Boston University School of Law
Scholarly Commons at Boston University School of Law

Faculty Scholarship

Summer 7-19-2018

Basic (Non-Technical) Requirements – Electronic Monitoring Agreement for Zappers, Phantomware, and Other Sales Suppression Devices Appendix A

Richard Thompson Ainsworth
Boston University School of Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship

Part of the Law Commons

Recommended Citation
Ainsworth, Richard Thompson and Chicoine, Robert, Basic (Non-Technical) Requirements – Electronic Monitoring Agreement for Zappers, Phantomware, and Other Sales Suppression Devices Appendix A (July 11, 2018). Boston Univ. School of Law, Law and Economics Research Paper No. 18-14.

This Article is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.

BU School of Law

BASIC (NON-TECHNICAL) REQUIREMENTS – ELECTRONIC MONITORING AGREEMENT FOR ZAPPERS, PHANTOMWARE, AND OTHER SALES SUPPRESSION DEVICES
APPENDIX A

Boston University School of Law
Law & Economics Series Paper No. 18-14

July 2018

Richard T. Ainsworth
Boston University School of Law

Robert J. Chicoine

Electronic copy available at: https://ssrn.com/abstract=3212003

BASIC (NON-TECHNICAL) REQUIREMENTS - ELECTRONIC MONITORING AGREEMENT FOR ZAPPERS, PHANTOMWARE, AND OTHER SALES SUPPRESSION DEVICES APPENDIX A

Richard T. Ainsworth
Robert J Chicoine

The *State of Washington v. Wong*, Wash. Super. Ct., No. 16-1-00179-0 is the State of Washington's first judicially resolved case involving an automated sales suppression device. Months of negotiations led to a plea agreement and the State's first electronic sales monitoring agreement (August 30, 2017). The taxpayer violated RCW 82.32.290 (4)(a) by knowingly possessing, and knowingly using a Zapper to suppress sales.[1]

The penalties in this case were severe. Not only were all taxes, penalties, and interest lawfully due required to be paid, but as a Class C felony incarceration of up to 5 years, a $10,000 fine, or both were possible.[2] An even a more severe penalty for the taxpayer involved prohibited her from participating in any business unless she:

> … entere[d] into a written agreement with the department for the electronic monitoring of the business's sales, by a method acceptable to the department, for five years at the business's expense.[3]

The State of Washington enacted Senate Bill 5715 in 2013, codified at RCW 82.32.290, to prohibit electronic sales suppression (ESS). As of August, 2017, no regulations had been issued, and no guidance had been published on any enforcement aspect of the law. Much of the time and effort expended on both sides of the *Wong* case can be attributed to this ambiguity. Abstract issues which could inspire policy debates in another forum immediately became concrete concerns of a specific client operating a specific business. This context substantially slowed the process.

The Electronic Monitoring Agreement in this case is comprised of two parts – the basic agreement (Appendix A), and the technology requirements (Exhibit 1). This paper concerns Appendix A. Exhibit 1 was considered in an earlier article.[4] This paper examines the provisions of the agreement, sets out the arguments and analysis of both sides, and offers suggestions that might be useful to others engaged in similar negotiations of this kind.

---

[1] A Zapper places sales suppression programming on a removable CD or memory stick. Phantomware is similar suppression programming which is also prohibited by the Washington statute, but it is installed within the ECR/POS system, and is not readily removable from them. Zappers and Phantomware perform the same sales suppression functions in much the same manner.
[2] RCW 9a.20.021.
[3] RCW 82.32.290(4)(b)(iii)
[4] For a discussion of the technology requirements (Exhibit 1) *see*: Richard T. Ainsworth & Robert J. Chicoine, *The Technology Requirements of the First Electronic Monitoring Agreement in U.S. for Zappers*, 86 STATE TAX NOTES 239 (October 16, 2017).

Electronic copy available at: https://ssrn.com/abstract=3212003

As of the drafting of this paper, no other Electronic Monitoring Agreement (EMA) has been achieved by the DOR with any other taxpayer. In addition, there does not appear to be another EMA on the horizon.[5] The DOR has concluded audits, and has made sizeable adjustments with at least eight other taxpayers who violated the same statute, while in possession of and using the same suppression device (the Profitek Zapper), which was purchased from the same salesman as in the *Wong* case.[6] There is no EMA in any of these cases. It is not entirely clear why this is the case.

It is possible that the absence of other EMAs is a strategic decision. Those EMAs, which are required by statute just as surely as the EMA in the *Wong* case, may have been held in abeyance pending resolution of the *Wong* case and further negotiations between the DOR and these taxpayers. It is also possible that the State granted immunity to these taxpayers in exchange for assistance with either State or Federal investigations into other Zapper-users, the salesman (John Yin), or the manufacturer (InfoSpec/Profitek). The salesman and the manufacturer are both deemed liable for all losses attributable to the Profitek Zapper throughout the State of Washington.[7]

Strategic Objectives of the Defense

The defense hoped to accomplish nine objectives through the negotiation of the Basic Monitoring Agreement:

(1) *Approval of a specific electronic monitoring system in advance*. Although the statute requires the Taxpayer to identify and pay for an electronic monitoring system that is "acceptable to the department" there is absolutely no regulatory guidance on what is "acceptable to the department" either is specific terms, or in general principles. This differs from all other jurisdictions adopting monitoring solutions. Each of those jurisdictions post a list of acceptable solutions on the tax authority's web page.

(2) *Limitations on discretionary enforcement by the DOR*. In initial conversations with the DOR the government's position, which was largely derivative of the statutory "acceptable to the department" language, was that the DOR would determine compliance with the electronic monitoring provisions of the statute in its sole discretion. The defense sought to place this enforcement effort within the normal course of DOR activities so that it would be subject to administrative and judicial review.

(3) *Limitations of the allegation of material breach*. Initial conversations with the DOR suggested that a determination of breach of the electronic monitoring agreement, which could bring with it a near immediate closure of the Taxpayer's business, was also a

---

[5] Personal communication Washington Attorney General's Office

[6] The US Attorney provided this information in its case against the Profitek Zapper salesman, John Yin. As of February 2, 2017, Profitek Zapper cases #1, #2, #3, and #5 were assessed ("State Tax Due"): $73,324.00, $132,000.00, $80,000.00, and $149,811.00. The corresponding payments were ("State Tax Paid"): $74,045.15; $511,832.00; $55,304.79 and $105,647.39. The attachment records four more Profitek Zapper cases: #4, #6, #7 and #8 with assessments of: $125,000.00; $87,997.00; $38,467.00; and $394,835.00 respectively. *USA v. John Yin*, Government's Opposition to Defense Motion to Continue Sentencing for a Second Time, Attachment 2, Docket No. 2:16-cr-00314-RAJ (W.D. WA) April 11, 2017. Attachment 1 to the same memorandum of opposition lists nine cases, making it clear that the *State of Washington v. Wong* is in-addition to the eight listed in Attachment 2.

[7] RCW 82.32.290(4)(a). ("It is unlawful for any person to knowingly sell, … manufacture, … any automated sales suppression device or phantom-ware.")

Electronic copy available at: https://ssrn.com/abstract=3212003

discretionary DOR judgement. The defense sought to place an allegation of breach within the context of a normal enforcement paradigm. This would include notice of alleged breach, engaging in a dialogue with the Taxpayer about the alleged breach, an opportunity to cure the breach, and a reasonable accommodation for working with technology Vendors who in most instances would have a better idea of where problems were and how they could be resolved than would the restaurant operator herself.

(4) *Rights of cure*. Initial conversations with the DOR did not convince the defense team that the DOR was considering that the Taxpayer was entitled to cure technological flaws, or operational defects that may arise during the five-year term of the monitoring agreement without violating it, much less deal with the consequences of a security provider going out of business. It was important to the defense team to have the DOR recognize that the Taxpayer would have rights to cure problems as they arose, and set out those pathways in the agreement.

(5) *Adjudication procedures in cases of alleged breach.* It was not clear to the defense team how allegations of breach would be adjudicated, and whether or not there would be a stay on enforcement actions pending the adjudication. This concern was a function of the DOR's claim that it had full discretion to determine a breach.

(6) *Limitations on future modifications as technology changes.* The defense team was concerned that a five-year technology dependent agreement was likely to run into issues with advances in technology that could not be anticipated. While the Taxpayer was willing to modernize the electronic monitoring system as technology advanced, it did not want to be forced to do so under threat of violating the agreement. Some upgrades may involve significant financial commitments, or involve major business disruptions. The defense team wanted to secure a commitment that the system installed and certified on day one would satisfy monitoring requirements for the full five-year term.

(7) *Simplicity of enforcement without unnecessary business disrupting intrusions*. The defense team wanted to encourage commitment to a plan and process of enforcement that would maximize remote technology oversight and minimize disruptive on-site visits from the audit division during peak business hours.

(8) *Specifying as much as possible the obligations and commitments of government actors and third-party vendors*. The defense team was concerned that the Basic Monitoring Agreement might become a one-sided document specifying the commitments by the Taxpayer that would make Basic Monitoring Agreement a workable mechanism to appropriately record and collect sales data and tax collections. To the defense team a workable agreement would specify as much as possible the commitments and obligations of all three parties (Taxpayer, DOR and third-party Vendors). One of the difficulties the Taxpayer had encountered with the DOR was its resistance to directly engage with the third-party technology Vendors who were providing the technology solutions, and preferred to deal with the Taxpayer. The defense felt that this approach would make most discussions difficult triangular conversations, particularly where almost all providers of solutions with deep experience in this marketplace are foreign.

(9) *Protections from closure of the business.* The overall thrust of the defense team's negotiation was to assure the Taxpayer that if the agreement was adhered to that there were protections against unfair business closure. The damage to an established business can be significant and difficult to repair if a business is closed unexpectedly. Our concern was that a "process" would be installed through the agreement that would

Electronic copy available at: https://ssrn.com/abstract=3212003

provide mechanisms to fairly answer and respond to any concerns that the DOR would have about the monitoring system throughout the five-year term of the agreement without ever closing the business.

The Basic Monitoring Agreement (redacted)

The Basic Monitoring Agreement of Appendix A (set out below) has been converted into a universal form that can be referred to and used as a guide by others engaged in a similar negotiation. The names of the taxpayer, the third-party security provider, the POS/ECR manufacturer, and the government revenue authority have been replaced with blanks and letters. The following notations appear, rather than real names:

- Taxpayer = the name of the individual or business involved;
- X = the name and model number of the POS system involved;
- Y = the manufacturer of the POS system;
- Z = the name of the third-party security system to be installed in X with the permission of Y;
- State DOR = the name of the government revenue authority involved; and

Citation to Statute = the applicable statutory provision granting authority to the State DOR to audit the business records and other matters.

BASIC ELECTRONIC MONITORING AGREEMENT

This Electronic Monitoring Agreement (the "Agreement") is made and entered into by, between and among the ___________(State) DOR_________ and ___________(Taxpayer)_______, pursuant to ________(Statute) _______.

1. INTRODUCTION

A. Under _____(Statute) ______ (the "Statute"), it is unlawful for any person who has been convicted of violating ______(Statute) ______ to engage in business, or participate in any business as an owner, officer, director, partner, trustee, member, or manager of the business, unless:

(i) All taxes, penalties, and interest lawfully due are paid;
(ii) The person pays in full all penalties and fines imposed on the person for violating this section; and
(iii) The person, if the person is engaging in business subject to tax under this title, or the business in which the person participates, enters into a written agreement with the department for the electronic monitoring of the business's sales, by a method acceptable to the department, for five years at the business's expense.

B. For the purpose of meeting their requirements under ______(Statute)______ and this Agreement, Taxpayers, have purchased a satisfactory electronic Point of Sales software system and a POS electronic monitoring solution, (jointly referred to as the "Monitoring

Electronic copy available at: https://ssrn.com/abstract=3212003

Software") from the Vendor who will install, update and service the Monitoring Software.

2. PURPOSE

The purpose of this Agreement is to provide for electronic monitoring of Taxpayers' sales for a five-year period, in accordance with ______(Statute) _______.

3. DEFINITIONS

A. "Business" includes __________(Specify taxpayer) ____________..

B. "Electronic Monitoring" means use of the Monitoring Software, use of the minimum hardware necessary to implement the Monitoring Software, and transmission of data for retention to a Department-approved storage unit, such as a cloud storage server, in accordance with the specifications identified in Ex. 1, which is incorporated as part of this Agreement.

C. "Sales Information" means information about every sales transaction recorded by Vendor, as of the date of installation at the Taxpayers place of business, as specifically described in Exhibit 1.

D. "Material Breach" is a failure of a party to cure an obligation that is so important and essential to the Agreement that nonperformance substantially defeats the purpose of the Agreement.

E. "Vendor" means the entity with which Taxpayers contract to record and transmit the sales information to the Department as required under this Agreement, as described in Exhibit 1.

4. DURATION

This Agreement is effective as of the date of final signature by all parties. The Agreement shall continue for five years from the date Electronic Monitoring is installed and operational, unless otherwise terminated as provided in this Agreement, or by the mutual consent of the parties. Taxpayers shall provide the Department with written notice at least 48-hours prior to the date on which Electronic Monitoring will begin. The Department will promptly confirm its receipt of notice. Taxpayer will instruct the Vendor to proceed upon execution of the Agreement, and will exercise its best efforts to have the Electronic Monitoring System installed and operational within 90 days of the effective date of the Agreement.

5. TAXPAYERS' OBLIGATIONS

Electronic copy available at: https://ssrn.com/abstract=3212003

A. Taxpayers shall:

1. Purchase the Monitoring Software and the minimum technological hardware necessary to implement the Monitoring Software at Taxpayers' place of business(es).

2. Take all action reasonably necessary to allow the Vendor to install, test and maintain the Electronic Monitoring system, in accordance with this Agreement and the specifications of Ex. 1.

3. Cause key employees to participate in training as to the use and operation of Electronic Monitoring System.

4. Take reasonable steps to prevent manipulation or tampering with the Electronic Monitoring system by third parties, including employees.

5. Authorize the Vendor to transmit reports and supporting data to the Department as described in Ex 1.

6. Authorize the Department to communicate with the Vendor regarding the reports, data, and information described in Exhibit 1.

7. Retain the Sales Information in accordance with _____(Statute)______.

B. Taxpayers have sufficiently identified the hardware and software it intends to use as an Electronic Monitoring system for the five-year monitoring period and provided the Department with sufficient detail demonstrating how the how the Electronic Monitoring satisfies the Statute. The Department approves the use of Electronic Monitoring and the collection of data described in Exhibit 1 as an acceptable method of monitoring in accordance with the Statute.

6. DEPARTMENT OBLIGATIONS

A. The Department shall:

1. Within 30 days of installation, perform all tests and inspections necessary to provide written confirmation to Taxpayers and to the Vendor that the Electronic Monitoring Software as installed meets or exceeds the requirements of the Department. If the Vendor that installed the Electronic Monitoring system that is the subject of this Agreement needs to be replaced, the Taxpayers will identify a replacement system, and the Department will perform appropriate tests and inspections on the replacement Monitoring Software.

2. If Taxpayer or the Vendor notifies the Department that software or hardware modifications are necessary, the Department will test and inspect the Electronic

Electronic copy available at: https://ssrn.com/abstract=3212003

Monitoring modifications within 30 days. If the Department does not conduct the testing and inspection within 30 days of receipt of notice, the modifications will be deemed in compliance with the Agreement until the Department performs the testing and inspection.

3. Take reasonable steps to ensure key employees understand the use and operation of Electronic Monitoring System.

4. Take reasonable steps to protect data transmission from corruption as a result of malware and other security threats.

7. ACCESS TO SALES INFORMATION AND BUSINESS RECORDS

A. Taxpayers shall provide the Department with access to the sales information, as set forth in Exhibit 1, so that the Department may monitor, evaluate, and verify that Taxpayers are complying with this Agreement. Inspections may take place at the Department's discretion so long as they do not disrupt Taxpayers' normal business operations. Nothing in this agreement limits the Department's right to examine records in accordance with ______(Statute)_______.

B. Taxpayers shall be on a monthly electronic filing status for all taxes and shall remit all payments electronically to the Department.

8. MODIFICATIONS TO ELECTRONIC MONITORING

A. Taxpayers shall not replace or make any material changes to the Electronic Monitoring Software or hardware without prior written approval from the Department, which approval may not be unreasonably withheld. Material modifications are new features, which may be developed using latest development technology (.net, Java, etc.), and may require adaptation and training by the end user. They will potentially affect normal operations of the business and are expected to occur once every two or three years.

B. Taxpayers may implement routine software updates to the Monitoring Software without Department approval. Routine updates include actions such as hot fixes, bug fixes, and minor changes to customized features specific to the business. They do not affect normal operations of the business and are expected to occur periodically throughout the monitoring period.

C. Taxpayers shall provide written notice to the Department of all outages, including power loss and system malfunctions, on the first business day following Taxpayers' discovery of the power loss or system malfunctions. Such notice shall include: the date and time of power loss or system malfunction, and if known, the duration of the power loss or system malfunction, the date and time when normal operations resumed, and the cause or reason

Electronic copy available at: https://ssrn.com/abstract=3212003

for the power loss or system malfunction. This notification process may be automated in full or in part by the Vendor and conducted through the Electronic Monitoring Software.

D. The Department will not require any material modifications to the Electronic Monitoring Software or hardware, unless mutually agreed on by the parties or specifically required by a change in the law.

9. ASSIGNMENTS OR CHANGES TO BUSINESS

Taxpayers shall provide the Department with at least 60 days-notice prior to selling, assigning, changing ownership, changing the management structure (including changes in officers, directors, partners, trustees, members, or manager of the business), or adding locations.

10. FAILURE TO PERFORM

A. If the Department encounters a concern or inconsistency with the data, the Department shall provide notice to Taxpayers and Vendor of the concern or inconsistency and an opportunity to cure within a reasonable period of time given the nature of the technical problem. The Department will provide Taxpayers with written confirmation that the concern or inconsistency has been cured. This notification and confirmation process may be automated by the Vendor and preserved through the Electronic Monitoring System.

B. If the Department determines that Taxpayers may be in material breach as defined in Section 3, it shall provide Taxpayers with notice and a written explanation of the alleged breach, including identifying the factual and legal bases for the determination. Taxpayers shall have 60 days from the date of notice to cure the material breach, or a reasonable period of time given the nature of the breach.

C. If the failure to perform is beyond the control of Taxpayers, such as the failure of the Vendor to perform, Taxpayers shall timely seek a replacement Vendor to ensure compliance with this Agreement. The Department may require Taxpayers to perform reasonable interim measures to monitor sales information. In the event of a failure to perform beyond the control of Taxpayers, the 5-year monitoring period is tolled for any period during which Electronic Monitoring consistent with this Agreement or Department-approved interim measures are not in place.

D. Upon an uncured material breach, the Department may seek any one or more of the following remedies: termination of the Agreement; institute proceedings for the revocation of Taxpayers' certificate of registration under ____(Statute)____ through an adjudicative proceeding under ____(Statute)____; or pursue any other remedy permitted

Electronic copy available at: https://ssrn.com/abstract=3212003

by law. In addition, a material breach of this Agreement may be a class C felony. See ____(Statute)____.

11. WAIVER

Any waiver by any party with regard to any of its rights under this Agreement shall be in writing and shall not constitute a waiver to any other or future rights of the party. Any waiver may be automated, recorded and preserved within the Electronic Monitoring System.

12. SEVERABILITY

If any provision of this Agreement or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, and to this end the provisions of this Agreement are declared to be severable.

13. TERMINATION

This Agreement shall remain in full force and effect until terminated as provided in this Agreement. The parties may terminate the Agreement by mutual consent in writing. Taxpayers have no right to unilateral termination of this Agreement.

14. JURISDICTION

This Agreement shall be construed and interpreted in accordance with the laws of the State of Washington.

15. AGREEMENT AMENDMENTS AND MODIFICATIONS

This Agreement may be waived, changed, modified, or amended only by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

16. LIMITATION OF LIABILITY

In no event shall the Department be liable for any damages arising out of this Agreement, including but not limited to, loss of earnings or profits.

17. NOTICES

Electronic copy available at: https://ssrn.com/abstract=3212003

All notices required by this Agreement shall be made to the following individuals:

Commentary on the Basic Monitoring Agreement

PREAMBLE:

The opening paragraph specifies the parties to the agreement, and the operating statute. There can be multiple taxpayers, both individual(s) as owners and the corporations they own can be parties to the agreement with the DOR.

An important omission from the list of parties are the technology providers. Neither the provider of the Point of Sale (POS) system, nor the provider of the security system are parties to the *Wong* agreement. During the negotiation the taxpayer argued that communication would be greatly facilitated if the technology providers could be included as formal parties to the agreement. The hope was that the DOR would communicate directly with the technology providers. The taxpayer anticipated that there would be moments during the five-year term of the agreement where it would be beneficial for technologists with the DOR to be allowed access, as needed, to the technology professionals at either of the providers.

As this agreement stands however, communications under this agreement will occasionally be triangular, not binary. If, for example, a difficult software update or a “patch” in one or more systems in use under the agreement puts the systems “out of sync” with one another, then the process would be:

(a) the DOR would communicate with the taxpayer about the problem;
(b) the taxpayer would relay the DOR’s concerns to the technology providers;
(c) the technology providers would resolve the problem with the taxpayer; and
(d) the taxpayer would report back to the DOR with the solution.

The DOR’s concern was that it did not want to appear to be endorsing a particular technology provider by establishing direct contact with them. Extending the agreement to these parties, and working with them directly would suggest an endorsement. The taxpayer, as a small restaurateur without a dedicated technology person on staff, had hoped that the agreement could authorize the DOR and her providers to “work things out” between themselves, bringing her in at the end of the process.

The taxpayer has made it clear that she will authorize whatever level of direct communication may be necessary to make the agreement work.

1. INTRODUCTION:

In PART A the Agreement recites the portion of the statute violated by the taxpayer, including the penalty provision requiring a Monitoring Agreement, and the requirement that the monitoring must be “… by a method acceptable to the department …”

In PART B the Agreement indicates that the taxpayer has “purchased a satisfactory electronic Point of Sale software system and a POS electronic monitoring solution.” The DOR

Electronic copy available at: https://ssrn.com/abstract=3212003

resisted this provision as it suggested an endorsement of a POS system and a monitoring solution. The taxpayer strongly insisted that this provision be included in the agreement.

With no regulations sketching in objective terms the parameters of a "method acceptable to the department" the taxpayer felt it was at considerable risk if the department did not approve a specific monitoring method in advance of the Agreement.

There are a number of competing systems on the market offering digital security in the specific situation at hand. The taxpayer is aware that many of them can be found to have flaws in one respect or another. If the DOR had a concern, or developed a concern about an attribute in a system, a method that appeared to be "acceptable to the department" might become unacceptable, and this would impact the taxpayer both financially and operationally.

For example, some "black box" solutions work on old software (Quebec's black box works on Windows XP for example), and others save only some of the transaction data and do not transmit to the tax administration (the Swedish black box by Retail Innovation for example). Other systems secure data so late in the transaction process that they end up preserving post-manipulation data as if it were an accurate record of sales (the newest Epson printers that save data to the cloud fall into this category). A further large number of electronic monitoring solutions are suspect because the same company that provides the POS also provides the digital security. These systems (like those offered by Sintel Systems) present the same conflict as InfoSpec/Profitek which made both the POS system and the Zapper that defeated it. This conflict was the basis of the *Wong* case, and the DOR was insistent that the InfoSpec/ Proiftek POS would not be an acceptable part of any taxpayer proposed solution.

2. PURPOSE:

This section recites the statute on electronic monitoring.

3. DEFINITIONS:

In PART A the taxpayer is defined as a business.

In PART B "electronic monitoring" is defined to include hardware and software technology components, but also the activity of transmitting the secured data to the DOR. The DOR must specify the type of storage unit, but it is the taxpayer's responsibility to get the data to that unit. Data stored only in site is not sufficient.

On this point, the Agreement references the technical requirements in Exhibit 1 at paragraph E where the *Method for Transmitting the Data Files* is specified. The requirements include specifications on encryption/ decryption of data at the DOR facility and a requirement that the DOR acknowledge receipt.

In PART C "sales information" is defined, again by referencing Exhibit 1 at (D)(2)(i) where twelve specific data points are indicated, some of which, like "number of open tills," may seem outside the common meaning of "sales information," but are understood in the sales suppression field to be critical to securing accurate sales records.

Electronic copy available at: https://ssrn.com/abstract=3212003

In PART D "material breach" is defined *not* as the violation an obligation under the agreement, but as the *failure to cure* or restore an obligation that is essential to the Agreement. This definition is important in two respects:

(a) it removes the element of surprise where a taxpayer might unintentionally violate an obligation under the Agreement, and quickly thereafter find their business subject to closure, and a new class C felony imposed under RCW 82.32.290(4)(c)(ii); and
(b) it implicitly requires that the DOR and the taxpayer talk with one another about how to achieve the stated goal of a successfully functioning Monitoring Agreement.

The taxpayer wanted to limit the DOR's initial intent to adopt a highly discretionary enforcement option, one that reflected a very narrow reading of the statute. Early on in the negotiations the DOR took the position that they had complete discretion in determining material breach, and that the DOR could act (if necessary) on a moment's notice.

This definition instead places "material breach" at the conclusion of a reasonably dynamic exchange between the taxpayer and the DOR. It assumes a conversation between the parties where, if a breach appears to have occurred it needs to be identified and brought to the attention of the Taxpayer in an exchange where the taxpayer will have the opportunity to attempt a cure. This formulation keeps the common goal of achieving a workable monitoring agreement in front of both of the parties.

In PART E "vendor" is defined as both of the technology providers (POS provider and software security provider) that are under contract with the taxpayer to provide electronic monitoring "… by a method acceptable to the department …" This definition is applied to make the legal relationship between DOR, the taxpayer, and the technology providers clear.

4. DURATION

The statute indicates that the monitoring agreement must be in place for "five years." No other timing matters are mentioned in the statute. Because there are no regulations or other guidance, this provision makes the following dates clear:

(a) Effective date of the agreement – at final signature of all parties;
    i. Vendor commencement – at the effective date in (a) as notified by taxpayer;
    ii. Vendor's installation and system operation target date – 90 days after (a);
(b) Beginning of five-year monitoring period – at the date when the Electronic Monitoring system is fully installed and operational;
    i. Notice of beginning of the period – taxpayer notifies DOR 48 hours prior to (b)
(c) Termination of the agreement – see paragraph 13.

Importantly, there is no tolling of the five-year period. Once the period begins it runs without interruption. The period ends prematurely only with a termination event. During the negotiation of the Agreement the taxpayer brought up the possibility that the five-year period would be tolled by actions of the taxpayer or of the DOR. With one exception for a "failure to perform" event covered by section 10, any kind of administrative tolling was rejected by the DOR, along with any suggestion that the DOR could ever materially breach the agreement or could "fail to perform" under the agreement as that principle is discussed in Section 10.

Electronic copy available at: https://ssrn.com/abstract=3212003

5. TAXPAYERS' OBLIGATIONS:

There are two parts to section five. The seven primary obligations of the taxpayer are listed in PART A. These are forward-looking obligations:

a. purchase the Monitoring system,
b. allow the Vendor to install, test and maintain the system
c. train key employees in use of the system
d. prevent manipulation of the system
e. authorize the Vendor to transmit reports to the DOR
f. authorize the DOR to communicate with the Vendor about those reports, and
g. retain sales information for the statutory period.

PART B takes a different approach. This section is backward-looking. It indicates that the taxpayer has already satisfied critical parts of its obligations. It indicates that the Taxpayer brought the technology Vendor to a meeting with the DOR. The Vendor made a presentation explaining what it was prepared to install for the Taxpayer. After the presentation, the DOR "approved" the Electronic Monitoring system, certified that it "satisfied the Statute," and indicated that its approval encompassed the entire five-year period of the Agreement.

Getting the DOR's approvals in PART B were critical to the Taxpayer being able to make the forward-looking commitments in PART A.

6. DEPRTMENT OBLIGATIONS:

Four points are covered in this section. Two deal with the DOR's obligation to certify the taxpayer's/ vendor's system, and provide written notice of the certification to the taxpayer and the Vendor. Two others replicate obligations of the taxpayer.

Certification. The certification provisions [6(A)(1) and (2)] reflect the taxpayer's concern that five years is a very long time in technology-terms. Systems change, programs have difficulty integrating with newer operating systems, bugs are found and patched, and companies that were at the top of their field fall behind. None of this is the fault of the taxpayer, or can be predicted with any specificity, but if software changes are necessary, then DOR will need to re-certify the taxpayer's system. Thus, the two certification provisions require:

1. initial certification of the Electronic Monitoring Software within 30 days of installation;
2. re-certification of any replacement system, or replacement parts of the system;
3. re-certification of the whole system where software or hardware modifications are deemed necessary within 30 day of the modification; and
4. if the DOR is not able to re-certify, then the replacement system is deemed re-certified until such time as the DOR can certify that the modified system is in compliance with the Agreement.

A fifth element or related permutation concerns what would happen if the DOR could not re-certify the system after making an inspection. If this occurred, then the material breach provisions of this document would apply and this open up the dynamic exchange between the Taxpayer and the DOR where the Taxpayer would conduct a reasonable search for a compliant system. Per the duration provisions at section 4 above the 5-year running of the Electronic Monitoring Agreement would not be tolled during this period.

Electronic copy available at: https://ssrn.com/abstract=3212003

Parallel obligations. In two areas, the DOR is committed to take steps to further the workability of the agreement. The DOR agrees to take reasonable steps to train its key employees on the use and operation of the Electronic Monitoring System. This commitment is comparable to the Taxpayer's obligation to train its employees on the use of the Electronic Monitoring System at 5(A)(3) above.

The DOR also agrees to take steps to protect transmissions from corruption. This commitment is comparable to the Taxpayer's obligation to prevent manipulation or tampering with the Electronic Monitoring System at 5(A)(4) above.

7. ACCESS TO SALES INFORMATION AND BUSINESS RECORDS:

This provision is drafted in an "abundance of caution" context to expressly extend the audit authority of the DOR to encompass the sales information in the Electronic Monitoring System. While the applicable statutory provisions [RCW 82.32.070] are more than likely broad enough to include this authority, both parties thought it would be good to make this clear.

Audit may occur at the DOR's discretion, limited only by not being disruptive to the Taxpayer's business operations.

The requirement at 7(B) that "all taxes" shall be filed monthly and electronically and "all payments" remitted electronically is understood by the parties within the context of the Agreement to mean all *Retail Sales Taxes* and *Business and Occupation* taxes, both of which can have monthly filing obligations and both of which can be electronically paid.

8. MODIFICATIONS TO ELECTRONIC MONITORING:

Modifications. The modification provisions are important to this Agreement, because it is clear that the system that is installed on day 1 will not be the same system at the end of the first year, and certainly not by the end of the second year. This technology is expected to change in big and small ways throughout the duration of this agreement.

Software modifications can either be material or routine, and the line between them is drawn internally. The standard is not external. Modifications are "material" based on the degree to which they impact the Electronic Monitoring System. Two elements are emphasized:

(a) does it require adaptation and training of the end user, and
(b) does it affect normal operations of the business?

Because a material modification will require end user re-training and will probably impact the business and accounting flows of the Taxpayer, Section 8(A) requires written notification of, and approval of the DOR. When this occurs, the re-certification provisions of Section 6 will be activated, but only by a material modification, not by a non-material (or routine) modification or software update.

The best estimates of the Vendor are that material modifications may occur each two or three years, and routine software updates (non-material modifications) may occur two or three

Electronic copy available at: https://ssrn.com/abstract=3212003

times each year. The DOR will not require a material modification, and will effectively rely on the good judgement of the Vendor when Monitoring System modifications are needed.

Outages, power loss and malfunctions. In instances where the Electronic Monitoring System "goes down" for whatever reason, the Agreement in Section 8(C) requires a record to be made and notice to be delivered to the DOR. Most Electronic Monitoring Systems keep this record digitally, and Section 8(C) allows this record and the notification to the DOR be done through an online report.

9. ASSIGNMENTS OR CHANGES TO BUSINESS:

This provision is in the Basic Monitoring Agreement entirely at the insistence of the DOR. It is a notification provision requiring the Taxpayer to notify the DOR of a further violation, specifically a violation of RCW 82.32.290(4)(b). In the particular facts of the *State of Washington v. Wong* this requirement was not problematical.

RCW 82.32.290(4)(b) criminalizes the further participation in "any business" by a person who has a primary conviction under RCW 82.32.290, unless that further business (which could be the same business, a different, additional, or newly established business) also installs an Electronic Monitoring System. The provision states:

> (b) It is unlawful for any person who has been convicted of violating this section to engage in business, or participate in any business as an owner, officer, director, partner, trustee, member, or manager of the business, unless:

This provision functions like an electronic monitoring ankle bracelet today. Developed at Harvard almost 50 years ago by social psychologist studying under B.F. Skinner and Timothy Leary as a positive reinforcement tool, the modern ankle bracelet has more of a negative criminal enforcement association. It is used today to track low risk criminals with the stated benefit of reducing the cost of physical incarceration.[8]

The application of the Electronic Monitoring System in the Washington statute appears to us to follow the negative thread spun from our experiences with the electronic monitoring ankle bracelet which have been found to burden (in application) specific social classes. In a business context, the same mechanisms have been found to unconstitutionally burden the right to work.

Case law in this area has a long history beginning with *Yick Wo v. Hopkins*, 118 U.S. 356 (1886) which considered a regulation making it illegal to operate a laundry in a wooden structure, and where the application of the regulation (which was race-neutral on its face) was found to be administered in a prejudicial manner – it targeted minorities. The Equal Protection Clause and the 14th Amendment were implicated, as well as the fundamental right that all citizens have to securing meaningful employment. The same would apply in Washington.

In the present case however, Ms. Wong intends to continue her present business, making the "any business" language of RCW 82.32.290(4)(b) is less burdensome. In a different case, or

[8] Emma Anderson, *The Evolution of Electronic Monitoring Devices*, NPR (May 24, 2014) available at: http://www.npr.org/2014/05/22/314874232/the-history-of-electronic-monitoring-devices

Electronic copy available at: https://ssrn.com/abstract=3212003

in an instance where a new, additional or different business was contemplated this provision in the agreement, which connects back to the questionable language of the statute would be challenged more forcefully.

10. FAILURE TO PERFORM:

The Electronic Monitoring Agreement contemplates failures to perform only from the Taxpayer's side. A failure to perform can only be identified by the DOR. The DOR must notify the Taxpayer of the failure. Neither the Taxpayer, nor any Vendor, nor any third party is allowed identify a failure to perform. The PARTS in paragraph 10 are understood by the Taxpayer and the DOR to run in sequence A, B, C, and then D. This is how they were discussed and developed during negotiations.

PART A: This part deals with data inconsistencies (or concerns with data generally). Because this is a data-based issue, the DOR is required to provide dual sets of notices, one to the Taxpayer, and the other to the data-Vendors under contract with the Taxpayer. The reason for the dual notices is reasonably clear. Neither party to this agreement (the DOR or Taxpayer) expects that the Taxpayer will have the technical expertise to understand, or solve the problem.

For this reason, a "reasonable period of time" is provided for cure. The period of time is deliberately open-ended, because the "nature of the technical problem" cannot be foreseen, and in a 5-year technology agreement the number, type and complexity of the problems can be daunting. In addition, this is one of the areas where the triangular relationship (DOR-Taxpayer-Vendor) creates difficulties where a binary relationship (DOR-Vendor) would be more efficient.

When cure occurs the DOR will provide written notification to the Taxpayer. The Taxpayer will need to notify the Vendor that the cure is in place and accepted by the DOR.

This is another function where the electronic monitoring systems in place globally have automated communications. Vendors, like the one selected for this case) routinely automate and preserve communication exchanges about technical issues. (See: *Outages, power loss and malfunctions* in Paragraph 8 above.)

It is expected by both parties that a re-certification of the system will follow a notice-examination-cure-confirmation of cure sequence. This re-certification will occur under paragraph 6 (above), including both

(a) the presumption of re-certification if the DOR is not able to formally re-certify within the 30-day period set out in that paragraph, and
(b) the non-tolling of the 5-year period for the Electronic Monitoring Agreement as the examination and cure is being worked out.

This is standard practice in this field, as to do otherwise would allow a taxpayer to go "off-line" whenever a technical problem arose, and the purpose of this Agreement is to keep the Taxpayer reporting as fully as possible throughout the monitoring and oversight period.

PART B: This part follows in sequence from PART A. It is assumed by the Taxpayer and the DOR that at the first signs of a data "concern or inconsistency" the DOR will initiate a

Electronic copy available at: https://ssrn.com/abstract=3212003

PART A communication where the Taxpayer and Vendor will investigate the issues "within a reasonable period of time given the nature of the technical problem." It is only after this investigation that the DOR will issue a "cure" (PART A) or a "material breach" (PART B) notice to the Taxpayer (alone).

This notice is expected to provide in significant detail what is the nature of the problem. It rests on the full examination in PART A, during which the DOR has been in direct contact with the Vendor after exchanging the required communications with the Vendors directly. The difficulties at this point are anticipated to be such that the Taxpayer may need to secure the assistance of another Vendor. In this section, a 60 day period is suggested for the further efforts to cure, but it is further extended to "a reasonable period of time given the nature of the breach."

The 5-year provision of the Monitoring Agreement is not tolled during the PART B examination and efforts to cure.

PART C: This part contemplates a situation where the failure of effective electronic monitoring is due not to the Taxpayer, but to the Vendor who has previously been selected by the Taxpayer, approved and certified by the DOR. During the negotiation of this Agreement we considered situations like the bankruptcy of the Vendor or the termination of its business. In that event two courses of action were anticipated.

In the first, the Taxpayer will "timely seeks a replacement" and perform "reasonable interim measures." The Vendor-event would be reasonably sudden. From a system perspective the "failure" could be indistinguishable from a data inconsistency-event in PART A if the Taxpayer is seeking timely Vendor-replacement and taking reasonable interim measures. It is expected that the DOR will provide notice, and the Taxpayer will be taking steps to cure. A total collapse of Vendor participation would easily amount to a "material breach" as contemplated in PART B, and this would activate the 60 day cure period.

In the second, the Taxpayer is not "timely seek[ing] a replacement," and not able to perform "reasonable interim measures." Although there will be notice and a search for a Vendor-replacement, as well as an identification of Department-approved interim measures, the failure is severe. In this circumstance, the failure to perform is truly "beyond the control of the taxpayer," and would become a termination event. In this instance, the 5-year monitoring period will be tolled "for any period during which the Electronic Monitoring … or Department-approved interim measures are not in place."

PART D: This part specifies DOR remedies if the failure to perform constitutes an "uncured material breach." In this instance, cure efforts (which are always open to the Taxpayer) have been exhausted, and the failure to perform remains. Depending on the circumstances the DOR may seek

(a) termination of the Agreement;
(b) revocation of the Taxpayer's certificate of registration; or
(c) other remedy permitted by law.

In all case the remedy sought by the DOR will be part of an adjudicative process. The business will not be subject to immediate closure.

Electronic copy available at: https://ssrn.com/abstract=3212003

11. WAIVER:

Standard waiver provision requiring all waivers to be in writing, and limiting any waiver to the present context without impacting future rights. Also referencing the Electronic Monitoring System which can be used to record and preserve any waivers.

12. SEVERABILIUTY:

Standard severability provision whereby if any provision is deemed invalid, that determination will not determine the validity of any other provision.

13. TERMINATION:

Termination is by mutual consent, or through an action by the DOR. The DOR may terminate this agreement as provided in Paragraph 10(D) based on proof of an uncured material breach. The Taxpayer is not granted a right to terminate the agreement unilaterally.

14. JURISDICTION:

The rules, practice and procedures of the State of Washington shall be used to construe and interpret the Agreement.

15. AGREEMENT AMENDMENTS AND MODIFICATIONS:

The Agreement is open to amendment and modification by mutual agreement, in writing and signed by both parties.

16. LIMITATION OF LIABILITY:

The DOR is not liable for any damages arising out of the Agreement. The loss of earnings or profits is specifically mentioned as an example of a damage which migh occur, but for which the government is not liable.

17. NOTICES:

Individuals receiving notices under this Agreement are specifie.

CONCLUSION

In this paper we focused on the business-sensitive legal points around which we developed our negotiation position that resulted in the first American Electronic Monitoring Agreement. It was clear to us before and during these discussions that the DOR was (and probably still is) exploring how to best structure and implement an electronic monitoring agreement. We sincerely feel that the Washington DOR needs to issue regulations in this area, not only because it is new to almost all taxpayers, but because a monitoring agreement can have a significant impact on business operations.

Electronic copy available at: https://ssrn.com/abstract=3212003

Many of the strategic decisions were made as we thought through permutations of business, technology, and government actions and reactions to tax reporting events. The keys for us were assuring accurate compliance with the tax statutes in a manner that allowed the DOR to confidently oversee business activities remotely, and accomplishing this in a manner that had minimal commercial impact on the restaurant involved. We were keenly aware that American experience in this area is close to non-existent and that we would need to borrow heavily from foreign tax administrations and third-party vendors.

Electronic copy available at: https://ssrn.com/abstract=3212003