WASHINGTON
COURTS

August 8, 2021

TO: Data Dissemination Committee

FROM: Kevin Cottingham, AOC Data Dissemination Administrator

RE: Should the Washington National Guard be permitted to use elevated access to court records to conduct background checks on applicants to the military?

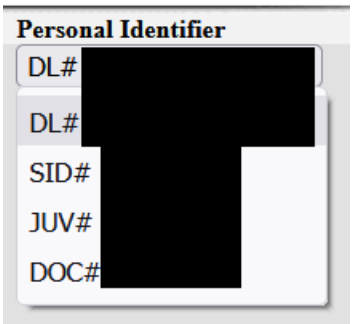
This issue was brought before the JISC Data Dissemination Committee at the request of Whatcom County Clerk, Superior Court Administrator and Juvenile Court Administrator David Reynolds. Mr. Reynolds was contacted by a Washington National Guard recruiter after that recruiter used JABS to conduct a background check on an applicant to the military. This recruiter inquired about a JUVIS number connected to an individual involved in a confidential dependency action that was actually unknown to the subject of the action—they were an infant when their court involvement resulting from their parents' divorce took place. Discussion took place at the DDC's June 2021 meeting but, due to limited time being allotted for discussion, ended in a vote to table the discussion until the August 2021 meeting and lower the Washington National Guard's JIS-Link access level in the interim. This memo summarizes the position of the Administrative Office of the Courts on the issue at hand.

There are actually two separate issues and recommendations involved—first, the visibility in JABS of the JUVIS number to users of all levels, and second, the Washington National Guard's use of its elevated law enforcement-level access to court records to conduct background checks on applicants. AOC's recommendations are 1) to direct the JABS team to remove the JUVIS number from JABS's identifier dropdown menu, and to 2) standardize policies for all elevated requestors by not allowing the Washington National Guard to use elevated access to conduct background checks and dissolving their current elevated JIS-Link site.

Display of the JUVIS Number in the JABS "Personal Identifier" List

When a user searches a name in JABS, the system returns a list of names and addresses for individuals responsive to their search. Each name has a "Personal Identifier" dropdown menu that lists identifiers attached to the well-identified person

records (WIP) contained in the Judicial Information System (JIS). See below for an example.



The item after "JUV#" is called a JUVIS number, which is a person-level identifier created when a juvenile is attached to a case in Odyssey or JCS. While this dropdown menu is undoubtedly helpful to end users, the display of the JUVIS number is problematic when viewed in light of the strict statutes pertaining to the confidentiality of certain juvenile records.

At issue are several statutes found in Chapter 13 RCW. Juvenile offender records are governed in general by RCW 13.50.050, which marks the "official juvenile court file of any alleged or proven juvenile offender [as] open to public inspection, unless sealed pursuant to RCW 13.50.260." Once sealed, per RCW 13.50.260, "proceedings in the case shall be treated as if they never occurred, and the subject of the records may reply accordingly to any inquiry about the events, records of which are sealed. **Any agency shall reply to any inquiry concerning confidential or sealed records that records are confidential, and no information can be given about the existence or nonexistence of records concerning an individual**" [emphasis added]. RCW 13.50.100 outlines the rules regarding juvenile non-offender records—truancy, at-risk youth, and dependency actions, for example—and states that they "shall be confidential and shall be released only pursuant to this section and RCW 13.50.010".[1] The statute goes on to state that "records retained or produced by any juvenile justice or care agency may be released to other participants in the juvenile justice or care system only when an investigation or case involving the juvenile in question is being pursued by the other participant or when that other participant is assigned the responsibility of supervising the juvenile."[2] While court rules typically govern the procedural matter of sealing across most case types,[3] the judiciary provides greater deference to statutes when juvenile court records are at issue.[4]

The broad access to the JUVIS number granted by the JABS search screen is not compliant with these statutes. When an individual listed in a search has a JUVIS

---

[1] RCW 13.50.100(2).
[2] RCW 13.50.100(3).
[3] *State v. Noel*, 101 Wash.App. 623, 628 (2000).
[4] *State v. S.J.C.*, 183 Wash.2d 408, 417 (2015).

number attached to their record, the number displays in the dropdown menu regardless of the security level of the user conducting the search, and makes no determination regarding whether that user is involved in a case or investigation regarding the individual at issue. That said, JABS is not displaying any of the cases it should not be displaying. Prosecutors can see minimal details about any sealed juvenile offender case, and law enforcement agents and public defenders can see nothing. Case type-based rules prevent any juvenile non-offender case from showing at any level. As a person-level identifier the JUVIS number at issue is not directly tied to the *cases* governed by the aforementioned statutes, but treating the JUVIS number differently from the cases results in an outcome contrary to statute. When a JABS user sees a JUVIS number connected to an individual on the search screen, that user can infer that individual's involvement in confidential cases—if there are no unsealed juvenile offender cases visible in someone's case history but they have a JUVIS number, the most likely reason would be confidential cases.[5] The judiciary is not treating these cases "as if they never occurred" while potentially flagging the presence of such cases to all users, even if those users cannot access anything substantive about the cases themselves.

To resolve the issue, the DDC should direct the JABS team to simply remove the JUVIS number from the list of identifiers found in the "Personal Identifier" dropdown menu. Doing so will bring the system into compliance with the statutes and result in little difference to end users, since those who need the number for representation should be able to obtain it from the individual or through court records. Since the change being requested is solely visual in nature—the DDC is not directing courts to disassociate JUVIS numbers from person records—users should still be able to search by a JUVIS number to get to an individual's person record, in case of a name change or some other circumstance in which a user would have a JUVIS number and not a name. However, if an individual searching by JUVIS number mistypes, they might look at the wrong record, and would have no way of discovering their error since the screen will no longer display the JUVIS number. If the DDC finds it necessary to cover such a use case, requirements that more closely mirror the statutes can be drawn up for the JABS team to implement.

The Washington National Guard's Use of JABS to Conduct Background Checks

The Washington National Guard uses its elevated access to conduct background checks on applicants for the military as a preliminary step before their applications packet is sent to the Department of Defense. The National Guard characterizes their use as a protection for applicants—their background checks ensure that a complete listing of court involvement is sent to the DOD, as any incomplete list could result in the eventual ejection of the applicant from the military and charges of Fraudulent

[5] A JUVIS number can be assigned during a dissolution of marriage action with children, but employees within AOC who work with juvenile records believed this to be a relatively small minority compared to the number of juveniles who received a JUVIS number from a juvenile offender or non-offender case.

Enlistment, meaning a total ban from membership in the armed forces for life. Regardless of the National Guard's intent, the DDC should prevent it from using elevated access to court records for background checks—this use is contrary to established DDC policy and results in the exposure of confidential court records. Because no proper use has been named by the National Guard at the time this memo is being written, the DDC should additionally deactivate the elevated WNG$ site.

First, background checks are generally not allowed under the JIS-Link Service Agreement that must be signed before JABS access is granted. Setting court users aside, JABS access is generally granted to three groups: law enforcement users, prosecutors, and public defenders. Each subscriber must sign a service agreement that contractually limits the use of JABS to the reason that entitles them to access the application in the first place in section 6.1: "[Subscriber agrees to ensure that]: Access and use of the JIS-Link service by its employees is only for the purpose of conducting official law enforcement business," for the law enforcement contract, for example. While the DDC has not specifically defined "official law enforcement business" in the past, court guidance can provide some insight into the term. In 2005, for example, the Washington State Supreme Court ruled that DOC internal records pertaining to inmate health care and medical personnel disciplinary actions could not be withheld from a Public Records Act request on the basis of an exception which allowed withholding of "Specific intelligence information and specific investigative records compiled by . . . law enforcement, and penology agencies, and state agencies vested with the responsibility to discipline members of any profession, the nondisclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy."[6] The Supreme Court reached this conclusion by using the Black's Law Dictionary definition of law enforcement ("The detection and punishment of violations of the law") and reasoning, then, that the investigations at hand were "not conducted for purposes of 'law enforcement.'" The Court even noted that investigations into medical malfeasance obviously *could* rise to the level of law enforcement, but DOC's purposes at issue were more administrative. Alternatively, see the various cases deciding the metes and bounds of judicial immunity. In *Adkins v. Clark County*, the Supreme Court upheld a decision granting judicial immunity to a bailiff who erroneously gave a dictionary to a jury,[7] but the Court of Appeals, Division III, withheld immunity from a court commissioner who erroneously processed an order withdrawing a warrant in *Mauro v. Kittitas County*.[8] The Supreme Court summarized the test in a few simple sentences, stating that "Judicial immunity shields judges from liability when they engage in judicial conduct without a clear absence of jurisdiction" and that judicial conduct is "something a judge normally does as part of his or her official duties." The bailiff, in this case, was

---

[6] Prison Legal News, Inc. v. Dep't of Corr., 154 Wash. 2d 628, 636 (2005) (citing RCW 42.17.310, recodified at RCW 42.56.240).
[7] *Adkins v. Clark Cnty.*, 105 Wash. 2d 675 (1986).
[8] *Lallas v. Skagit Cnty.*, 167 Wash. 2d 861 (2009).

performing a judge's duty when instructing the jury, but the commissioner processing an order was not.

"Official law enforcement business" then, can be defined as either the "detection and punishment of violations of the law" or "something a police officer normally does as part of his or her official duties." Under either, background checks for military applicants clearly fall outside the definition, and would be an administrative purpose.[9] That said, some privilege must have been granted to the National Guard in the past by either AOC or the DDC, as notes on the WNG$ site's JIS-Link administrative page confirm past AOC knowledge that military recruiters, and not military police or other law enforcement officials, have been using the access since 2011. That said, no records of such a decision can be found. AOC's recommendation is simply to remove this privilege—it is not to diminish the National Guard's access to being below that of similarly-situated requestors, but to standardize the purposes for which elevated access to court records may be used in a way that comports with statutory requirements and court rules.

In addition to the contract, the DDC has explicitly voted on this subject multiple times. Due to the broad access granted by applications such as JABS and JIS-Link when coupled with elevated access levels, the committee has historically been reluctant to expand the use of such applications. See, for example, the October 23, 2020, meeting when the Data Dissemination Committee required that the Washington State Supreme Court use public-level access and bulk data dissemination reports to conduct research, rather than using its own access to JABS. Judicial entities do not even use judicial records when making hiring decisions; Administrative Office of the Courts employees, for example, are fingerprinted by the Washington State Patrol and processed through WATCH as part of a background check before being hired by AOC. The position of the both AOC and the Data Dissemination Committee has historically been to follow Chapter 10.97 RCW, which states that "it is the policy of the state of Washington to provide for the completeness, accuracy, confidentiality, and security of criminal history record information and victim, witness, and complainant record information as defined in this chapter"[10] and requires that all courts and criminal justice agencies send disposition data to the Washington State Patrol.[11] Criminal background checks for employment purposes are properly conducted through WSP's Criminal Records Division's data, not through restricted court records, as statutes provide clear guidance to WSP regarding what data to disclose on a background check.

Second, as discussed above, the National Guard does not have access to many of the underlying cases it seeks through its background check processes; continuing to allow

---

[9] If law enforcement agents within the Washington National Guard were to use the JABS site for law enforcement purposes, AOC's recommendation would be to establish a public-level site for background checks alongside the existing elevated site. As of the writing of this memo, no such use has been identified by the Washington National Guard.
[10] RCW 10.97.010.
[11] RCW 10.97.045.

such checks creates confusion for all involved and puts applicants in a position where they are forced to reveal confidential cases. In the case at hand, the National Guard had no statutory right to know about the individual's dependency action, but the JUVIS number discovered through JABS signaled that there was some case history the applicant was failing to disclose. The individual thus had to disclose confidential case information or risk the National Guard believing they were hiding relevant history of court involvement. To make matters worse, such involvement would actually have had no impact on the individual's application; dependency actions are not sent from courts to federal agencies, and the DOD would have had no way of knowing that the individual left the dependency action off the application.

Third, new statutes clearly prohibit the National Guard's dissemination of sealed juvenile case information to the federal Department of Defense and signal a clear direction from the legislature on juvenile records. Specifically, see House Bill 2794 from 2020, which made several significant changes to RCW 13.50.260. Originally, subsection 8(d) stated that "The Washington state patrol shall ensure that the Washington state identification system provides criminal justice agencies access to sealed juvenile records information." The new bill changed "criminal justice agencies" to "Washington state criminal justice agencies". RCW 13.50.260(11) is unchanged, and states that "persons and agencies that obtain sealed juvenile records information pursuant to this section may communicate about this information with the respondent, but may not disseminate or be compelled to release the information to any person or agency not specifically granted access to sealed juvenile records in this section." The change in subsection 8 disallows federal criminal justice agencies from receiving sealed juvenile offender record, and, when coupled with subsection 11, now prohibits the National Guard from sending such records to federal agencies like the Department of Defense. AOC recognizes that the Washington National Guard acts as both a federal and state agency depending on its role, and can be governed by either set of laws depending on the specifics of a situation.[12] The new RCW 13.50.260 cleanly covers either scenario. When acting as a federal agency, the Washington National Guard is not allowed access to confidential juvenile records; when acting as a state agency, the Washington National Guard is allowed access to some,[13] but not allowed to disseminate any confidential juvenile records. While the statutes do authorize agencies to speak about confidential records with the subject of the records, the National Guard should ensure that it is the applicant who is disseminating any information about him- or herself, and not the National Guard.

Fourth, other military branches clearly have found public access to court records sufficient for their purposes. No relevant matches in our systems could be found when

---

[12] *See, e.g.* Adam Ashton, *State Military Department paying $110,000 to settle public records suit*, THE NEWS TRIBUNE, Apr. 1, 2015, *available at* https://www.thenewstribune.com/news/local/military/article26274163.html; Public Records Disclosure, WASH. MIL. DEP'T (last visited Aug. 16, 2021), https://mil.wa.gov/public-record-disclosure.

[13] That said, statutes clearly stipulate that such agencies may receive information through WASIS.

searching sites for “air”, and the last elevated Navy-related site closed in 2007. An old level 22 site called “US Army Recruiting” closed in 2013, and in 2018, a new billed and public-level site to replace it was established. According to billing records, the site has seen fairly high use nearly every month for the previous 12 months shown on the Administrative Portal. DDC staff are the points of contact for groups applying to obtain elevated JIS-Link and JABS access, and do not appear to have ever been contacted by any other branch of the military requesting the access that the National Guard had before June 25.

Finally, any practical benefit that the use of JABS may have granted has since largely been nullified by the release of the new JIS-Link application. Until just a few months ago, public users were required to use the old JIS-Link application, which was entirely keyboard-driven. JABS has always been web-based, and controlled largely via the mouse, making it more intuitive for modern users. It also groups together well-identified person records on one screen, making it uniquely valuable for background checks. The new application, however, is all of those things—it is web-based and mouse-driven, and groups well-identified person records together for convenience. Differences in security settings between a level 22 law enforcement account and a level 1 public account should similarly present no issues. The cases available to users of both levels are exactly the same. The differences are largely in the data presented for the case, and will likely make little difference to the National Guard—case financials, address history, identifiers, etc.