Cryptographic Techniques to Ensure Fair Randomness in Legal Processes

Henry Corrigan-Gibbs and Keith Winstein
Department of Computer Science
WASHINGTON — When a three-judge panel of the federal appeals court in California struck down bans last month on same-sex marriage in Idaho and Nevada, it was no surprise. The panel included two of the court’s leading liberals.

A group opposing same-sex marriage said the composition of the panel was also no coincidence. In an unusual accusation in a recent court filing, the group said the two judges served on a disproportionate number of cases involving gay rights.
Random assignment
Random assignment of Judges to Panels.
WASHINGTON — When a three-judge panel of the federal appeals court in California struck down bans last month on same-sex marriage in Idaho and Nevada, it was no surprise. The panel included two of the court’s leading liberals.

A group opposing same-sex marriage said the composition of the panel was also no coincidence. In an unusual accusation in a recent court filing, the group said the two judges served on a disproportionate number of cases involving gay rights.
WASHINGTON — When a three-judge panel of the federal appeals court in California struck down bans last month on same-sex marriage in Idaho and Nevada, it was no surprise. The panel included two of the court’s leading liberals.

A group opposing same-sex marriage said the composition of the panel was also no coincidence. In an unusual accusation in a recent court filing, the group said the two judges served on a disproportionate number of cases involving gay rights.
WASHINGTON — When a three-judge panel of the federal appeals court in California struck down bans last month on same-sex marriage in Idaho and Nevada, it was no surprise. The panel included two of the court’s leading liberals.

A group opposing same-sex marriage said the composition of the panel was also no coincidence. In an unusual accusation in a recent court filing, the group said the two judges served on a disproportionate number of cases involving gay rights.

At the same time, a new study by two law professors supports the idea that many federal appeals courts are not selecting their panels perfectly randomly.
“We found strong evidence in the majority of circuits that they’re not using a random assignment process to form their panels,” said Marin K. Levy, a law professor at Duke and one of the study’s authors.
“We found strong evidence in the majority of circuits that they’re not using a random assignment process to form their panels,” said Marin K. Levy, a law professor at Duke and one of the study’s authors.

Adam S. Chilton, a law professor at the University of Chicago and the study’s other author, said there was only a two percent probability that the real panels were generated by pure chance.
“We found strong evidence in the majority of circuits that they’re not using a random assignment process to form their panels,” said Marin K. Levy, a law professor at Duke and one of the study’s authors.

Adam S. Chilton, a law professor at the University of Chicago and the study’s other author, said there was only a two percent probability that the real panels were generated by pure chance.

“If any of the 12 circuits are using a nonrandom process,” he said, “it’s most likely to be the Ninth Circuit.”
*Draft Document*

Challenging the Randomness of Panel Assignment in the Federal Courts of Appeals

Adam S. Chilton* & Marin K. Levy**

ABSTRACT

A fundamental academic assumption about the federal courts of appeals is that the three-judge panels that hear cases have been randomly configured. Scores of scholarly articles have noted this “fact,” and it has been relied on heavily by empirical researchers. Even though there are practical reasons to doubt that judges would always be randomly assigned to panels, this assumption has never been tested. This Article fill this void by doing so.

To determine whether the circuit courts utilize random assignment, we have created what we believe to be the largest dataset of panel assignments of those courts constructed to date. Using this dataset, we tested whether panel assignments are, in fact, random by comparing the actual assignments to truly random panels generated by code that we have created to simulate the panel generation process. Our results show evidence of non-randomness in the majority of the federal courts of appeals. Moreover, our findings specifically show a lack of randomness along several key dimensions: the distribution of conservative judges, female judges, and minority judges.

To be sure, the analysis here is descriptive, not explanatory or normative. We do not ourselves mean to suggest that “perfect randomness” is a desirable goal. We are simply testing an existing assumption.
Biased assignment

Judges

Panels
Biased assignment
Biased assignment

Judges

Panels
Biased assignment

Judges

Panels

Biased assignment
Beyond panel assignments...
Panel assignments are just one example of an important (but opaque) computerized government process:
Panel assignments are just one example of an important (but opaque) computerized government process:

- visa lotteries
- tax audits
- airport screening
- school lotteries

Beyond panel assignments...
Panel assignments are just one example of an important (but opaque) computerized government process:

- visa lotteries, tax audits, airport screening,
- school lotteries, etc.

**Risk:** “Black-box” algorithms and processes may exhibit subtle biases and faults.
Panel assignments are just one example of an important (but opaque) computerized government process:
  visa lotteries, tax audits, airport screening, school lotteries, etc.

**Risk:** “Black-box” algorithms and processes may exhibit subtle biases and faults.

**Hope:** Cryptographic tools can make almost any algorithm open and accountable.
Plan
Plan

**PART I:** Have the federal Courts of Appeals been using biased randomness in their panel assignments?
Plan

**PART I:** Have the federal Courts of Appeals been using biased randomness in their panel assignments?

**PART II:** How can we ensure that the government faithfully executes a random process?
Plan

PART I: Have the federal Courts of Appeals been using biased randomness in their panel assignments?

The study has two major design flaws. These flaws invalidate the study’s claims.

PART II: How can we ensure that the government faithfully executes a random process?
Plan

PART I: Have the federal Courts of Appeals been using biased randomness in their panel assignments?

The study has two major design flaws.
These flaws invalidate the study’s claims.

PART II: How can we ensure that the government faithfully executes a random process?

These cryptographic techniques also apply to:
visa lotteries, tax audits, airport screening, school lotteries, etc.
PART I
The Perils of Retrospective Analysis

PART II
Cryptographic Techniques to Ensure Fair Randomness
PART I
The Perils of Retrospective Analysis

PART II
Cryptographic Techniques to Ensure Fair Randomness
Challenging the Randomness of Panel Assignment in the Federal Courts of Appeals

Adam S. Chilton* & Marin K. Levy**

ABSTRACT

A fundamental academic assumption about the federal courts of appeals is that the three-judge panels that hear cases have been randomly configured. Scores of scholarly articles have noted this “fact,” and it has been relied on heavily by empirical researchers. Even though there are practical reasons to doubt that judges would always be randomly assigned to panels, this assumption has never been tested. This Article fills this void by doing so.

To determine whether the circuit courts utilize random assignment, we have created what we believe to be the largest dataset of panel assignments of those courts constructed to date. Using this dataset, we tested whether panel assignments are, in fact, random by comparing the actual assignments to truly random panels generated by code that we have created to simulate the panel generation process. Our results show evidence of non-randomness in the majority of the federal courts of appeals. Moreover, our findings specifically show a lack of randomness along several key dimensions: the distribution of conservative judges, female judges, and minority judges.

To be sure, the analysis here is descriptive, not explanatory or normative. We do not ourselves mean to suggest that “perfect randomness” is a desirable goal. We are simply testing an existing assumption.
Study Methods
Study Methods

1. **Prepare** a set of 144 hypotheses to test.
   
   e.g., H59: *The number of all-female panels in the 2nd Circuit is consistent with a random assignment.*
Study Methods

1. **Prepare** a set of 144 hypotheses to test.
   
   e.g., H59: *The number of all-female panels in the 2nd Circuit is consistent with a random assignment.*

2. **Collect** a data set of the actual panel assignments in 12 U.S. Courts of Appeals.
Study Methods

1. **Prepare** a set of 144 hypotheses to test.
   e.g., H59: *The number of all-female panels in the 2nd Circuit is consistent with a random assignment.*

2. **Collect** a data set of the actual panel assignments in 12 U.S. Courts of Appeals.

3. **Test** how likely the actual panel assignments would be under a truly random (ideal) assignment.
# Appendix B: Simulated Distribution of Female Judges

<table>
<thead>
<tr>
<th>D.C. Circuit</th>
<th>Actual Panels</th>
<th>Simulated Mean</th>
<th>90% Confidence Interval</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Women</td>
<td>158</td>
<td>166</td>
<td>149 - 184</td>
<td></td>
</tr>
<tr>
<td>1 Women</td>
<td>272</td>
<td>261</td>
<td>242 - 279</td>
<td></td>
</tr>
<tr>
<td>2 Women</td>
<td>77</td>
<td>79</td>
<td>66 - 93</td>
<td></td>
</tr>
<tr>
<td>3 Women</td>
<td>3</td>
<td>4</td>
<td>1 - 7</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1st Circuit</th>
<th>Actual Panels</th>
<th>Simulated Mean</th>
<th>90% Confidence Interval</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Women</td>
<td>131</td>
<td>137</td>
<td>123 - 150</td>
<td></td>
</tr>
<tr>
<td>1 Women</td>
<td>148</td>
<td>140</td>
<td>126 - 154</td>
<td></td>
</tr>
<tr>
<td>2 Women</td>
<td>18</td>
<td>21</td>
<td>14 - 29</td>
<td></td>
</tr>
<tr>
<td>3 Women</td>
<td>1</td>
<td>0</td>
<td>0 - 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2nd Circuit</th>
<th>Actual Panels</th>
<th>Simulated Mean</th>
<th>90% Confidence Interval</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Women</td>
<td>558</td>
<td>570</td>
<td>540 - 600</td>
<td></td>
</tr>
<tr>
<td>1 Women</td>
<td>608</td>
<td>594</td>
<td>564 - 624</td>
<td></td>
</tr>
<tr>
<td>2 Women</td>
<td>155</td>
<td>160</td>
<td>141 - 180</td>
<td></td>
</tr>
<tr>
<td>3 Women</td>
<td>11</td>
<td>11</td>
<td>6 - 16</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3rd Circuit</th>
<th>Actual Panels</th>
<th>Simulated Mean</th>
<th>90% Confidence Interval</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Women</td>
<td>311</td>
<td>296</td>
<td>275 - 317</td>
<td>***</td>
</tr>
<tr>
<td>1 Women</td>
<td>263</td>
<td>297</td>
<td>275 - 318</td>
<td>**</td>
</tr>
<tr>
<td>2 Women</td>
<td>93</td>
<td>72</td>
<td>59 - 86</td>
<td></td>
</tr>
<tr>
<td>3 Women</td>
<td>2</td>
<td>4</td>
<td>1 - 8</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4th Circuit</th>
<th>Actual Panels</th>
<th>Simulated Mean</th>
<th>90% Confidence Interval</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Women</td>
<td>263</td>
<td>263</td>
<td>243 - 283</td>
<td></td>
</tr>
<tr>
<td>1 Women</td>
<td>266</td>
<td>268</td>
<td>248 - 288</td>
<td></td>
</tr>
<tr>
<td>2 Women</td>
<td>67</td>
<td>62</td>
<td>50 - 75</td>
<td></td>
</tr>
<tr>
<td>3 Women</td>
<td>1</td>
<td>3</td>
<td>1 - 6</td>
<td>*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5th Circuit</th>
<th>Actual Panels</th>
<th>Simulated Mean</th>
<th>90% Confidence Interval</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Women</td>
<td>271</td>
<td>278</td>
<td>256 - 301</td>
<td></td>
</tr>
<tr>
<td>1 Women</td>
<td>422</td>
<td>419</td>
<td>394 - 443</td>
<td></td>
</tr>
<tr>
<td>2 Women</td>
<td>176</td>
<td>164</td>
<td>145 - 183</td>
<td></td>
</tr>
<tr>
<td>3 Women</td>
<td>8</td>
<td>16</td>
<td>10 - 23</td>
<td>**</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6th Circuit</th>
<th>Actual Panels</th>
<th>Simulated Mean</th>
<th>90% Confidence Interval</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Women</td>
<td>391</td>
<td>392</td>
<td>366 - 419</td>
<td></td>
</tr>
<tr>
<td>1 Women</td>
<td>566</td>
<td>563</td>
<td>534 - 591</td>
<td></td>
</tr>
<tr>
<td>2 Women</td>
<td>219</td>
<td>226</td>
<td>204 - 248</td>
<td></td>
</tr>
<tr>
<td>3 Women</td>
<td>30</td>
<td>25</td>
<td>17 - 33</td>
<td></td>
</tr>
</tbody>
</table>
Problem 1: Multiple Hypothesis Testing
Problem 1: Multiple Hypothesis Testing

- When testing 144 hypotheses at the $p < 0.1$ level, we expect 14 “false discoveries” by random chance alone.
Problem 1: Multiple Hypothesis Testing

- When testing 144 hypotheses at the $p < 0.1$ level, we expect 14 “false discoveries” by random chance alone.

- Even if all courts are using good randomness, C-L will falsely accuse eight circuits of bad behavior on average.
Why can multiple hypothesis testing be problematic?
Why can multiple hypothesis testing be problematic?

*By analogy…* Say that every day, every state lottery picks a number between 1 and 50.
Why can multiple hypothesis testing be problematic?

*By analogy…* Say that every day, every state lottery picks a number between 1 and 50.

THE LOTTONS ARE USING BAD RANDOMNESS!!! They always draw number 18 on Thursday.
Why can multiple hypothesis testing be problematic?

*By analogy…* Say that every day, every state lottery picks a number between 1 and 50.

**THE LOTTO ARE USING BAD RANDOMNESS!!!** They always draw number 18 on Thursday.

Really? Let’s check next Thursday…
<table>
<thead>
<tr>
<th>State</th>
<th>Value</th>
<th>State</th>
<th>Value</th>
<th>State</th>
<th>Value</th>
<th>State</th>
<th>Value</th>
<th>State</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>2</td>
<td>Hawaii</td>
<td>12</td>
<td>Mass.</td>
<td>38</td>
<td>N.M.</td>
<td>39</td>
<td>S.D.</td>
<td>11</td>
</tr>
<tr>
<td>Alaska</td>
<td>32</td>
<td>Idaho</td>
<td>13</td>
<td>Michigan</td>
<td>12</td>
<td>New York</td>
<td>27</td>
<td>Tenn.</td>
<td>6</td>
</tr>
<tr>
<td>Arizona</td>
<td>17</td>
<td>Illinois</td>
<td>13</td>
<td>Minn.</td>
<td>9</td>
<td>N.C.</td>
<td>42</td>
<td>Texas</td>
<td>32</td>
</tr>
<tr>
<td>Arkansas</td>
<td>43</td>
<td>Indiana</td>
<td>46</td>
<td>Miss.</td>
<td>15</td>
<td>N.D.</td>
<td>12</td>
<td>Utah</td>
<td>29</td>
</tr>
<tr>
<td>California</td>
<td>6</td>
<td>Iowa</td>
<td>18</td>
<td>Missouri</td>
<td>50</td>
<td>Ohio</td>
<td>17</td>
<td>Vermont</td>
<td>2</td>
</tr>
<tr>
<td>Colorado</td>
<td>4</td>
<td>Kansas</td>
<td>39</td>
<td>Montana</td>
<td>8</td>
<td>Okla.</td>
<td>47</td>
<td>Virginia</td>
<td>12</td>
</tr>
<tr>
<td>Conn.</td>
<td>12</td>
<td>Kentucky</td>
<td>17</td>
<td>Nebraska</td>
<td>27</td>
<td>Oregon</td>
<td>23</td>
<td>Wash.</td>
<td>8</td>
</tr>
<tr>
<td>Delaware</td>
<td>43</td>
<td>Louisiana</td>
<td>1</td>
<td>Nevada</td>
<td>31</td>
<td>Penn.</td>
<td>18</td>
<td>W. Va.</td>
<td>30</td>
</tr>
<tr>
<td>Florida</td>
<td>32</td>
<td>Maine</td>
<td>34</td>
<td>N.H.</td>
<td>47</td>
<td>R.I.</td>
<td>5</td>
<td>Wisc.</td>
<td>9</td>
</tr>
<tr>
<td>Georgia</td>
<td>48</td>
<td>Maryland</td>
<td>11</td>
<td>N.J.</td>
<td>7</td>
<td>S.C.</td>
<td>2</td>
<td>Wyoming</td>
<td>7</td>
</tr>
<tr>
<td>State</td>
<td>Number</td>
<td>State</td>
<td>Number</td>
<td>State</td>
<td>Number</td>
<td>State</td>
<td>Number</td>
<td>State</td>
<td>Number</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>Alabama</td>
<td>2</td>
<td>Hawai'i</td>
<td>12</td>
<td>Mass.</td>
<td>38</td>
<td>N.M.</td>
<td>39</td>
<td>S.D.</td>
<td>11</td>
</tr>
<tr>
<td>Alaska</td>
<td>32</td>
<td>Idaho</td>
<td>13</td>
<td>Michigan</td>
<td>12</td>
<td>New York</td>
<td>27</td>
<td>Tenn.</td>
<td>6</td>
</tr>
<tr>
<td>Arizona</td>
<td>17</td>
<td>Illinois</td>
<td>13</td>
<td>Minn.</td>
<td>9</td>
<td>N.C.</td>
<td>42</td>
<td>Texas</td>
<td>32</td>
</tr>
<tr>
<td>Arkansas</td>
<td>43</td>
<td>Indiana</td>
<td>46</td>
<td>Miss.</td>
<td>15</td>
<td>N.D.</td>
<td>12</td>
<td>Utah</td>
<td>29</td>
</tr>
<tr>
<td>California</td>
<td>6</td>
<td>Iowa</td>
<td>18</td>
<td>Missouri</td>
<td>50</td>
<td>Ohio</td>
<td>17</td>
<td>Vermont</td>
<td>2</td>
</tr>
<tr>
<td>Colorado</td>
<td>4</td>
<td>Kansas</td>
<td>39</td>
<td>Montana</td>
<td>8</td>
<td>Okla.</td>
<td>47</td>
<td>Virginia</td>
<td>12</td>
</tr>
<tr>
<td>Conn.</td>
<td>12</td>
<td>Kentucky</td>
<td>17</td>
<td>Nebraska</td>
<td>27</td>
<td>Oregon</td>
<td>23</td>
<td>Wash.</td>
<td>8</td>
</tr>
<tr>
<td>Delaware</td>
<td>43</td>
<td>Louisiana</td>
<td>1</td>
<td>Nevada</td>
<td>31</td>
<td>Penn.</td>
<td>18</td>
<td>W. Va.</td>
<td>30</td>
</tr>
<tr>
<td>Florida</td>
<td>32</td>
<td>Maine</td>
<td>34</td>
<td>N.H.</td>
<td>47</td>
<td>R.I.</td>
<td>5</td>
<td>Wisc.</td>
<td>9</td>
</tr>
<tr>
<td>Georgia</td>
<td>48</td>
<td>Maryland</td>
<td>11</td>
<td>N.J.</td>
<td>7</td>
<td>S.C.</td>
<td>2</td>
<td>Wyoming</td>
<td>7</td>
</tr>
<tr>
<td>State</td>
<td>Rank</td>
<td>State</td>
<td>Rank</td>
<td>State</td>
<td>Rank</td>
<td>State</td>
<td>Rank</td>
<td>State</td>
<td>Rank</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>------------</td>
<td>------</td>
<td>------------</td>
<td>------</td>
<td>------------</td>
<td>------</td>
<td>------------</td>
<td>------</td>
</tr>
<tr>
<td>Alabama</td>
<td>2</td>
<td>Hawaii</td>
<td>12</td>
<td>Mass.</td>
<td>38</td>
<td>N.M.</td>
<td>39</td>
<td>S.D.</td>
<td>11</td>
</tr>
<tr>
<td>Alaska</td>
<td>32</td>
<td>Idaho</td>
<td>13</td>
<td>Michigan</td>
<td>12</td>
<td>New York</td>
<td>27</td>
<td>Tenn.</td>
<td>6</td>
</tr>
<tr>
<td>Arizona</td>
<td>17</td>
<td>Illinois</td>
<td>13</td>
<td>Minn.</td>
<td>9</td>
<td>N.C.</td>
<td>42</td>
<td>Texas</td>
<td>32</td>
</tr>
<tr>
<td>Arkansas</td>
<td>43</td>
<td>Indiana</td>
<td>46</td>
<td>Miss.</td>
<td>15</td>
<td>N.D.</td>
<td>12</td>
<td>Utah</td>
<td>29</td>
</tr>
<tr>
<td>California</td>
<td>6</td>
<td>Iowa</td>
<td>18</td>
<td>Missouri</td>
<td>50</td>
<td>Ohio</td>
<td>17</td>
<td>Vermont</td>
<td>2</td>
</tr>
<tr>
<td>Colorado</td>
<td>4</td>
<td>Kansas</td>
<td>39</td>
<td>Montana</td>
<td>8</td>
<td>Okla.</td>
<td>47</td>
<td>Virginia</td>
<td>12</td>
</tr>
<tr>
<td>Conn.</td>
<td>12</td>
<td>Kentucky</td>
<td>17</td>
<td>Nebraska</td>
<td>27</td>
<td>Oregon</td>
<td>23</td>
<td>Wash.</td>
<td>8</td>
</tr>
<tr>
<td>Delaware</td>
<td>43</td>
<td>Louisiana</td>
<td>1</td>
<td>Nevada</td>
<td>31</td>
<td>Penn.</td>
<td>18</td>
<td>W. Va.</td>
<td>30</td>
</tr>
<tr>
<td>Florida</td>
<td>32</td>
<td>Maine</td>
<td>34</td>
<td>N.H.</td>
<td>47</td>
<td>R.I.</td>
<td>5</td>
<td>Wisc.</td>
<td>9</td>
</tr>
<tr>
<td>Georgia</td>
<td>48</td>
<td>Maryland</td>
<td>11</td>
<td>N.J.</td>
<td>7</td>
<td>S.C.</td>
<td>2</td>
<td>Wyoming</td>
<td>7</td>
</tr>
</tbody>
</table>

Scientist Discovers Evidence of Fraud in Iowa and Pennsylvania State Lotteries
<table>
<thead>
<tr>
<th>State</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>12</td>
</tr>
<tr>
<td>Alaska</td>
<td>32</td>
</tr>
<tr>
<td>Arizona</td>
<td>17</td>
</tr>
<tr>
<td>Arkansas</td>
<td>43</td>
</tr>
<tr>
<td>California</td>
<td>6</td>
</tr>
<tr>
<td>Colorado</td>
<td>4</td>
</tr>
<tr>
<td>Conn.</td>
<td>12</td>
</tr>
<tr>
<td>Delaware</td>
<td>43</td>
</tr>
<tr>
<td>Florida</td>
<td>32</td>
</tr>
<tr>
<td>Georgia</td>
<td>48</td>
</tr>
<tr>
<td>Hawaii</td>
<td>12</td>
</tr>
<tr>
<td>Idaho</td>
<td>13</td>
</tr>
<tr>
<td>Illinois</td>
<td>13</td>
</tr>
<tr>
<td>Indiana</td>
<td>46</td>
</tr>
<tr>
<td>Iowa</td>
<td>18</td>
</tr>
<tr>
<td>Kansas</td>
<td>39</td>
</tr>
<tr>
<td>Kentucky</td>
<td>17</td>
</tr>
<tr>
<td>Louisiana</td>
<td>1</td>
</tr>
<tr>
<td>Maine</td>
<td>34</td>
</tr>
<tr>
<td>Maryland</td>
<td>11</td>
</tr>
<tr>
<td>Mass.</td>
<td>38</td>
</tr>
<tr>
<td>Michigan</td>
<td>12</td>
</tr>
<tr>
<td>Minn.</td>
<td>9</td>
</tr>
<tr>
<td>Miss.</td>
<td>15</td>
</tr>
<tr>
<td>Missouri</td>
<td>50</td>
</tr>
<tr>
<td>Montana</td>
<td>8</td>
</tr>
<tr>
<td>Nebraska</td>
<td>27</td>
</tr>
<tr>
<td>Nevada</td>
<td>31</td>
</tr>
<tr>
<td>N.H.</td>
<td>47</td>
</tr>
<tr>
<td>N.J.</td>
<td>7</td>
</tr>
<tr>
<td>N.M.</td>
<td>39</td>
</tr>
<tr>
<td>New York</td>
<td>27</td>
</tr>
<tr>
<td>N.C.</td>
<td>42</td>
</tr>
<tr>
<td>N.D.</td>
<td>12</td>
</tr>
<tr>
<td>Ohio</td>
<td>17</td>
</tr>
<tr>
<td>Okla.</td>
<td>47</td>
</tr>
<tr>
<td>Oregon</td>
<td>23</td>
</tr>
<tr>
<td>Penn.</td>
<td>18</td>
</tr>
<tr>
<td>R.I.</td>
<td>5</td>
</tr>
<tr>
<td>S.C.</td>
<td>2</td>
</tr>
<tr>
<td>S.D.</td>
<td>11</td>
</tr>
<tr>
<td>Tenn.</td>
<td>6</td>
</tr>
<tr>
<td>Texas</td>
<td>32</td>
</tr>
<tr>
<td>Utah</td>
<td>29</td>
</tr>
<tr>
<td>Vermont</td>
<td>2</td>
</tr>
<tr>
<td>Virginia</td>
<td>12</td>
</tr>
<tr>
<td>Wash.</td>
<td>8</td>
</tr>
<tr>
<td>W. Va.</td>
<td>30</td>
</tr>
<tr>
<td>Wisc.</td>
<td>9</td>
</tr>
<tr>
<td>Wyoming</td>
<td>7</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>Alabama</td>
<td>2</td>
</tr>
<tr>
<td>Alaska</td>
<td>32</td>
</tr>
<tr>
<td>Arizona</td>
<td>17</td>
</tr>
<tr>
<td>Arkansas</td>
<td>43</td>
</tr>
<tr>
<td>California</td>
<td>6</td>
</tr>
<tr>
<td>Colorado</td>
<td>4</td>
</tr>
<tr>
<td>Conn.</td>
<td>12</td>
</tr>
<tr>
<td>Delaware</td>
<td>43</td>
</tr>
<tr>
<td>Florida</td>
<td>32</td>
</tr>
<tr>
<td>Georgia</td>
<td>48</td>
</tr>
<tr>
<td>State</td>
<td>Rank</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
</tr>
<tr>
<td>Alabama</td>
<td>2</td>
</tr>
<tr>
<td>Alaska</td>
<td>32</td>
</tr>
<tr>
<td>Arizona</td>
<td>17</td>
</tr>
<tr>
<td>Arkansas</td>
<td>43</td>
</tr>
<tr>
<td>California</td>
<td>6</td>
</tr>
<tr>
<td>Colorado</td>
<td>4</td>
</tr>
<tr>
<td>Conn.</td>
<td>12</td>
</tr>
<tr>
<td>Delaware</td>
<td>43</td>
</tr>
<tr>
<td>Florida</td>
<td>32</td>
</tr>
<tr>
<td>Georgia</td>
<td>48</td>
</tr>
</tbody>
</table>
Wait a minute…

Even if the lottery weren’t rigged, we would expect to see a few **18**s just by random chance.
Problem 1: Multiple Hypothesis Testing
Problem 1: Multiple Hypothesis Testing

*The Courts of Appeals study falls into the same trap:*
Problem 1: Multiple Hypothesis Testing

The Courts of Appeals study falls into the same trap:

The authors run a large number of statistical tests (144) and find 21 significant results.
Problem 1: Multiple Hypothesis Testing

*The Courts of Appeals study falls into the same trap:* The authors run a large number of statistical tests (144) and find 21 significant results.

- The probability that we would see these results due to random chance is > 5%.
Problem 1: Multiple Hypothesis Testing

*The Courts of Appeals study falls into the same trap:* 

The authors run a large number of statistical tests (144) and find 21 significant results.

- The probability that we would see these results due to random chance is > 5%.

“[T]here is evidence that the ideological balance of panels is non-random in five circuits: the D.C. Circuit, the Second Circuit, the Fourth Circuit, the Eight Circuit, and the Ninth Circuit.”
Problem 1: Multiple Hypothesis Testing

The Courts of Appeals study falls into the same trap:
The authors run a large number of statistical tests (144) and find 21 significant results.

- The probability that we would see these results due to random chance is > 5%.

“[T]here is evidence that the ideological balance of panels is non-random in five circuits: the D.C. Circuit, the Second Circuit, the Fourth Circuit, the Eight Circuit, and the Ninth Circuit.”

- As in the lotto example: we expect false discoveries due to chance alone. We expect more than four false discoveries, the study finds five.
Problem 1: Multiple Hypothesis Testing

The Courts of Appeals study falls into the same trap:

The authors run a large number of statistical tests (144) and find 21 significant results.

- The probability that we would see these results due to random chance is > 5%.

“[T]here is evidence that the ideological balance of panels is non-random in five circuits: the D.C. Circuit, the Second Circuit, the Fourth Circuit, the Eight Circuit, and the Ninth Circuit.”

- As in the lotto example: we expect false discoveries due to chance alone. We expect more than four false discoveries, the study finds five.

“[T]here was evidence of non-randomness in seven of the twelve region circuits”
Problem 1: Multiple Hypothesis Testing

The Courts of Appeals study falls into the same trap:

The authors run a large number of statistical tests (144) and find 21 significant results.

- The probability that we would see these results due to random chance is > 5%.

“[T]here is evidence that the ideological balance of panels is non-random in five circuits: the D.C. Circuit, the Second Circuit, the Fourth Circuit, the Eight Circuit, and the Ninth Circuit.”

- As in the lotto example: we expect false discoveries due to chance alone. We expect more than four false discoveries, the study finds five.

“[T]here was evidence of non-randomness in seven of the twelve region circuits”

- By chance alone, we would expect to find such statistical deviations in more than eight circuits.
Problem 1: Multiple Hypothesis Testing

The Courts of Appeals study falls into the same trap:

The authors run a large number of statistical tests (144) and find 21 significant results.

- The probability that we would see these results due to random chance is > 5%.

“[T]here is evidence that the ideological balance of panels is non-random in five circuits: the D.C. Circuit, the Second Circuit, the Fourth Circuit, the Eight Circuit, and the Ninth Circuit.”

- As in the lotto example: we expect false discoveries due to chance alone. We expect more than four false discoveries, the study finds five.

“[T]here was evidence of non-randomness in seven of the twelve region circuits”

- By chance alone, we would expect to find such statistical deviations in more than eight circuits.
Problem 2: “Cherry-Picking” Hypotheses
Problem 2: “Cherry-Picking” Hypotheses

Problem 2: “Cherry-Picking” Hypotheses


Nov 12  We explain our concerns about the study design to the authors via email.
Problem 2: “Cherry-Picking” Hypotheses


Nov 12  We explain our concerns about the study design to the authors via email.

Nov 17  We post a note to SSRN explaining the problems with the study’s methods.
Problem 2: “Cherry-Picking” Hypotheses


Nov 12  We explain our concerns about the study design to the authors via email.

Nov 17  We post a note to SSRN explaining the problems with the study’s methods.

Jan 3, 2015  The authors send us a revised draft for comment.
Problem 2: “Cherry-Picking” Hypotheses


Nov 12  We explain our concerns about the study design to the authors via email.

Nov 17  We post a note to SSRN explaining the problems with the study’s methods.

Jan 3, 2015  The authors send us a revised draft for comment.

• In the revising the paper, the authors altered their statistical tests and *discarded two thirds of their hypotheses.*
Problem 2: “Cherry-Picking” Hypotheses


Nov 12  We explain our concerns about the study design to the authors via email.

Nov 17  We post a note to SSRN explaining the problems with the study’s methods.

Jan 3, 2015  The authors send us a revised draft for comment.

- In the revising the paper, the authors altered their statistical tests and **discarded two thirds of their hypotheses**.
- They discarded the hypotheses that the data set didn’t support (i.e., with the weakest $p$-values).
Problem 2: “Cherry-Picking” Hypotheses


Nov 12  We explain our concerns about the study design to the authors via email.

Nov 17  We post a note to SSRN explaining the problems with the study’s methods.

Jan 3, 2015  The authors send us a revised draft for comment.

  • In the revising the paper, the authors altered their statistical tests and discarded two thirds of their hypotheses.
  • They discarded the hypotheses that the data set didn’t support (i.e., with the weakest $p$-values).

**Problem:** Editing the hypotheses after running the statistical tests can lead to spurious findings (“$p$-hacking”).
Problem 2: “Cherry-Picking” Hypotheses

Example: Say you run a medical trial comparing Aspirin vs New Drug X.
Problem 2: “Cherry-Picking” Hypotheses

Example: Say you run a medical trial comparing Aspirin vs New Drug X.
Problem 2: “Cherry-Picking” Hypotheses

Example: Say you run a medical trial comparing Aspirin vs New Drug X.
Problem 2: “Cherry-Picking” Hypotheses

Example: Say you run a medical trial comparing Aspirin vs New Drug X.
Problem 2: “Cherry-Picking” Hypotheses

Example: Say you run a medical trial comparing Aspirin vs New Drug X.
Problem 2: “Cherry-Picking” Hypotheses

Example: Say you run a medical trial comparing Aspirin vs New Drug X.
Problem 2: “Cherry-Picking” Hypotheses

Example: Say you run a medical trial comparing Aspirin vs New Drug X.

Clinical Trial Finds New Drug X Safer Than Aspirin Among Men
Outcome
Outcome

• In response to the authors’ request, we reviewed an updated draft.
Outcome

• In response to the authors’ request, we reviewed an updated draft.

• We replied that omitting the weaker results from the final paper is not legitimate (this would amount to $p$-hacking).
• In response to the authors’ request, we reviewed an updated draft.

• We replied that omitting the weaker results from the final paper is not legitimate (this would amount to $p$-hacking).

In response to the authors’ request, we reviewed an updated draft.

We replied that omitting the weaker results from the final paper is not legitimate (this would amount to p-hacking).

“A recent article, however, employing sophisticated statistical methods, identifies four circuits—D.C., Second, Eighth, and Ninth—in which assignments are not random, but indeed appear to produce an ideological slant.”

In response to the authors’ request, we reviewed an updated draft. We replied that omitting the weaker results from the final paper is not legitimate (this would amount to p-hacking).

Result:


“A recent article, however, employing sophisticated statistical methods, identifies four circuits—D.C., Second, Eighth, and Ninth—in which assignments are not random, but indeed appear to produce an ideological slant. The study provides no quantitative evidence for this claim.
Recommendations
Recommendations

For lawyers: Be wary of statistical claims; it is easy to generate spurious “statistically significant” ($p < 0.05$) findings:
Recommendations

For lawyers: Be wary of statistical claims; it is easy to generate spurious “statistically significant” ($p < 0.05$) findings:

Bad Science
Recommendations

For lawyers: Be wary of statistical claims; it is easy to generate spurious “statistically significant” \((p < 0.05)\) findings:

Bad Science
  • Run 20 independent studies.
For lawyers: Be wary of statistical claims; it is easy to generate spurious “statistically significant” ($p < 0.05$) findings:

Bad Science
- Run 20 independent studies.
  → On average, one will yield a “significant” result.
Recommendations

For lawyers: Be wary of statistical claims; it is easy to generate spurious “statistically significant” ($p < 0.05$) findings:

Bad Science

- Run 20 independent studies.
  - On average, one will yield a “significant” result.
- Discard the 19 non-significant results.
Recommendations

For lawyers: Be wary of statistical claims; it is easy to generate spurious “statistically significant” ($p < 0.05$) findings:

Bad Science
- Run 20 independent studies.
  - On average, one will yield a “significant” result.
- Discard the 19 non-significant results.
- Insert the “significant” result into your petition.
Recommendations

For lawyers: Be wary of statistical claims; it is easy to generate spurious “statistically significant” \((p < 0.05)\) findings:

Bad Science
- Run 20 independent studies.
  - On average, one will yield a “significant” result.
- Discard the 19 non-significant results.
- Insert the “significant” result into your petition.

For law review editors: Consider consulting external reviewers about papers with a heavy computational or statistical angle.
PART I
The Perils of Retrospective Analysis

PART II
Cryptographic Techniques to Ensure Fair Randomness
PART I
The Perils of Retrospective Analysis

PART II
Cryptographic Techniques
to Ensure Fair Randomness
Randomness

The Chilton-Levy study raises a provocative question:

How can the public be sure that the assignments are random?
Randomness

The Chilton-Levy study raises a provocative question:
How can the public be sure that the assignments are random?
Randomness

The Chilton-Levy study raises a provocative question:
How can the public be sure that the assignments are random?
The Chilton-Levy study raises a provocative question:
How can the public be sure that the assignments are random?
The Chilton-Levy study raises a provocative question: How can the public be sure that the assignments are random?
The Chilton-Levy study raises a provocative question: How can the public be sure that the assignments are random?
The Chilton-Levy study raises a provocative question: How can the public be sure that the assignments are random?
The Chilton-Levy study raises a provocative question: How can the public be sure that the assignments are random?
Other Applications
Other Applications

Verifiable randomness sources have a host of other applications:
[Bonneau et al. 2015] [Kroll et al., 2017]
Other Applications

Verifiable randomness sources have a host of other applications:
[Bonneau et al. 2015] [Kroll et al., 2017]

• Visa lottery
Other Applications

Verifiable randomness sources have a host of other applications: [Bonneau et al. 2015] [Kroll et al., 2017]

- Visa lottery
- Actual lottery
Verifiable randomness sources have a host of other applications: [Bonneau et al. 2015] [Kroll et al., 2017]

- Visa lottery
- Actual lottery
- IRS audits
Verifiable randomness sources have a host of other applications:
[Bonneau et al. 2015] [Kroll et al., 2017]

- Visa lottery
- Actual lottery
- IRS audits
- Random screening at airports (customs, security, etc.)
Other Applications

Verifiable randomness sources have a host of other applications:
[Bonneau et al. 2015] [Kroll et al., 2017]

- Visa lottery
- Actual lottery
- IRS audits
- Random screening at airports (customs, security, etc.)
- School lotteries
Other Applications

Verifiable randomness sources have a host of other applications:
[Bonneau et al. 2015] [Kroll et al., 2017]

• Visa lottery
• Actual lottery
• IRS audits
• Random screening at airports (customs, security, etc.)
• School lotteries
• …
Three Cryptographic Ideas

1. Coin-Flipping Protocols
2. Fair Exchange
3. Randomness Beacons
Three Cryptographic Ideas

1. Coin-Flipping Protocols
2. Fair Exchange
3. Randomness Beacons
Tool 1: Coin-Flipping Protocol
Tool 1: Coin-Flipping Protocol

**Claim:** If we have a means to produce a single unpredictable number $N$, that is enough to select a random panel.
Tool 1: Coin-Flipping Protocol

**Claim:** If we have a means to produce a single unpredictable number $N$, that is enough to select a random panel.

→ Make a list of all possible panels, use the $N$-th panel. (We can think of $N$ as between 1 and 100.)
Tool 1: Coin-Flipping Protocol

Claim: If we have a means to produce a single unpredictable number $N$, that is enough to select a random panel.

→ Make a list of all possible panels, use the $N$-th panel. (We can think of $N$ as between 1 and 100.)

Principle: The best (only?) way to be sure that a “random” number is really random is to pick it yourself. [Blum 1983]
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

“Cryptographic commitment”
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

"Cryptographic commitment"
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

"Cryptographic commitment"
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

“Cryptographic commitment”
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

37
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office
Tool 1: Coin-Flipping Protocol

Petitioner

Clerk’s Office

Respondent
Tool 1: Coin-Flipping Protocol

Petitioner → Clerk’s Office

Respondent → Clerk’s Office
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office
Tool 1: Coin-Flipping Protocol
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office

Key
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office

12
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office

12

37

12

37

Key
Tool 1: Coin-Flipping Protocol

Petitioner

Respondent

Clerk’s Office

12

37
Tool 1: Coin-Flipping Protocol

Use $12 + 37 = 49$ as the random number.
Tool 1: Coin-Flipping Protocol

If the sum is over 100, use only the last two digits.

Petitioner

Respondent

Clerk’s Office

Use $12 + 37 = 49$ as the random number.
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole...
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…
Problem: The respondent sees the output $N$ before the petitioner does. This creates a loophole...
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…
Problem: The respondent sees the output $N$ before the petitioner does. This creates a loophole…

Petitioner: My number is 37, so we will get panel 49.

Respondent: 

Clerk’s Office: 12
Problem: The respondent sees the output $N$ before the petitioner does. This creates a loophole…

I don’t like panel 49.
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole...

Petitioner

Respondent

I lost my key! Let’s start over.
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…

Petitioner

Respondent

The Russians hacked my laptop! Let’s start over.

Clerk’s Office

12
Are we done?

**Problem:** The respondent sees the output $N$ before the petitioner does. This creates a loophole…
Are we done?

**Problem**: The respondent sees the output $N$ before the petitioner does. This creates a loophole…

- **Petitioner**
  - Petitioner may choose the panel.

- **Respondent**

- **Clerk’s Office**
Three Cryptographic Ideas

1. Coin-Flipping Protocols
2. Fair Exchange
3. Randomness Beacons
Three Cryptographic Ideas

1. Coin-Flipping Protocols
2. Fair Exchange
3. Randomness Beacons
Tool 2: Fair Exchange

[Blum 1981], [Damgård 1993]
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner → Clerk’s Office

Respondent
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk's Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent

Clerk’s Office

12
Tool 2: Fair Exchange

Respondent: I lost my key! Let’s start over.

Petitioner

Clerk’s Office
Tool 2: Fair Exchange

Petitioner

Respondent
Tool 2: Fair Exchange

Petitioner

Respondent
Tool 2: Fair Exchange

Petitioner

Respondent
Tool 2: Fair Exchange

You get panel number 12 + 37 = 49.
Three Cryptographic Ideas

1. Coin-Flipping Protocols
2. Fair Exchange
3. Randomness Beacons
Three Cryptographic Ideas

1. Coin-Flipping Protocols
2. Fair Exchange
3. Randomness Beacons
Tool 3: Randomness Beacon

[Rabin 1983]
Tool 3: Randomness Beacon

[Rabin 1983]

• These first two solutions (coin-flipping and fair exchange) require interaction between the parties.
Tool 3: Randomness Beacon

[Rabin 1983]

- These first two solutions (coin-flipping and fair exchange) require interaction between the parties.

- An alternative approach is to derive panel assignments from a public unpredictable randomness source.
Tool 3: Randomness Beacon

[Rabin 1983]

• These first two solutions (coin-flipping and fair exchange) require interaction between the parties.

• An alternative approach is to derive panel assignments from a public unpredictable randomness source.
  – Tomorrow’s closing prices of the NYSE and NASDAQ
Tool 3: Randomness Beacon

[Rabin 1983]

• These first two solutions (coin-flipping and fair exchange) require interaction between the parties.

• An alternative approach is to derive panel assignments from a public unpredictable randomness source.
  – Tomorrow’s closing prices of the NYSE and NASDAQ
  – Front page of next week’s New York Times
Tool 3: Randomness Beacon

[Rabin 1983]

• These first two solutions (coin-flipping and fair exchange) require interaction between the parties.

• An alternative approach is to derive panel assignments from a public unpredictable randomness source.
  – Tomorrow’s closing prices of the NYSE and NASDAQ
  – Front page of next week’s New York Times
  – Blocks in the Bitcoin network [Bonneau et al. 2015]
Tool 3: Randomness Beacon

[Rabin 1983]

- These first two solutions (coin-flipping and fair exchange) require *interaction* between the parties.

- An alternative approach is to derive panel assignments from a *public unpredictable randomness source*.
  - Tomorrow’s closing prices of the NYSE and NASDAQ
  - Front page of next week’s *New York Times*
  - Blocks in the Bitcoin network [Bonneau et al. 2015]

- Using a public randomness source allows *anyone* to verify the correct use of randomness.
Three Cryptographic Ideas

1. Coin-Flipping Protocols
2. Fair Exchange
3. Randomness Beacons
Are these schemes practical?
Are these schemes practical?

Maybe…
Are these schemes practical?

Maybe…

+ Many randomized government processes (panel assignments, tax audits, etc.) are computerized.
Are these schemes practical?

Maybe…

+ Many randomized government processes (panel assignments, tax audits, etc.) are computerized.
+ The cryptographic building blocks are all completely standard and are already in your PC.
Are these schemes practical?

Maybe…

+ Many randomized government processes (panel assignments, tax audits, etc.) are computerized.

+ The cryptographic building blocks are all completely standard and are already in your PC.

Maybe not…
Are these schemes practical?

Maybe…

+ Many randomized government processes (panel assignments, tax audits, etc.) are computerized.
+ The cryptographic building blocks are all completely standard and are already in your PC.

Maybe not…

– The software that runs our government is rarely open to public scrutiny.
Are these schemes practical?

Maybe…

+ Many randomized government processes (panel assignments, tax audits, etc.) are computerized.

+ The cryptographic building blocks are all completely standard and are already in your PC.

Maybe not…

– The software that runs our government is rarely open to public scrutiny.

– There is an incentive problem: codifying procedures removes flexibility.

Conclusions
Conclusions

The legal system, like everything else, is increasingly computerized.
Conclusions

The legal system, like everything else, is increasingly computerized.

- **Risk:** “Black-box” algorithms and processes may exhibit subtle biases and faults.
Conclusions

The legal system, like everything else, is increasingly computerized.

• **Risk:** “Black-box” algorithms and processes may exhibit subtle biases and faults.

• **Hope:** In theory, we can use cryptographic tools to make almost any algorithm open and accountable.
Conclusions

The legal system, like everything else, is increasingly computerized.

• **Risk:** “Black-box” algorithms and processes may exhibit subtle biases and faults.

• **Hope:** In theory, we can use cryptographic tools to make almost any algorithm open and accountable.

What will it take to turn this theory into practice?
Conclusions

The legal system, like everything else, is increasingly computerized.

- **Risk:** “Black-box” algorithms and processes may exhibit subtle biases and faults.
- **Hope:** In theory, we can use cryptographic tools to make almost any algorithm open and accountable.

What will it take to turn this theory into practice?

Help out!

Do you know anyone who could help us get access to the code used to generate panel assignments in the Courts of Appeals? Email us!

henrycg@cs.stanford.edu
keithw@cs.stanford.edu
Conclusions

The legal system, like everything else, is increasingly computerized.

- **Risk**: “Black-box” algorithms and processes may exhibit subtle biases and faults.

- **Hope**: In theory, we can use cryptographic tools to make almost any algorithm open and accountable.

What will it take to turn this theory into practice?

**Help out!**

Do you know anyone who could help us get access to the code used to generate panel assignments in the Courts of Appeals? Email us!

  henrycg@cs.stanford.edu
  keithw@cs.stanford.edu

**Want more?**

*Cybersecurity: A Legal and Technical Perspective*
LAW 4004 (Spring 2017) - Boneh and Granick