects of the changes in the administration of the US courts documented in the current report on the protection of human rights and enforcement of the law cannot be overstated. Gains in

integrity of the justice system, which were achieved through generations of struggle, have been lost over the past decade through the introduction of PACER and CM/ECF.

Published Local Rules of Court

The results showed that neither the US district courts, nor the US courts of appeals, published local rules of court to spell out their new procedures, which were adopted by these courts as part of implementation of PACER and CM/ECF. For example the Clerk of the Court, US District Court, Central District of California, claimed that the new procedures were established in General Order 08-02. However, general orders are not the legitimate vehicle for establishing new rules of court. Moreover, General Order 08-02, upon review by a reasonable person would be found vague and ambiguous in defining the new practices of digital administration of the courts. Furthermore – General Order 08-02 was published by the Court as an unsigned order with no name of its author and his/her authority. The Unofficial Anderson Manual of the same court provides additional details regarding the new procedures of the Court. However a third party "unofficial" publication could never be deemed a legitimate vehicle for Local Rules of Court in compliance with the law.

The US Rulemaking Enabling Act was signed into law in 1934, authorizing the US Supreme Court and to lesser degree other US courts to promulgate the Federal Rules of Civil/Criminal Procedure. The Rulemaking Enabling Act never mandated the courts to publish new rules. However, failure to publish rules pertaining to fundamental court procedures must be seen as contradictory to due process and fair hearings. Rulemaking by the US courts has a long history as a bone of contention. The Federal Rules of Evidence promulgated by the US Supreme Court in 1972 raised substantial objections, which eventually led the US Congress to enact substantial modifications of the rules. Therefore, it appears that when it came to establishment of PACER and CM/ECF where major changes were introduced in court procedures, the courts took the approach of never publishing any rules at all.

Any computer program by definition is an assembly of assertions, or rules. Therefore, the case management systems of the courts inherently embedded in them numerous rules. Regardless of the fact that such rules were written in computer language of some kind, the courts were required to publish them as rules of court in natural language as well. The US courts deliberately kept such rules hidden from the public and from attorneys appearing before the courts.

Public Access to Judicial Records

Effectively, the setup created by the US courts through PACER and CM/ECF segregated litigants into two separate and unequal groups.[xxxvi] Those assigned to PACER access alone were denied access to critical judicial records—the NEFs and NDAs. Therefore, such litigants and the public at large were unable under current conditions to distinguish between authenticated and unauthenticated judicial records—those which were deemed by the courts themselves as valid and effectual,

versus those which were deemed by the courts themselves as void, not voidable. Needless to say, such a setup at a minimum limited PACER users to a vague and ambiguous perspective on judicial records. The evidence (an example is provided from the Middle District of Florida) showed that even competent experienced attorneys failed to understand the new unpublished rules, and showed the inherent inability of such attorneys to distinguish the validity, or lack thereof in particular court records.[xxxvii]

The failure to define the NEFs in Local Rules of Court in the California Central District and other US courts, combined with their vague and ambiguous description in General Order 08-02, their universal exclusion of the NEF from PACER, and the routine denial of access to NEFs by clerks, were unlikely to be viewed by a reasonable person as merely coincidental. In parallel, the US courts and courts of appeals were shown in the current report to routinely engage in posting in PACER dockets, and in the case of the US district courts, also listing as "entered", papers which were either unverified or never authenticated and therefore could never be deemed by the courts themselves as valid and effectual judicial records. Through such concerted actions, each and all of them in contravention of the law, the public at large, and pro se litigants in particular, were misled into assuming that various records which were deemed void by the courts, were in fact the law of the land.

Judicial Records–Verification and Authentication

The current report documents vague and ambiguous conditions regarding the nature of valid and effectual verification by judges and authentication by clerks of judicial records. Regardless, the finding clearly documents the issuance of records that were never verified and/or authenticated, but were presented as such in the PACER records.

The refusal of the Clerk and Chief Judge of the US District Court, Central District of California, to investigate allegations of misconduct at the Court relative to the issuance of invalid, void, unauthenticated judicial records, and their posting in PACER dockets as "entered", or to initiate corrective actions, provided further evidence that the conduct of the courts in this regard did not result from inadvertent errors.

A further review of the NEF and NDA[xxxviii] forms raised grave concerns. In particular courts, e.g. US District Court, South Carolina, a feature was implemented which made the link between the NEF and the respective record expire after 15 days. There could not possibly be an explanation for such a feature that would be consistent with valid authentication practices of court records.[xxxix]

Comparison of standard authentication counterparts, e.g.–Certification of Acknowledgement by notary public,[xl] and an older, paper-based Certificate of Mailing and Notice of Entry by Clerk,[xli] to the NEF and NDA, revealed additional inherent defects with respect to four basic features: a) title, b) certification statement, c) relationship to the certified record, and d) signature/authority.

The two former forms included in their titles the word "Certificate" or "Certification", while the NEF and NDA failed to include such words in their titles. The former forms included the key statement "I certify..." while the NEF and

NDA included no such statement. The former forms, upon execution were directly, physically, attached to the record being authenticated (in some jurisdictions to this date—through ribbons and sealed wax or embossed foil), but the NEF and NDA were entirely detached from the authenticated records, and were instead hyperlinked—a practice which was explicitly prohibited by the US District Court, Central District of California, General Order 08-02. In at least in one case, Shelley v Quality Loan Services (09-56133) at the US Court of Appeals, 9th Circuit, a false hyperlink was allegedly employed to generate an invalid, void NDA.[xlii] The Court refused to correct the defect even upon request by the Appellant. The former forms, when executed, included "wet" graphical signatures in traditional signature boxes, where the name of the individual executing the authentication was typed below the signature line, and his/her authority to certify the authentication record was spelled out. In addition—a stamp or an imprint of a personal seal or a court stamp were affixed. The NEF and NDA fail to name the individual who purportedly executed any authentication, the authority of the clerk of the court is never invoked, and no stamp or seal or any personal signature of any kind appear in the NEF and NDA that could possibly be deemed as indicating an intention to take responsibility. A checksum string, in and of itself, carries no such significance at all. In short—the NEF and NDA, as implemented in CM/ECF, failed to make any claim of certification of authentication of a specific court record, and failed to convey any intention to take responsibility by an individual invoking the authority of the Clerk of the Court.

The Validity, or Lack Thereof, of PACER and CM/ECF as a Whole

Based on the deficiencies described above, a reasonable person is likely to conclude that the NEFs and NADs are inherently vague and ambiguous, if not void, and thus undermine the validity of the CM/ECF court records as a whole. Furthermore, a valid case management system should never have permitted the issuance of court records and inclusion of such records in court dockets while no valid NEFs or NDAs bearing an electronic "Document Stamp" were issued—if the courts considered such a checksum string as being of any significance. Likewise, a valid and secure case management system should never have permitted persons who were not authorized as deputy clerks to access court dockets and execute transactions that should have been permitted only to authorized persons. Combined with other deficiencies it is practically certain that PACER and CM/ECF as a whole would never have been deemed valid case management systems had the systems been subjected to publicly and legally accountable validation—certified, functional logic verification.

The law[xliii] requires US judges to "initiate appropriate action when the judge becomes aware of reliable evidence indicating the likelihood of unprofessional conduct by a judge or lawyer." However, the evidence in the current report documents the refusal of judges to correct false and misleading court records. Moreover, it is unreasonable to assume that none of the judges in the US, who are trained in the law and immersed in administration of the courts, noticed the glaring defects in PACER and CM/NEF.[xliv, xlv] Therefore it is reasonable to conclude that the compromised integrity documented in the current report was intentional. An abun-

dance of cases involving financial institutions among the cases that were compromised would likewise give conditions at the US courts as one of the fundamental causes of the current financial crisis and dysfunctional state of US banking regulation.[xlvi]

With it, the systems as they are present unique possibilities. Had the US courts permitted public access to the NEFs and NDAs, as required by law, it would be possible to construct a machine generated "Index of Judicial Corruption"—for any US judge who sat on the bench in the past decade, based on the issuance of invalid authentication records, with no understanding at all of the legal matters involved.

Certified Logic Verification and Data Mining are Keys to the Solution

The compromised integrity of the US courts is linked in the current study to the transition of the courts to digital administration. However, such an outcome was not inherent in the transition. On the contrary, digital technologies could provide case management systems that would enhance the integrity and transparency of the courts.

The following are proposed as guidelines for corrective measures:

a) Online public access and case management systems of the courts, which are critical for the safeguarding of human rights and the democratic nature of society, must be subjected to publicly and legally accountable validation (certified, functional logic verification)[xlvii] in all stages of implementation and maintenance. Verification in general, and in relational database management systems in particular,[xlviii] is in principle an NP-complete problem. However, the systems in question are not of such a complexity level as would prohibit functional verification. Moreover, functional logic verification of such systems must be of the highest priority. Therefore any unnecessary complexity must be avoided. User defined integrity constraints must be precisely specified and implemented, and all stages of software implementation must be subjected to structured programming approaches,[xlix] to make them readily amenable to verification.

- Professionals who are versed in computer science and also in the basics of the law—in particular—the law as it pertains to court administration - must undertake verification of such systems. Legally and publicly accountable certification of logic verification implies a process, similar to that which is practiced today relative to building plans, which are subject to public scrutiny in various public planning and zoning boards, and later—through scrutiny of the completed civil engineering projects by authorized inspectors. Within the context of such public process, it is assumed that new principles of public logic documentation and representation would evolve over time as 'standards of care'.

b) Online public access and case management systems of the courts must be required to allow a high level of transparency of judicial records and the systems as a whole. Transparency of the systems at present is limited, and varies considerably among the various courts, with no foundation in the law. Inherent in transparency is also the requirement that all Local Rules of Court, which

are implemented in such systems, be explicitly published in natural language, and posted for public comment and challenge, as required by the US Rulemaking Enabling Act. The only examples presented in the current report involved the failure to publish rules, which were embedded in PACER and CM/ECF, and pertained to verification and authentication of records. However, numerous other rules were found embedded in the systems, which were never published. Further transparency should be required, to allow zero-knowledge monitoring of integrity of the systems through data mining by computing/informatics professionals and the public at large.

c) The public at large must be educated that engagement in data mining of systems that are critical for the safeguarding of human rights and the democratic nature of society is a fundamental civic duty. Case management systems of the courts should be required to permit a high level of transparency, both of the public records inherent in them, and also transparency to allow zero-knowledge monitoring through data mining.[1]

Conclusions

The transition to digital administration entailed a sea change in procedures of the US courts. The transition took place over a relatively short time, and was independently executed by the US judiciary, with insufficient public and legal accountability. The transition resulted in a precipitous deterioration in the integrity of the courts, which undermined the safeguarding of human rights and enforcement by regulatory agencies in the United States. The conditions that were generated as a result are unprecedented in democratic societies in the modern era. They are employed for deprivation of the rights of the people, and to benefit those in government and large corporations. The proposed solution should involve publicly accountable validation (certified, functional logic verification) of case management systems of the courts, system transparency, and ongoing data mining—a civic duty and a prerequisite for the integrity of the courts in the digital era. Although the current report documents conditions at the US courts, similar risks are faced by other nations as well. The international computing/informatics community should assume a leading role in the protection of rights and the democratic nature of society in the digital era.

References

[i] The matters covered in the current study were covered in greater detail in a series of three papers, as a solicitation of expert opinions: `http://www.scribd.com/doc/29525744/`, `http://www.scribd.com/doc/29525890/`, `http://www.scribd.com/doc/29527583/`.

[ii] Codd, E F: The relational model for database management: version 2, ACM Classic Books Series, Addison-Wesley Publishing Company, Inc (1990)

[iii] US Constitution and Acts of Congress, pertaining parts, see—NEF—A Review: `http://www.scribd.com/doc/24732941/`

[iv] *Federal Rules of Civil/Criminal Procedures*

[v] *Rulemaking Enabling Act* 28 USC § 2071–2077: `http://inproperinla.com/10-06-18-rulemaking-enabling-act-s.pdf`

[vi] In US law the right to access judicial records is considered a First Amendment right, as reaffirmed in *Nixon v Warner Communications*, Inc (1978), 435 U.S. 589 (1978). In British law it is deemed a Common Law right.

[vii] US Constitution and Acts of Congress, see–NEF a review: http://www.scribd.com/doc/24732941/

[viii] *Federal Rules of Civil/Criminal Procedures*

[ix] F. Coenen: Verification and Validation Issues in Expert and Database Systems: The Expert Systems Perspective, dexa, 16 pp., 9th International Workshop on Database and Expert Systems Applications (DEXA'98), (1998)

[x] PACER login page: https://pacer.login.uscourts.gov/cgi-bin/login.pl?court_id=00idx

[xi] CM/ECF of the US District Court, Central District of California–login page: https://ecf.cacd.uscourts.gov/cgi-bin/login.pl

[xii] The US Constitution Article I, §9, clause 2: http://www.archives.gov/exhibits/charters/constitution.html

[xiii] NEFs–A review, including samples from various courts: http://www.scribd.com/doc/24732941/

[xiv] Authentication of court records serves dual purpose: (1) Authentication by the clerk of the record duly filed by the judge, or by a party, and entered by the clerk into a given court docket, and (2) Certification that due notice was given to all parties of the entry of the new record.

[xv] artial list of courts and cases, where data were derived for the current report: http://inproperinla.com/10-06-23-partial-list-of-courts-and-cases-s.pdf

[xvi] Access to Local Rules of Court, General Orders, and other specific information of the US District Court, Central District of California: http://www.cacd.uscourts.gov/

[xvii] *Local Rules of Court* of the US District Court, Central District of California: http://www.scribd.com/doc/28862438/

[xviii] *Local Rules of Court* of the US Court of Appeals, 9th Circuit March 30, 2010 records, which were downloaded from the web site of the US Court of Appeals, 9th Circuit: the Local Rules of Court, the General Orders, the CM/ECF User's Guide, and Transcripts of CM/ECF instructional videos. http://inproperinla.com/10 03 30 nda at 9th cca rules orders manuals video transcripts s.pdf

[xix] *General Order 08 02* of the US District Court, Central District of California: http://www.scribd.com/doc/27632471/

[xx] *General Orders* of the US District Court, Central District of California: http://www.scribd.com/doc/28861084/

[xxi] Pertinent parts of the *General Order 08-02* of the US Court, Central District of California: http://inproperinla.com/10-06-18-pertinent-parts-of-general-order-08-02-s.pdf

[xxii] General Orders, CM/ECF User's Guide, and Transcripts of CM/ECF instructional videos of the US Court of Appeals, 9th Circuit: http://inproperinla.com/10 03 30 nda at 9th cca rules orders manuals video transcripts s.pdf

[xxiii] US District Court Central District of California CM/ECF "Unofficial Anderson Manual" http://www.scribd.com/doc/28869533/

[xxiv] See xxii, above.

[xxv] Declaration regarding attempt to access court records at the US District Court, Central District of California. http://www.scribd.com/doc/28932321/

[xxvi] *Richard Fine v Sheriff of Los Angeles County* (2:09-cv-01914) at the US District Court in Los Angeles, California–PACER docket: http://www.scribd.com/doc/32567529/

[xxvii] Unauthenticated court orders of the US District Court, Vermont, in *Huminski v Rutland Police Department* (1:99-cv-160): http://www.scribd.com/doc/25112472/

[xxviii] Two NEFs in *Richard Fine v Sheriff of Los Angeles County* (2:09-cv-01914): http://inproperinla.com/10-06-18-two-nefs-in-fine-v-sheriff-2-09-cv-01914-s.pdf

[xxix] The PACER docket texts for the two court papers, whose NEFs were reproduced in xxxviii, above: http://inproperinla.com/10-06-18-docket-text-for-two-records-in-fine-v-sheriff-s.pdf

[xxx] List of 15 records in *Fine v Sheriff* "entered" in the docket by "dt"–a court employee, but not deputy clerk: http://inproperinla.com/10-06-18-list-of-15-records-entered-by-dt-in-fine-v-sherif-s.pdf

[xxxi] Requests filed with Clerk of the Court Terry Nafisi regarding validity of the docket in Fine v Sheriff: http://inproperinla.com/10-01-17-req-responses-by-clerk-of-us-court-terry-nafisi-re-integrity-of-dockets-in-zernik-v-connor-and-fine-v-sheriff-s.pdf

[xxxii] June 30, 2009 *Order* by the US Court of Appeals, 9th Circuit, in the *Petition–Fine v Sheriff* (09-71692): http://inproperinla.com/10-06-18-june-30-2009-order-of-%20us-court-of-appeals-9th-fine-v-sheriff-s.pdf

[xxxiii] Orders in the Appeal–*Fine v Sheriff* (09-56073): See under index at: http://inproperinla.com/

[xxxiv] Pacer docket of *Richard Fine v Sheriff of Los Angeles County* (2:09-cv-01914) at the US District Court in Los Angeles, California: http://www.scribd.com/doc/32567529/

[xxxv] *Richard Fine v Sheriff of Los Angeles County* (09-56073) - appeal at the US Court of Appeals, 9th Circuit–Docket of the appeal http://inproperinla.com/00-00-00-us-app web-ct-9th-fine-v-sherifh-of-la-0-a-10-03-27-docket-of-appeal-09-56073.pdf

[xxxvi] Separate and unequal: http://inproperinla.com/10-06-18-separate-and-unequal-s.pdf

[xxxvii] Correspondence with Attorney Jack Thompson and Attorney Bob Hurt regarding records of the US District Court, Middle District of Florida: http://inproperinla.com/10-06-07-thomson-v-florida-bar-6-10-cv-442-authentication-s.pdf

[xxxviii] Invalid NDA of the US Court of Appeals, 9th Circuit, on the February 18, 2010 *Mandate* on the *Appeal* from *Petition for Writ of Habeas Corpus* at the US District Court, Central District of California. The *Mandate* itself was not verified by the circuit judges. http://inproperinla.com/10-06-18-nda-of-the-us-court-of-appeals-on-mandate-in-fine-s.pdf

[xxxix] User's Manual for CM/ECF from US District Court, South Carolina, describing a feature where the linkage between the NEF and the respective court record expires after 15 days: http://inproperinla.com/00-00-00-us-dist-ct-a-pacer-cm-ecf-a-cm-ecf-manual-us-dist-ct-nc-faq_v2-2007.pdf

[xl] Sample Certificates of Acknowledgement by public notary: http://inproperinla.com/10-06-16-notary-public-certification-of-acknowledgement.pdf

[xli] Text of Certificate of Mailing and Notice of Entry by Clerk: http://inproperinla.com/10-06-18-text-of-certificate-of-mailing-and-notice-of-entry-s.pdf

[xlii] In the case of *Shelley v Quality Loan Services* (09-56133) at the US Court of Appeals, 9th Circuit, the Order denying petition for a stay, was unsigned, and the NDA was invalid–hyperlinked to a false order. Moreover, the court refused to correct the error upon request by Appellant: Order: http://inproperinla.com/00-00-00-us-app-ct-9th-shelley_09-10-22-a-order-denying-petition-for-stay-unsigned.pdf
Email correspondence with Mr Shelly regarding order, where NDA was hyperlinked to a false record, and the US Court of Appeals, 9th Circuit refused to correct a false NDA: http://inproperinla.com/00-00-00-us-app-ct-9th-shelley_09-10-22-dubious-nda-10-03-26-shelley-email-notice-re-dubious-oct-22-2009-order-and-nda.pdf
False NDA, where the NDA was linked to an unrelated order from a prisoner's habeas corpus petition, still listed as the respective record in the NDA: http://inproperinla.com/00-00-00-us-app-ct-9th-shelley_09-10-22-dubious-nda-9th-circuit.pdf

[xliii] *Code of Conduct of US Judges, Canon 1, Canon 3B(3)*

[xliv] Repeat requests for the Clerk of US District Court, Los Angeles, to state that the docket in *Fine v Sheriff* was valid and effectual in compliance with US law were never answered: http://inproperinla.com/10-01-17-req-responses-by-clerk-of-us-court-terry-nafisi-re-integrity-of-dockets-in-zernik-v-connor-and-fine-v-sheriff-s.pdf

[xlv] Shelley v Quality Loan Services (09-56133)—see xlii, above.

[xlvi] See xv, above.

[xlvii] F. Coenen, see ix, above.

[xlviii] Codd, see viii, above.

[xlix] Dahl, O J, Dijkstra, E W, Hoare, C A R: Structured programming, ACM Classic Books Series (1972)

[l] Robling Denning, D. E.: Cryptography and data security, Addison-Wesley Publishing Company, Inc (1982)

Acknoledgement

The author is grateful for helpful discussions with human rights experts and computer science academic faculty.

Call for Papers

Papers to be included in the next issue should be preferably focused on topics related to social-networks in one or more of the following subjects (the list is indicative rather than exhaustive):

Sentiment/Opinion Analysis in Natural-Language Text Documents

Algorithms, Methods, and Technologies for Building and Analysing Social Networks

Applications in the Area of Social Activities

Knowledge Mining and Discovery in Natural Languages Used in Social Networks

Medical, Economic, and Environmental Applications in Social Networks

Submitted papers should not have been previously published nor be currently under consideration for publication elsewhere. Each of the submitted research papers should not exceed 26 pages. All papers are refereed through a peer review process.

Submissions should be send in the PDF form via email to the following address: `SoNet.RC@gmail.com`

Accepted papers are to be prepared according to the instructions available at `http://www.konvoj.cz/journals/mmm/`.