Anthony Macchiarulo
185 West Broadway
New York, NY 10013

November 9, 2018

VIA E-MAIL: privacyrfc2018@ntia.doc.gov

National Telecommunications & Information Administration
U.S. Department of Commerce
1401 Constitution Ave., N.W., Room 4897
Washington, D.C. 20230
Phone: (202) 482-7002

Re: Docket No. 180821780-8780-01; New Approach to Consumer Data Privacy

Dear NTIA Privacy RFC:

I am writing to request the National Telecommunications & Information Administration ("NTIA") research the implementation of artificial intelligence ("AI") and Radio-frequency identification ("RFID") technology on global supply chain systems to prevent against international hardware espionage. More specifically, I am writing to request the expansion of AI and RFID research to support the NTIA manage consumer privacy risk. I propose goals for setting the broad outline for the direction that federal action should take in expanding AI and RFID and details as to how these goals can be achieved.

Although consumer privacy is violated through software conduits, invasion of privacy through hardware and the global supply chain are not given enough attention. The NTIA needs to pay more attention to the risk hardware traveling along the global supply chain poses to consumer privacy. By researching AI and RFID, the NTIA will be able to meet their goals of developing policy on issues related to the internet economy and help manage consumer privacy risk.

I. Foreign Espionage

Bloomberg reported how Chinese spies reached thirty U.S. companies, including Amazon.com, Inc. ("Amazon") by compromising America's supply chain. Amazon acquired a company named Elemental Technologies ("Elemental") in 2015 to create servers for Amazon Prime Video Services. Elemental had these servers manufactured in China from a company named Super Micro Computer, Inc. ("Super Micro"). In one of Amazon's third-party product tests of Elemental's servers, they found a tiny microchip seeded onto the server's hardware that was not part of the product's original design. This small chip was able to tell the device to communicate with one of several anonymous computers elsewhere on the internet that were loaded with more complex code. The tiny microchip was able to compromise one of the largest companies in the world, which in turn compromised the privacy of all users of that service.

Super Micro has relationships with many multinational corporations such as Apple, Inc. Super Micro's manufacturing plants were backdoor gateways for foreign espionage. The chip was so microscopic that it was difficult for the naked eye to detect. Elemental had contracts with the Olympic Games, the International Space Station, and the Central Intelligence Agency. Through Super Micro, Chinese spies had access to global privacy data. Large corporations and institutions are hubs of individual consumer privacy data. These corporations and institutions collect sensitive data on their customers, which in turn become exposed to spies.[1]

An AI scanner or RFID tag would have detected the espionage well before leaving the manufacturing facility. Tracking hardware with AI and RFID technology throughout every stage

[1] Jordan Robertson and Michael Riley, The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, Bloomberg (Oct. 4, 2018), https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies (last visited Oct. 8, 2018).

of the supply chain will protect consumer privacy. Shifting policy to allow for companies or logistic providers to track every movement of hardware from manufacturing to delivery between vendors, storage units, operations, and consumer distribution will prevent foreign privacy attacks.

II. The Fourth Amendment

The fourth amendment protects and encourages this type of surveillance of consumer privacy. The fourth amendment provides the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. No warrants shall be issued without probable cause, particularly describing the place to be searched, and the persons or things to be seized.[2]

In Florida v. Riley, the supreme court held there is no reasonable expectation the contents of a greenhouse were protected from public or official inspection of a helicopter with the naked eye. Here, the inspection of technological hardware with the use of AI and RFID should not be used to violate the privacy of company's products but aid in the protection of these products.[3]

The Federal government will need a warrant to implement AI scanners and RFID tags into logistic freight and the supply chain. In Kyllo v. United States, the court held where police obtain information about the inside of a home without physical intrusion, using a device not normally used by the public, the police action constitutes a fourth amendment search and is unreasonable without a warrant.[4] Therefore, I recommend gaining access to warrants as part of the harmonization of global logistics traceability agenda proposed. The court in U.S. v. Lacy, held a

[2] U.S. Const. Amend. IV.
[3] Florida v. Riley, 109 S.Ct. 693 (1989).
[4] Kyllo v. U.S., 121 S.Ct. 2038 (2011).

general warrant that specifies "the computer" and not anything more specific is okay.[5] Here, a general warrant should be sufficient.

Although the court in U.S. v. Carey, held the government cannot use a legitimate warrant to search a computer for evidence of illegal drug distribution to search for pornography.[6] The court in U.S. v. Campos, held legitimately searching for child pornography, a specific warrant need not force you to stop at the two images that started the investigation.[7] Here, a specific warrant for AI to scan hardware of any criminal activity or a warrant to place RFID tags on all products should not be a violation of the fourth amendment because it is just the starting point of traceability and violations discovered after the fact are no longer a violation of the fourth amendment but an aid to consumer privacy.

The court in Carpenter v. U.S. held tracking person's movements and location through extensive cell-site records is intrusive and a violation of fourth amendment rights.[8] Here, the tracking of products for personal security is not a violation of fourth amendment rights because it is no intruding on personal movements but searching for criminal behavior in hardware on a macro scale. Using AI and RFID technology on company specific products is for protection and is not the goal to intrude on the personal movements of consumers. Rather, the goal is to help consumers understand where and how their products are being manufactured. By creating this type of transparency, it will benefit the compliance with each sector's general guidelines of privacy.

[5] U.S. v. Scott Douglas Lacy, 119 F.3d 742 (9th Cir 1997).
[6] U.S. v. Carey, 551 F.2d 309 (10th Cir 1999).
[7] U.S. v. Campos, 237 Fed.Appx. 949 (5th Cir 2007).
[8] Carpenter v. U.S, 108 S.Ct. 316 (1987).

III. Notice and Choice

In the U.S., major privacy acts are sectoral. A few examples include The Children's Online Privacy Protection Act ("COPPA")[9], The Gramm–Leach–Bliley Act[10], and The Health Insurance Portability and Accountability Act ("HIPAA").[11]

Notice refers to providing consumers with information about how their data is used. This is usually found in a privacy policy. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Choice refers to giving consumers options to control how their data is used. Here, there was no notice or choice when foreign spies compromised Amazon's servers.

Two widely used notice and choice acts across the U.S. are the California Online Privacy Protection Act ("CalOPPA") and the California Consumer Privacy Act. CalOPPA requires privacy statements be conspicuous.[12] The California Consumer Privacy Act gives consumers the right to know who and where their data is being used and for what reason.[13]

Here, with AI and RFID technology, consumers would be able to track every stage of the distribution process, where every piece of hardware is located at any time, how it is being built, and by who. Giving consumers notice and the power of choice by way of AI and RFID technology is in conformance with CalOPPA and the California Consumer Privacy Act. Implementing AI and RFID technology, the NTIA can help protect against violations of sectoral privacy regulations.

[9] The Children's Online Privacy Protection Act.
[10] The Gramm–Leach–Bliley Act
[11] The Health Insurance Portability and Accountability Act.
[12] The California Online Privacy Protection Act.
[13] The California Consumer Privacy Act.

IV. General Data Protection Regulation ("GDPR")

The GDPR protects and encourages this type of surveillance of consumer privacy. Although privacy laws in the U.S. are sectoral, the global supply chain must comply with the GDPR and global privacy regulations. The GDPR relates to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Article I of the GDPR requires "The free movement of personal data within the European Union ('Union") be neither restricted nor prohibited for reasons connected with the protection of natural persons." [14] Here, AI and RFID technology will protect against free movement restrictions.

Article III of the GDPR provides for territorial scope. The GDPR covers all individuals within the European Economic Area ("EEA"). The GDPR operates much like a long-arm statute, where companies need to comply with European community law and national law, just like companies have to comply with federal and state laws.

The GDPR raises questions about International data flows. For example, moving data from Europe and then processing it in the U.S. may become problematic. The U.S. and Europe have different rules for processing personal data. Here, implementing AI and RFID tags into the flow of commerce will require strict compliance with privacy regulations in every country and will allow for the compliance of international data flows.

Article V of the GDPR provides for the principles relating to processing of personal data. Personal data must be processed lawfully, fairly and in a transparent manner. By implementing AI and RFID technology into the global supply chain, the lawful processing of personal data may be

[14] GDPR Art. I.

achieved because it will allow for an increase in global compliance with data regulations due to the conformity and transparency of the data that will be collected by supply chain systems.[15]

Article XXV of the GDPR provides for the protection of data by design and default. Data by design requires appropriate measures be taken throughout the entire life cycle of the product to avoid violations of privacy.[16] A privacy impact statement can help assist with this. Privacy impact statements help confirm companies meet privacy requirements during the lifecycle of the product's development.[17] When trying to prevent accidents, the people more capable of protecting against the problem should be working on them. Here, the developers building the AI and RFID technology should be focused on privacy from the start of the development process.

Data by default requires only necessary personal data be collected, stored, or processed and personal data not accessible to an indefinite number of people. Here, AI and RFID technology should only provide information to companies and consumers that need or require it. Implementing AI and RFID technology, the NTIA can help protect against not only violations of sectoral privacy regulations but also global violations of privacy regulations.

---

[15] GDPR Art. V.
[16] GDPR Art. XXV
[17] Rebecca Herold, Privacy Impact Assessment Full Report, Report (Jun. 1, 2012), https://iapp.org/media/pdf/knowledge_center/Generic_PIA_Report_-_The_Privacy_Professor_June_2012.pdf (last visited Oct. 20, 2018).

V. Data Collection and Breach Compliance

Data collection law protects and encourages this type of surveillance of consumer privacy. For example, California's Data breach notification law provides that as soon as a company knows of a data breach they must notify victims of that data breach. Some states give certain amount of days to notify the public. However, as long as there is a cure, the federal trade commission may not have to notify the public.[18]

Here, by collecting data instantaneously as events occur and anticipating future events, AI and RFID technology will be able to comply with data breach notification laws much more efficiently. For example, if a company's data is being breached via hardware, the AI and RFID technology can immediately notify the company for their compliance with these laws.

The Electronic Communications Privacy Act ("ECPA"), was an amendment to the Federal Communications Act. The act was enacted to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. The ECPA defines electronic communications as all types of computer mediated communication, such as email. Electronic communications do not include wire or oral communications.[19]

Here, collection will be easy to comply with using RFID technology on the blockchain. In its simplest form, a blockchain is a growing list of records. On the blockchain, all transactions of data are stored, recorded, and accounted for. The data collected by RFID tags on the blockchain can be made available to the public to increase transparency and allow for swift compliance with data collection regulations.

[18] The California Data Privacy Protection Act.
[19] The Electronic Communications Privacy Act

VI. Implementation of AI & RFID Technology

There are currently AI systems that are used to read and find abnormalities in brain scans. Qure.ai, a healthcare startup, was able to read head scans using AI and machine learning algorithms.[20] Using the same type of technology for scanning hardware as it moves from manufacturing to distribution is feasible by cross validating the data with specific company specifications. This can be achieved by hosting large data sets of what products are supposed to look like by companies and then scanned by algorithms to match the authenticity of the products. There are already machine learning algorithms being implemented for scanning baggage that comes through airports.[21] This same technology can be implemented on freight and logistics platforms. For example, by installing AI systems in manufacturing plants and shipping channels, hardware can be authenticated easily.

Integrating RFID technology into the global supply chain may be a cheaper alternative. RFID technology for supply chain traceability is already being developed by companies. The value internet of things ("VIoT"), the combination of blockchain and internet of things has real world applications of privacy protection that can be used today. One provider of VIoT technology is Waltonchain. Waltonchain's technology integrates blockchain with RFID Technology. Waltonchain manufacturers RFID tags that can be placed on any product for traceability and authenticity. The RFID tags communicate with a read-write terminal and an encrypted data collector, which post all data on the blockchain.

---

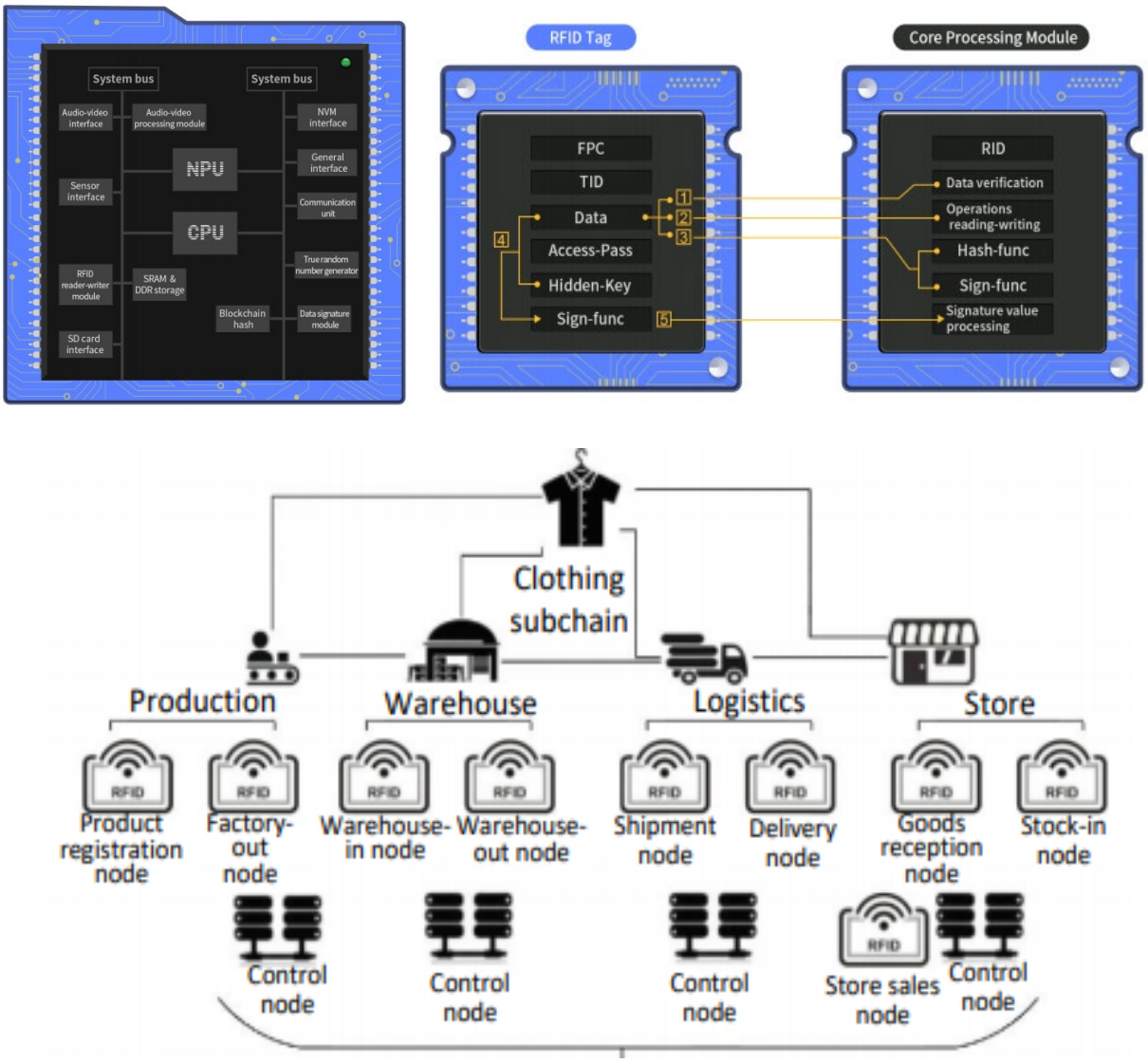
[20] Larry Dignan, Qure.ai launches AI system to read head CT scans and find abnormalities, ZDNet (Apr. 26, 2018), https://www.zdnet.com/article/qure-ai-launches-ai-system-to-read-head-ct-scans-and-find-abnormalities/ (last visited Oct. 12, 2018).

[21] Mark Rockwell, Harnessing machine learning for baggage scans, GCN (May 4, 2018), https://gcn.com/articles/2018/05/04/machine-learning-baggage-scans.aspx (last visited Oct. 12, 2018).

RFID technology allows a company or shipping provider to track every movement of products from manufacturing to delivery. Every piece of every product can be traced and accounted for on the ever-growing list of records on the blockchain. For example, in a standard motherboard the central processing unit ("CPU"), graphical processing unit ("GPU"), and random-access memory ("RAM") components may be manufactured and created in different locations. RFID tags will allow a consumer to verify exactly where, when, and how those products were assembled. This does not only extend to hardware, but also extends to food and soil traceability. For example, RFID tags can verify exactly what conditions and temperature food a consumer purchases from the supermarket were grown.

Waltonchain's RFID tags are inexpensive, around eleven cents each tag, and are practical for real use implementation. Each tag is loaded with its own CPU, secure digital card for storage, RFID read-write module, and blockchain hash module. The RFID tags connect to separate read write terminals for every part of the supply chain. Once the data is saved on the main blockchain, smart contracts can be written on sub-chains. These smart contracts can be used to make agreements between suppliers and companies in a more efficient manner than otherwise possible. Below is an example of Waltonchain's RIFD tags and their implementation on the clothing supply chain.[22]

[22] Waltonchain team, Whitepaper V2.0, Waltonchain (Sep. 4, 2018), https://waltonchain.org/templets/default/doc/Waltonchain%20White%20Paper%202.0_EN.pdf (last visited Oct. 20, 2018).



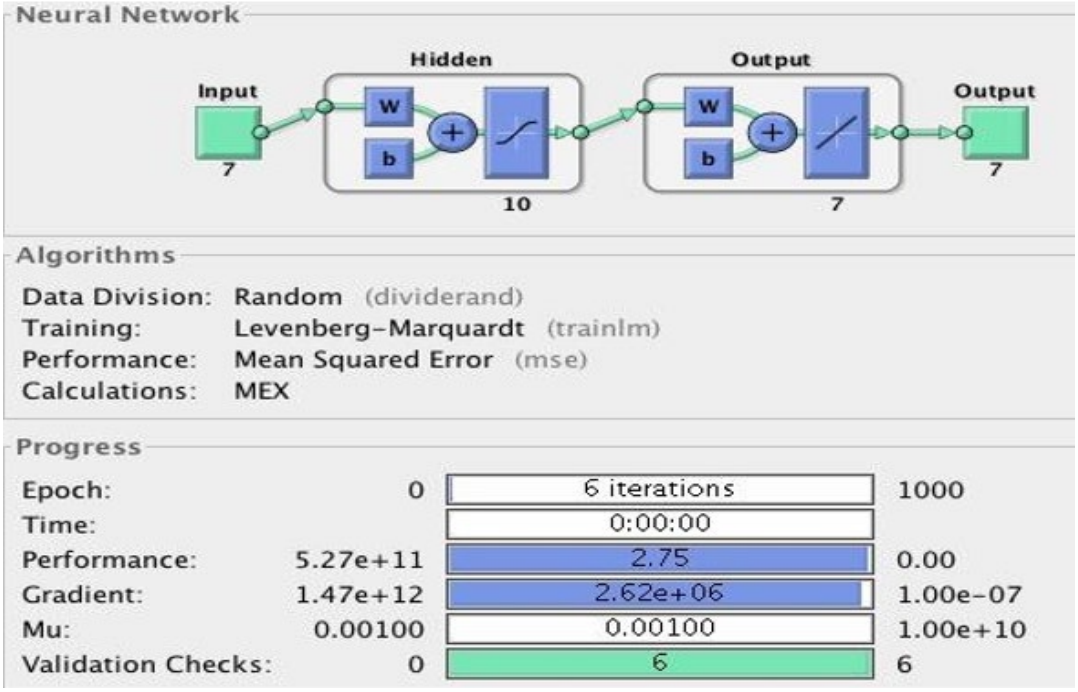
23

Machine learning should be used on the information gathered by AI and RFID tags. This will help prevent against future attempts of foreign espionage. A machine learning engine can test, train, and validate the data collected on a neural network.

[23] Waltonchain team, Whitepaper V1.0.4, Waltonchain (Aug. 0, 2018), https://www.waltonchain.org/doc/Waltonchain-whitepaper_en_20180208.pdf (last visited Oct. 20, 2018).

Neural networks take advantage of the way a biological brain solves problems with large clusters of biological neurons in neither a way that a standard computer nor a human process as efficiently. Neural Networks use a process called feed-forward backpropagation, which uses input variables to predict target variables. Neural Networks selfadjust input weights by testing millions of possibilities to optimize the target value proposed by the user, whether it is a specified value, a prediction, or optimization problem.

Here, the network would solve for the probabilty of a future event and where the AI algorithms and RFID blockchain systems should focus more strictly in the future. Companies such as Nvidia Corporation design GPUs specifically for this type of deep learning.[24] Below is an example of a mapped neural network for predicting future events.[25]



[24] Nvidia, Titan V, Nvidia Corporation (Oct. 10, 2018), https://www.nvidia.com/en-us/titan/titan-v/ (last visited Oct. 10, 2018).
[25] Anthony Macchiarulo, Machine Learning and Technical Analysis, Journal of Internet banking and Commerce (Apr. 4, 2018), http://www.icommercecentral.com/open-access/predicting-and-beating-the-stock-market-with-machine-learning-and-technical-analysis.php?aid=86901 (last visited Oct. 9, 2018).

VII. Conclusion

In conclusion, protecting consumer data privacy starts with protecting the multinational companies that serve consumers. If the global supply chain is not protected from foreign espionage and privacy attacks, then consumer privacy is at risk. AI and RFID surveillance is protected by the fourth amendment, sectoral privacy acts, and the GDPR. Building AI and RFID systems with privacy in mind from the start will help protect against future privacy violations. The application of AI and RFID technology will fulfill the NTIA's goals of consumer privacy management. Although the focus of many privacy professionals is on software, hardware, the entry point to the software is an evolving area of foreign espionage. As hardware hacking technology evolves, it is important the technology that combats this also evolves. In sum, an in-depth research into AI and RFID technology is required to protect against the invasion of privacy through hardware and the global supply chain.

Sincerely,

Anthony Macchiarulo

Anthony Macchiarulo
185 West Broadway
New York, NY 10013

November 9, 2018

Citations:

[1] Jordan Robertson and Michael Riley, The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, Bloomberg (Oct. 4, 2018), https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies (last visited Oct. 8, 2018).

[2] U.S. Const. Amend. IV.

[3] Florida v. Riley, 109 S.Ct. 693 (1989).

[4] Kyllo v. U.S., 121 S.Ct. 2038 (2011).

[5] U.S. v. Scott Douglas Lacy, 119 F.3d 742 (9th Cir 1997).

[6] U.S. v. Carey, 551 F.2d 309 (10th Cir 1999).

[7] U.S. v. Campos, 237 Fed.Appx. 949 (5th Cir 2007).

[8] Carpenter v. U.S, 108 S.Ct. 316 (1987).

[9] The Children's Online Privacy Protection Act.

[10] The Gramm–Leach–Bliley Act.

[11] The Health Insurance Portability and Accountability Act.

[12] The California Online Privacy Protection Act.

[13] The California Consumer Privacy Act.

[14] GDPR Art. I.

[15] GDPR Art. V.

[16] GDPR Art. XXV

[17] Rebecca Herold, Privacy Impact Assessment Full Report, Report (Jun. 1, 2012), https://iapp.org/media/pdf/knowledge_center/Generic_PIA_Report_-_The_Privacy_Professor_June_2012.pdf (last visited Oct. 20, 2018).

[18] The California Data Privacy Protection Act.

[19] The Electronic Communications Privacy Act

[20] Larry Dignan, Qure.ai launches AI system to read head CT scans and find abnormalities, ZDNet (Apr. 26, 2018), https://www.zdnet.com/article/qure-ai-launches-ai-system-to-read-head-ct-scans-and-find-abnormalities/ (last visited Oct. 12, 2018).

[21] Mark Rockwell, Harnessing machine learning for baggage scans, GCN (May 4, 2018), https://gcn.com/articles/2018/05/04/machine-learning-baggage-scans.aspx (last visited Oct. 12, 2018).

[22] Waltonchain team, Whitepaper V2.0, Waltonchain (Sep. 4, 2018), https://waltonchain.org/templets/default/doc/Waltonchain%20White%20Paper%202.0_EN.pdf (last visited Oct. 20, 2018).

[23] Waltonchain team, Whitepaper V1.0.4, Waltonchain (Aug. 0, 2018), https://www.waltonchain.org/doc/Waltonchain-whitepaper_en_20180208.pdf (last visited Oct. 20, 2018).

[24] Nvidia, Titan V, Nvidia Corporation (Oct. 10, 2018), https://www.nvidia.com/en-us/titan/titan-v/ (last visited Oct. 10, 2018).

[25] Anthony Macchiarulo, Machine Learning and Technical Analysis, Journal of Internet banking and Commerce (Apr. 4, 2018), http://www.icommercecentral.com/open-access/predicting-and-beating-the-stock-market-with-machine-learning-and-technical-analysis.php?aid=86901 (last visited Oct. 9, 2018).

Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, April 2018, vol. 23, no. 1

PREDICTING AND BEATING THE STOCK MARKET WITH MACHINE LEARNING AND TECHNICAL ANALYSIS

ANTHONY MACCHIARULO

Morgan Stanley and Co LLC NYC, NY, USA

Tel: **7185170966;**

Email: **macchiarulo.a@gmail.com**

Abstract

The paper studies whether machine learning or technical analysis best predicts the stock market and in turn generates the best return. The research back tests machine learning and technical analysis methods ten years in the past to predict ten years in the future. After prediction stage, the research incorporates the main findings into trading strategies to beat the S&P 500 index. To further this analysis, the paper examines all market periods and then examines the results specifically in up market and down-market periods. The sampling period is January 1995 through December 2005, and the trading period is January 2006 through December 2016. The null hypothesis is that machine learning and technical analysis would generate returns with no statistically significant difference. The study uses State Street's SPDR® SPY ETF as the benchmark. Data is retrieved from Bloomberg and Yahoo Finance. Outputs are calculated in R, MATLAB, SPSS, EVIEWS, Python, and SAS languages.

Keywords: **Machine Learning; Technical Analysis; Statistics; Predicting; Stock Market; Analysis; Investing; Trading; Securities**

INTRODUCTION

Machine Learning

The inspiration for the machine learning portion of the research stems from the paper "Stock Price Prediction uses Neural Network with Hybridized Market Indicators" by Ayodele, et al. [1] Sunday published in the Journal of Computing. This paper focuses on predicting the stock market with machine learning techniques such as neural networks, support vector machines, and various other projects.

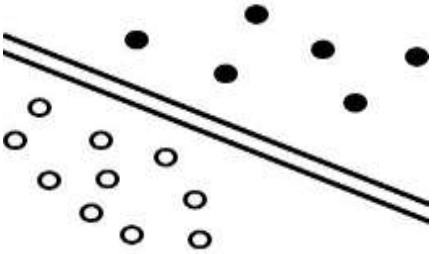
Machine Learning is a type of computational artificial intelligence that learns when exposed to new data. Machine Learning is used to predict the stock market. Some researchers claim that stock prices conform to the theory of random walk, which is that the future path of the price of a stock is not more predictable than random numbers. However, Stock prices do not follow random walks. There is sufficient evidence that shows that stock returns are predictable based on historical information. Three most prevalent Machine Learning Algorithms implemented in the field of finance are Support Vector Machines, Neural Networks, and Ensemble Learning. In the study, we use support vector machines to predict the relative direction of the stock market, and neural networks to predict the actual stock price and return. Ensemble learning allows us to combine the two machines into one prediction.

Support Vector Machine

Support Vector Machines increase the dimension of samples until it can linearly separate classes into a test set. Support Vector Machines use a mathematical formula known as the kernel function. The kernel function transforms the data so that there is a greater possibility of separable classes. When the machine has reached a state where it can linearly separate the classes, it attempts to find the optimal separation. When the machine has built its model, it can start to predict on new data by performing the same kernel transformation on the new data and decide what class it should belong to. The support vector machine creates a decision boundary where most points fall on either side of the boundary. The line in the support vector machine is known as the optimal hyper plane. A line is bad if it passes too close to the points because it will be too noise sensitive and it will not generalize correctly. Thus, the line passing as far as possible from all points is optimal. The standard formula for a hyper plane is $f(x)=\beta 0 + \beta Tx$. $\beta 0$ is referred to as the bias while βTx is the weight vector. The support vector uses Lagrange multipliers to obtain the weight and bias vector for the optimal hyper plane. Lagrange multiplier strategy attempts to find the local maximum and minimums of a function to equal constraints. The best

implication for a support vector machine is to predict the direction of the stock market, that being either positive for negative in different market types such as a bear or bull market. The Figure 1, details linear separation with the kernel function.

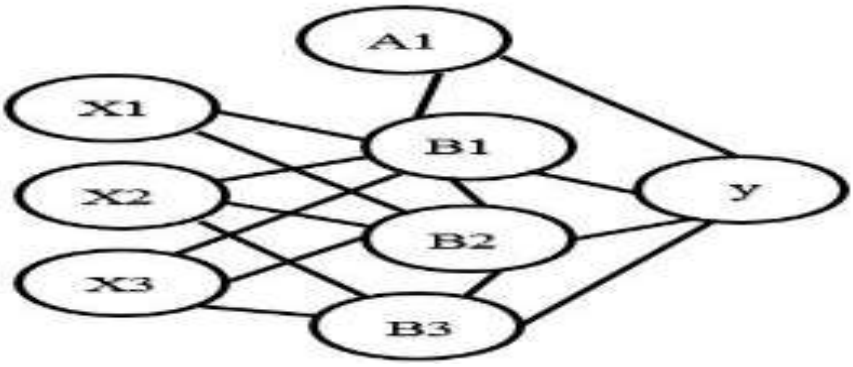
Figure 1: Support Vector Machine.



Neural Network

Neural networks take advantage of the way a biological brain solves problems with large clusters of biological neurons connected by axons in neither a way that a standard computer program cannot process nor a human process as efficiently. Neural Networks use a process called feed-forward backpropagation. The algorithm takes input variables and tries to predict the target variable. Neural Networks self-adjust input weights by testing millions of possibilities to optimize the target value to what is wanted by the user of the algorithm, whether it is a specified value, a prediction, or a maximization type of optimization problem. In our research, we will try to predict the stock market with the input variables. Trained data refers to the combination of input and target data. Neural network machines produce an R^2 of 0.99 if input and target data is consistent. An example of neural network is given below with three inputs, two hidden layers, and one target value (Figure 2).

Figure 2: Neural network.



Ensemble Learning

Ensemble Learning utilizes multiple learning algorithms to obtain better predictive powers. The learners are trained independently and predictions are combined to make the overall prediction. In our research, we will utilize ensemble learning to combine the results from the Neural Network and Support Vector Machines. Different techniques of ensemble learning relate to bootstrapping and stacking. Bagging or Bootstrap aggregating assigns equal weights to all the machines in the system. Stacking refers to separating algorithms and choosing the one with the best predictability. For our research stacking is the most efficient ensemble learning practice.

Noise

Noise is created from uncertainty and large impact events that can skew the machine learning process. The process of Cross validation is used to eliminate this from the model. Machine Learners attempt to build a model so that for a set of inputs, it can provide the wanted output. When the model emphasizes having low error too much, the model creates a decision boundary that is overly complicated and includes the noise. When the model allows for too great of an error, it is not able to properly divide the classes. To avoid the problems of over and under fitting; cross validation is used. Cross validation is a model evaluation method. Cross validation removes some of the data before training begins. When the training is done, the data that was removed is used to test the performance of the fitted model with unseen data.

Technical Analysis

The inspiration for the technical analysis portion of the research stems from the paper “Forecasting the NYSE composite index with technical analysis, pattern recognizer, neural network, and genetic algorithm: a case study in romantic decision support” by Leigh, et al. [2] published in the Journal of Finance. This paper focuses on predicting the stock market with technical analysis indicators as compared to neural network techniques of predicting the stock market.

As described in the paper, using technical analysis accepts a semi-strong form of the efficient markets hypothesis (“EMH”), which means that publicly available information about the stock should be factored into the stock price, and ignoring the weak form of EMH, which states that only past trading history has been built into the price. The paper examines the validity of the weak form of the EMH. In their comparison, they used a random-selection trading strategy to showcase the optimal weak EMH method. In their analysis, they took a series of price and volume patterns in different methods. They proved that the weak form EMH is not efficient in the face of momentum in stock prices. However, their most promising results were in the form of

neural networks which are incorporated into the machine learning [3-6].

DATA AND METHODOLOGY

Machine Learning

The first step in the machine learning process to examine historical data that will be tested and define the sample and testing period. The sampling period is January 1995 through December 2005, and the trading period is January 2006 through December 2016. The next step in the Machine Learning process is to collect the data that will be used to predict the future of the stock market. In a machine, there is a set of data that contains both input data and target data, target data is the answer which the algorithm should produce from the input. These two sets of data combined are usually referred to as the training data. The training data is given below. By using previous data the machine should be able to predict the next years with precision (Table 1) [7-12].

Table 1: Input data.

Driver	**Input Data**
S&P 500	Time
S&P 500	Open
S&P 500	High
S&P 500	Low
S&P 500	Close
S&P 500	Volume
Macroeconomic	United States 10 Yr. Treasury Bill
Macroeconomic	United States Inflation Rate
Macroeconomic	United States Unemployment Rate
Driver	Target Data
S&P 500	SPY Stock Price

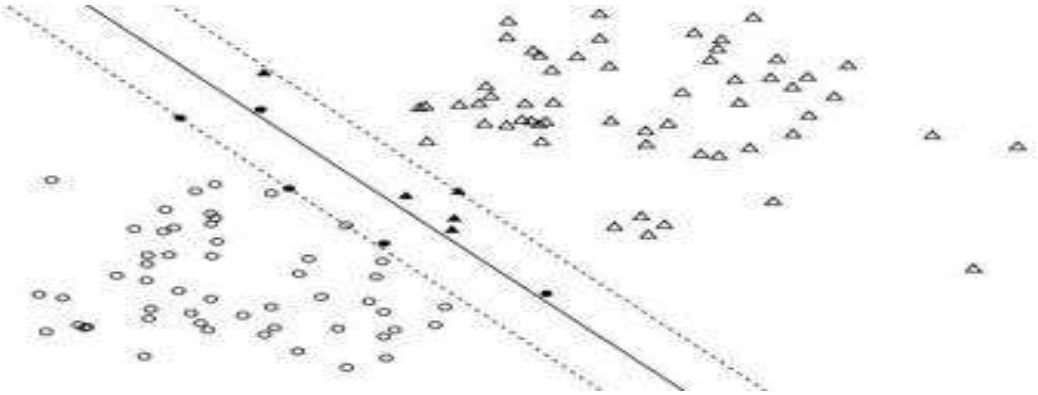
Support Vector Machine

The next study that must be performed is the Support Vector Machine. We will be

using the support vector machine to predict the market in both bull and bear trends. Using the input and target data we can fit the new model. The support vector machine asks for the number of data points and the number of dimensions. For the study, we will produce a set of positive and negative examples from two Gaussians. It is important to load standardized data such as sigma, the mean position, mean position for negative or bearish examples, and the mean position for bullish examples. Next the data must be trained. For the study, we split 80% into a training set and 20% into a test set. Using the kernel function, we predict the data points in the test set.

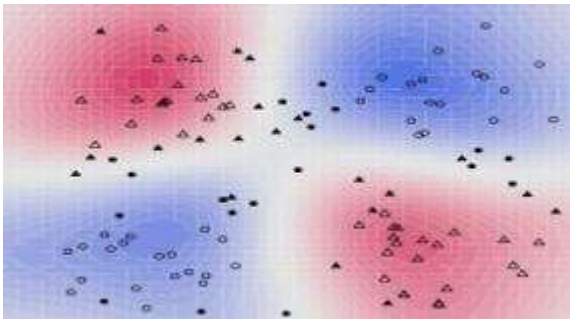
The dotted lines are the decision boundaries between positive and negative examples. The support vector is the black line. The triangle points above are the bullish scenario while the circle points below are the bearish scenario. The next step is to cross validate the training set to improve the quality of the machine and eliminate any noise. The k-fold and cross validation approaches are used by randomly splitting the number of samples into folds. Data is loaded into R. The Figure 3 is the linear support vector machine output.

Figure 3: Linear Support Vector Machine.



The linear support vector machine does not give all the information we need in predicting stock market direction. Just because we linearly separated positive or bullish and negative or bearish input parameters does not mean they are separable in real life. For example, if an economic rate falls that is considered a negative Gaussian but maybe the downward shift was a good sign for the economy. In the example of unemployment, if the unemployment rate decreases then that is good for the economy and is not accurately represented in the linear support vector machine. The nonlinear support vector machine tackles these problems in a more efficient manner. To transform the current machine into a nonlinear one we set the kernel parameter and a constant variable to one. Data is loaded into R, after running the nonlinear support vector machine, the results are shown in Figure 4.

Figure 4: Non-linear support vector machine.

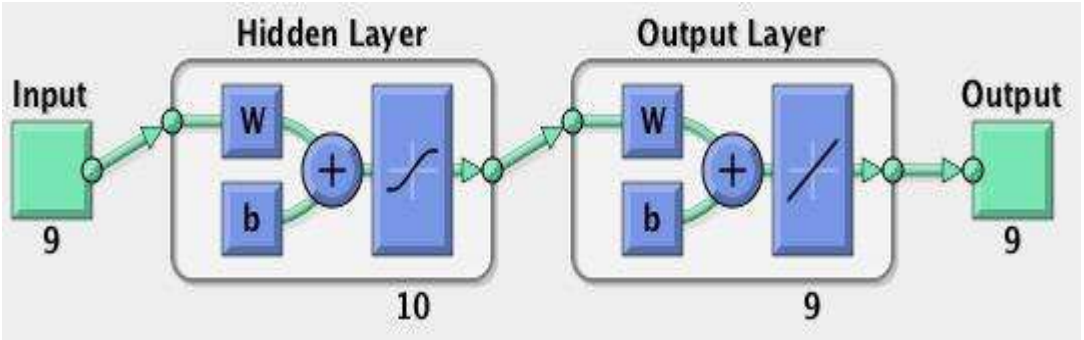


The linear and non-linear support vector machines tell the same conclusion in two different ways. For the linear support vector machine, there is more triangle or bullish points on the spectrum compared to bearish scenario. For the non-linear support vector machine, the bullish points are dispersed across the red heat map in much more quantities than the blue heat map. The darker red the heat map on the spectrum the more significance each point is making to the machine. In sum, this prediction dictates that there will be more bull trends than bear trends, which will make the stock market upward sloping and have a positive return for the trading period.

Neural Network

The next step is to fit the inputs and target into the neural network. The network developed will contain nine input variables with ten hidden layers. The target value or output in the neural network is the stock price in one year or the one-year return prediction for State Street's SPDR® SPY ETF ("SPY"). Data is loaded into MATLAB (Figure 5).

Figure 5: Neural network mapping.



Developing a neural network with external economic factors as inputs and the SPY stock price as output through feed-forward back propagation we assigned optimal

weights to the individual SPY data and the external economic factors to not only predict the stock price in one year but also show the allocation of factors that lead to the prediction.

To remain consistent nine input and target values are distributed daily. 70% of the neural network is trained, 15% validated, and 15% tested. After training, cross validating, and testing the data the network runs and produces R^2 for each piece of the network. The R^2 for training, cross validation and testing is 0.99. The R^2 for the model is 0.97. This means that the neural network was performed correctly can be accepted with large confidence. The error histogram shows that the errors are normally distributed around the mean. Running the same simulation in R gives the same results. Using two independent packages increases the reliability of the study being conducted. Below are the results (Figure 6 and Table 2) [13-22].

Figure 6: Neural network training, validation, testing.

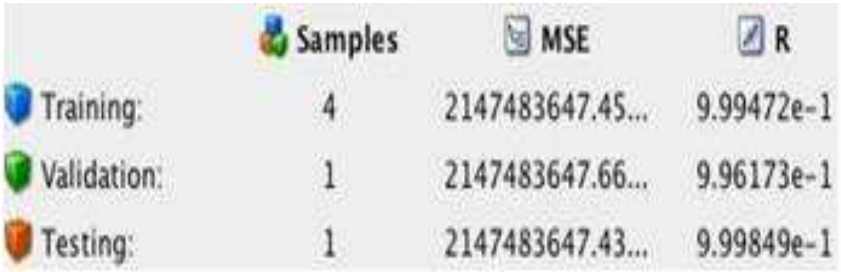


Table 2: Neural network output.

Input Data	**Weight**
Time	3.43%
Open	7.52%
High	8.32%
Low	7.94%
Close	41.32%
Volume	25.11%
10 Yr. T-Bill	2.02%
Inflation	3.12%
Unemployment	1.22%
Target	Result
SPY Stock Price	117.16%

The neural network predicts the stock market at very high precision. The neural network in both studies yielded a ten-year return of 117.16% on the close of trading

period. The neural network is only 1.04% below the actual return of 118.2%. That is very high predictability power. It is very interesting that the close price and volume of the SPY are the largest weights used by the network in determining the one year stock price. The external environmental factors play a much smaller role in the prediction determined by the network.

Machine Learning Trading Strategy

The next step is to develop the algorithm to trade based on the data. The support vector machine predicted the stock market to be upward sloping during the trading period and have a positive return. The support vector machine concludes this by dictating the number of bull and bear trends in the sample. With the support vector knowledge in mind running the neural network on the data predicted the stock market at a 1.04% margin of error. This is extremely high precision. In sum, the machine learning process has predicted that there will be more bull days than bear days and almost perfectly predicted the stock market. This type of knowledge is very powerful and useful to profit in finance.

When doing prediction, the close price and volume of the SPY are the largest weights used by the network in determining the one-year stock price. The external environmental factors play a much smaller role in the prediction determined by the network. Due to this discovery, the algorithm trades heavily based on lagged close prices and trading volume to maximize returns on the stock market. The algorithm trades by only rebalancing stocks in the S&P500 that are “winners” the day before that is a stock that ended positively the day before to incorporate the Support Vector Machine into the trades. Additionally, the rotation system does not execute rebalancing trades without there being larger volume compared to the stock’s average daily trading volume the day before. The results beat the S&P500 index as seen below. Additionally, we run a neural network in R for every previous period and if there was a larger weight given to closing price over trading volume we tweak the algorithm to check for close prices over trading volume 60% of the time as opposed to a 50/50 split. The vise-versa is true when trading volume was higher where we would trade on volume 60% of the time over close prices. The trading results are shown below. The algorithm is shown below before tweaking weights due to neural network parameter [23-30].

```
def initialize(context):
#constants
context.volu
me=0.5
context.clos
e=0.5
context.closed=data.history(sid(8554),
'price',          1,          '1d')
```

```
context.vol=data.history(sid(8554),
'volume', 1, '1d')
#ETF traded with weight
if context.vol > context.vol -1 and context.closed >
context.closed -1 then context.etfs={
  symbol('SPY'): 1.0, # State Street's SPDR® SPY ETF
}
end if
# Set commision
set_commission(commission.PerShare(cost=4.95, min_trade_cost=0.0))
# Rebalance portfolio
schedule_function(rebalance,date_rules.every_day(),
time_rules.market_open(minutes=35))
def rebalance (context, data):
for stock, weight in context.etfs.items():
order_target_percent(stock, weight*context.volume + weight*context.close)
```

The total return for the period is 204% as opposed to the S&P500 returns of 118.2%. The strategy beats the market on the long term as well. 69 times the machine learning strategy beats the market on a month to month basis out of 132 months. 52.27% of the time the strategy beats the markets monthly returns. The max drawdown of the strategy comes out to 46.9% during the recession. It is apparent the strategy does much better in a bullish market compared to a bearish market.

Running the strategy over ten years only produces a Beta of 0.72, which is less risky than investing in the market. Additionally, the Sharpe ratio is 0.51 and a Sortino negatively skewed at 0.71, and a volatility or standard deviation of 0.28. During the recession, the month with the highest beta was 2.598 during April 2007. This is expected and is much less risky than the market was during the time. In sum, the machine learning algorithm that learns based on the previous year and adjusts the strategy on percentage of buy and short based on trading volume and close prices beats the market by 85.8% over ten years with slightly higher volatility than the market. The strategy is more volatile 116 months out of the 131 months or 88.54% of the time the standard deviation of the strategy is higher than the market. For the higher volatility, the strategy to beat the market by almost doubles [31-34].

Technical Analysis

For each method, there were 120 total observations over the total sample period from January 2007 to December 2016. Machine learning had the highest overall average monthly return at 1.19%. During this same time-period, the S&P 500 had an average monthly return of .48%. The monthly average returns for the technical indicators ranged from .83% to -1.21%. The full listing of the average monthly returns listed in percent form is shown in Table 3.

Table 3: Whole sample period descriptive statistics (data in percent form).

	N	Minimum	Maximum	Mean	Std. Deviation
Machine Learning	120	-20.4	23.5	1.192917	7.347258
Bollinger Bands	120	-13.129	19.71627	0.831313	3.758738
Trading Envelopes	120	-13.129	19.71627	0.831313	3.758738
KBand	120	-13.129	13.31265	0.76489	4.25558
Cmdty Channel Index	120	-16.5331	13.06419	0.538209	3.622277
Stochastics	120	-9.02627	11.50051	0.492497	3.374356
William's %R	120	-9.02627	12.64072	0.408589	3.396424
Buy and Hold	120	-16.5331	14.2041	0.403511	4.553905
Fundamental Analysis	120	-18.46	10.18	0.383	4.45161
MA Envelopes	120	-6.10397	13.94343	0.289602	2.477517
RSI	120	-4.61304	12.65053	0.276992	1.865896
MACD	120	-9.07901	8.290536	0.255896	3.016252
Ichimoku	120	-5.92016	7.675862	0.050554	2.08152
Triangular MA	120	-8.58764	6.438574	-0.1277	2.515717
DMI	120	-14.0814	8.636103	-0.19479	2.808664
Exponential MA	120	-8.7846	8.829373	-0.22599	2.59998
MA Oscillator	120	-10.4149	10.87842	-0.23029	3.917283
Fear and Greed	120	-13.9833	9.543643	-0.23482	3.406039
Simple MA	120	-16.8559	8.496324	-0.54573	3.442464
Weighted MA	120	-15.3914	6.827461	-0.55405	3.148252
Variable MA	120	-23.4974	6.569704	-0.67838	3.79582
Parabolic	120	-23.3883	11.8544	-0.69678	4.676691
Accum/Distrib Osc	120	-21.6401	16.67208	-1.01638	5.40478

Rex Oscillator	120	-18.6651	11.25333	-1.02282	4.683956
Rate of Change	120	-18.1407	14.31845	-1.20797	4.95222
Valid N (list wise)	120				

After gathering the sample period data, we separated out the observations into those that occurred in an up market from those in a down market. This was done by looking at the returns of the S&P 500. For months when it was positive, the returns for that month were classified as up market and when it was negative; the returns were classified as down market. The up-market period had a total of 72 observed months. During this time, the S&P 500 had an average monthly return of 3.22%. Machine learning had 4.13% monthly average return, approximately 1% above the next highest method. As seen in Table 3, the technical indicators ranged from 2.99% to -1.01% (Table 4).

Table 4: Up market descriptive statistics (data in percent form).

		Minimum	**Maximum**	**Mean**	**Std. Deviation**
Machine Learning	72	-8.2	23.5	4.1289	5.96786
Fundamental Analysis	72	0.02	10.18	3.1292	2.30648
Buy and Hold	72	-2.49769	14.2041	2.988633	2.976227
Bollinger Bands	72	-2.44045	19.71627	1.092965	3.311484
Trading Envelopes	72	-2.44045	19.71627	1.092965	3.311484
Cmdty Channel Index	72	-4.63839	7.445843	0.391186	2.841843
RSI	72	-2.83878	12.65053	0.31323	2.091257
Stochastics	72	-5.28675	11.50051	0.296028	3.367026
Fear and Greed	72	-7.86461	9.543643	0.164008	2.801145
Triangular MA	72	-6.90072	4.913777	0.110924	2.06229
Ichimoku	72	-5.52048	4.376417	0.069515	1.529319
KBand	72	-6.10397	9.010012	0.060722	3.453896

Exponential MA	72	-8.7846	8.829373	0.056914	2.64089
MA Envelopes	72	-6.10397	8.57509	0.052518	1.949429
MACD	72	-6.44503	8.215632	0.041862	2.892891
William's %R	72	-6.86243	9.890922	0.034897	2.869658
DMI	72	-6.88233	4.667657	0.00081	2.372219
Parabolic	72	-9.11704	10.87842	-0.12789	3.630527
Rex Oscillator	72	-15.5689	11.25333	-0.30996	4.202107
Simple MA	72	-16.8559	8.496324	-0.3947	3.452201
Weighted MA	72	-15.3914	4.913777	-0.45	3.179792
MA Oscillator	72	-10.4149	10.87842	-0.61118	3.596882
Variable MA	72	-23.4974	6.569704	-0.63494	4.044417
Accum/Distrib Osc	72	-17.8133	8.257169	-0.89352	3.753331
Rate of Change	72	-17.8133	5.857087	-1.00538	4.130339
Valid N (list wise)	72				

For the down market, as seen below in Table 5, we only had a total of 48 observations. During the time, the S&P 500 had an average monthly return of -3.63%. Machine learning did not perform as well as in the whole sample and up market periods and had -3.21% for its monthly average return. However, the technical indicators were more varied ranging between 1.82% to -3.47% (Table 5).

Table 5: Down market descriptive statistics (data in percent form).

	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
KBand	48	-13.129	13.31265	1.821142	5.092432
William's %R	48	-9.02627	12.64072	0.969127	4.028968
Stochastics	48	-9.02627	8.703512	0.797199	3.399316

Cmdty Channel Index	48	-16.5331	13.06419	0.758744	4.575824
MA Envelopes	48	-5.4208	13.94343	0.645228	3.095968
MACD	48	-9.07901	8.290536	0.576946	3.196419
Bollinger Bands Trading Envelopes MA Oscillator	48	-13.129	15.85366	0.438836	4.352406
	48	-13.129	15.85366	0.438836	4.352406
	48	-9.04289	10.24691	0.341037	4.330465
RSI	48	-4.61304	4.268927	0.222634	1.484401
Ichimoku	48	-5.92016	7.675862	0.022111	2.726831
Triangular MA	48	-8.58764	6.438574	-0.48563	3.062873
DMI	48	-14.0814	8.636103	-0.49819	3.365372
Expoential MA	48	-8.53862	6.070957	-0.65036	2.504656
Weighted MA	48	-9.08872	6.827461	-0.71012	3.127204
Variable MA	48	-8.83962	5.930361	-0.74354	3.429761
Simple MA	48	-9.56601	5.930361	-0.77227	3.451656
Fear and Greed Accum/Distrib Osc	48	-13.9833	7.076658	-0.83306	4.112265
	48	-21.6401	16.67208	-1.20066	7.254137
Rate of Change	48	-18.1407	14.31845	-1.51186	6.01379
Parabolic	48	-23.3883	11.8544	-1.55011	5.850289
Rex Oscillator	48	-18.6651	10.76828	-2.09211	5.189241
Machine Learning	48	-20.4	14.19	-3.211	7.06144
Buy and Hold	48	-16.5331	2.241661	-3.47417	3.678578

Fundamental Analysis	48	-18.46	-0.1	-3.7363	3.64085
Valid N (listwise)	48				

RESULTS

To test for statistical significance for the machine learning results compared to those of the technical analysis, we used paired samples t-tests. The results, as seen below in Table 6, are ordered from the highest average monthly return to the lowest for each of the technical indicators, compared to the machine learning results which had the highest mean. At a 95% confidence level, machine learning outperformed the following technical indicators: fear and greed, simple MA, weighted MA, variable MA, parabolic, accum/distrib osc, Rex Oscillator, and rate of change. For the up-market period, machine learning had outperformed technical analysis results by a relatively large margin. As seen in Table 7 below, the results for the up-market period were better than those from the total 120 observations. At the 99% confidence level, machine learning outperformed compared to all but the buy and hold technical analysis method. Those two it outperformed with marginal significance at the 80% level. Compared to the results from the whole sample, this indicates that machine learning will be more likely to outperform in an up-market period.

Table 6: Paired t-test results (entire period, data in percent form).

Pair	Strategy	Mean	Std. Dev.	Std. Error Mean	Lower (95%)	Upper (95%)	T	Df	Sig (two tailed)
Pair 1	Bollinger Bands – Machine Learning	-0.36	8.2	0.74	-1.84	1.21	-0.48	119	0.63
Pair 2	Trading Envelopes – Machine Learning	-0.36	8.2	0.74	-1.84	1.12	-0.553	119	0.63
Pair 3	KBand – Machine Learning	-0.42	8.4	0.77	-1.96	1.104	-0.873	119	0.581
Pair 4	Cmdty Channel Index – Machine Learning	-0.654	8.2	0.74	-2.139	0.733	-0.967	119	0.384
Pair 5	Stochastics – Machine Learning	-0.7	7.9	0.72	-2.31	0.751	-1.01	119	0.335
Pair 6	Williams %R – Machine Learning	-0.78	8.49	0.77	-1.95	0.37	-1.34	119	0.314
Pair 7	Buy and Hold – Machine Learning	-0.8099	6.4	0.58	-1.99	0.29	-1.46	119	0.181

Pair 8	Fundamental Analysis – Machine Learning	-0.9033	6.09	0.55	-2.139	0.53	-1.24	119	0.148
Pair 9	MA Envelopes – Machine Learning	-0.915	7.94	0.77	-2.139	0.53	-1.3	119	0.215
Pair 10	RSI – Machine Learning	-0.93	7.68	0.74	-2.139	0.47	-1.19	119	0.194
Pair 11	MACD – Machine Learning	-1.14	8.68	0.74	-2.139	0.62	-1.776	119	0.236
Pair 12	Ichimoku – Machine Learning	-1.32	7.54	0.68	-3.009	0.22	-2.077	119	0.1
Pair 13	Triangular MA – Machine Learning	-1.38	8.13	0.72	-2.78	0.15	-2.32	119	0.078
Pair 14	DMI – Machine Learning	-1.41	8.12	0.74	-3.21	0.081	-2.3	119	0.064
Pair 15	Exponential MA – Machine Learning	-1.42	7.9	0.69	-3.41	0.01	-2.41	119	0.052
Pair 16	MA Oscillator – Machine Learning	-1.42	8.77	0.741	-3.8	0.16	-1.46	119	0.078
Pair 17	Fear and Greed – Machine Learning	-1.73	8.1	0.74	-3.667	-0.066	-1.24	119	0.04
Pair 18	Simple MA – Machine Learning	-1.74	8.3	0.74	-3.891	-0.25	-1.3	119	0.022
Pair 19	Weighted MA – Machine Learning	-1.14	8.4	0.722	-3.009	-0.24	-2.32	119	0.023
Pair 20	Variable MA – Machine Learning	-1.87	8.03	0.743	-2.78	-0.33	-2.3	119	0.017
Pair 21	Parabolic– Machine Learning	-1.88	8.241	0.74	-3.21	-0.36	-2.41	119	0.016
Pair 22	Accum/Distrib Osc. – Machine Learning	-2.02	8.805	0.74	-3.41	-0.61	-2.79	119	0.007
Pair 23	Rex Oscillator – Machine Learning	-2.21	8.031	0.74	-1.99	-0.76	-3.02	119	0.003
Pair 24	Rate of Change – Machine Learning	-2.4	8.24	0.734	-3.891	-0.9098	-3.11	119	0.002

The results for the down-market period showcased the weakness of machine learning. Although it performed above many technical indicators in the positive return period, it underperformed in the down-market period. Over the 48 observed months with a negative S&P 500 return, machine learning was close to being the lowest average monthly returns (Table 7).

Table 7: Up market paired samples t-test (data in percent form).

Pair	Strategy	Mean	Std. Dev.	Std. Error Mean	Lower (95%)	Upper (95%)	T	Df	Sig (two tailed)
Pair 1	Bollinger Bands – Machine Learning	-0.9997	5.675	0.66	-2.33	0.333	-1.4	71	0.139
Pair 2	Trading Envelopes – Machine Learning	-3.035	6.78	0.79	-4.62	-1.44	-3.7	71	0.118
Pair 3	KBand – Machine Learning	-3.034	6.857	0.79	-4.6	-1.44	-3.7	71	0
Pair 4	Cmdty Channel Index – Machine Learning	-3.73	6.42	0.802	-5.33	-2.13	-3.7	71	0
Pair 5	Stochastics – Machine Learning	-3.81	5.93	0.76	-6.72	-2.05	-3.7	71	0
Pair 6	Williams %R – Machine Learning	-3.82	6.87	0.808	-6.12	-2.04	-4.6	71	0
Pair 7	Buy and Hold – Machine Learning	-3.96	6.69	0.74	-4.62	-2.66	-4.7	71	0
Pair 8	Fundamental Analysis – Machine Learning	-4.01	5.93	0.75	-4.6	-2.45	-5.3	71	0
Pair 9	MA Envelopes – Machine Learning	-4.07	5.93	0.69	-5.33	-2.05	-5.8	71	0
Pair 10	RSI – Machine Learning	-4.09	7.17	0.809	-4.6	-2.04	-5	71	0
Pair 11	MACD – Machine Learning	-4.09	6.77	0.76	-6.72	-2.66	-5.1	71	0
Pair 12	Ichimoku – Machine Learning	-3.96	6.96	0.78	-6.12	-2.66	-5.5	71	0
Pair 13	Triangular MA – Machine Learning	-4.01	6.42	0.74	-6.11	-2.66	-5.6	71	0
Pair 14	DMI – Machine Learning	-4.07	5.93	0.801	-6.43	-2.45	-5.7	71	0
Pair 15	Exponential MA – Machine Learning	-4.07	6.87	0.74	-6.47	-2.45	-5.5	71	0
Pair 16	MA Oscillator – Machine Learning	-4.09	6.42	0.78	-6.72	-2.04	-5.6	71	0
Pair 17	Fear and Greed – Machine Learning	-4.09	6.42	0.74	-6.9	-2.66	-5.7	71	0
Pair 18	Simple MA – Machine Learning	-4.07	5.93	0.801	-6.11	-2.45	-5.5	71	0

Pair 19	Weighted MA – Machine Learning	-4.07	6.87	0.74	-6.43	-2.04	-5.6	71	0
Pair 20	Variable MA – Machine Learning	-4.09	6.78	0.78	-6.47	-2.66	-5.7	71	0
Pair 21	Parabolic– Machine Learning	-4.09	6.857	0.74	-6.72	-2.04	-5.7	71	0
Pair 22	Accum/Distrib Osc. – Machine Learning	-3.81	6.42	0.801	-6.47	-2.66	-5.5	71	0
Pair 23	Rex Oscillator – Machine Learning	-5.022	7.26	0.855	-6.729	-3.31	-5.8	71	0
Pair 24	Rate of Change – Machine Learning	-5.13	7.51	0.8855	-6.9	-3.36	-5.7	71	0

At a 95% confidence level, machine learning underperformed compared to the following technical analysis methods: KBand, William's %R, Stochastics, Cmdty Channel Index, MA Envelopes, MACD, Bollinger Bands, Trading Envelopes, RSI, Ichimoku, Triangular MA, DMI, Exponential MA, Weighted MA, Variable MA and Fear and Greed. With a marginal significance of 20%, machine learning significantly unperformed compared to Simple MA, Accum/Distrib OSC, and Rate of Change (Table 8).

Table 8: Down market paired samples t-test.

Pair	**Strategy**	**Mean**	**Std. Dev.**	**Std. Error Mean**	**Lower (95%)**	**Upper (95%)**	**T**	**Df**	**Sig (two tailed)**
Pair 1	Bollinger Bands – Machine Learning	5.03	7.74	1.118	3.15	6.9	4.5	47	0
Pair 2	Trading Envelopes – Machine Learning	4.1	8.45	1.22	2.13	6.22	3.4	47	0.001
Pair 3	KBand – Machine Learning	3.99	7.11	1.02	2.27	5.7	3.8	47	0
Pair 4	Cmdty Channel Index – Machine Learning	3.96	8.921	1.28	1.62	5.94	3.48	47	0.001
Pair 5	Stochastics – Machine Learning	3.64	7.74	1.118	3.15	6.9	3.22	47	0.001
Pair 6	Williams %R – Machine Learning	3.78	7.11	1.02	2.27	5.7	3.8	47	0.005
Pair 7	Buy and Hold – Machine Learning	2.37	8.921	1.28	1.62	5.94	3.48	47	0.005
Pair 8	Fundamental Analysis –	2.01	8.57	1.237	1.57	5.72	2.95	47	0.005

	Machine Learning								
Pair 9	MA Envelopes – Machine Learning	2.69	7.74	1.118	3.15	6.9	2.95	47	0.005
Pair 10	RSI – Machine Learning	3.99	7.11	1.02	2.27	5.7	3.8	47	0.005
Pair 11	MACD – Machine Learning	3.96	8.921	1.28	1.62	5.94	3.48	47	0.002
Pair 12	Ichimoku – Machine Learning	3.64	7.74	1.118	3.15	6.9	3.45	47	0.037
Pair 13	Triangular MA – Machine Learning	2.21	8.08	1.02	1.57	4.787		47	0.347
Pair 14	DMI – Machine Learning	2.23	8.24	1.28	1.66	4.85	3.22	47	0.231
Pair 15	Exponential MA – Machine Learning	2.27	8.4	1.237	0.58	4.873	3.8	47	0.783
Pair 16	MA Oscillator – Machine Learning	3.99	8.37	1.118	0.46	4.53	3.48	47	0.581
Pair 17	Fear and Greed – Machine Learning	3.96	8.412	1.213	0.401	4.49	2.95	47	0.005
Pair 18	Simple MA – Machine Learning	3.64	7.68	1.02	0.517	4.47	1.499	47	0.005
Pair 19	Weighted MA – Machine Learning	3.99	9.29	1.28	-0.23	4.23	1.541	47	0.006
Pair 20	Variable MA – Machine Learning	3.96	7.63	1.237	-0.85	4.26	0.95	47	0.47
Pair 21	Parabolic– Machine Learning	3.64	9.47	1.118	-1.19	3.95	-0.264	47	0.783
Pair 22	Accum/Distrib Osc. – Machine Learning	1.1	8.15	1.12	-0.85	3.09	-2.64	47	0.581
Pair 23	Rex Oscillator – Machine Learning	-0.26	6.89	0.99	-1.932	1.406	-0.261	47	0.006
Pair 24	Rate of Change – Machine Learning	-0.5252	6.7	0.97	-2.15	1.1	-0.541	47	0.47

CONCLUSION

In conclusion, after analyzing the results, we conclude that using machine learning as a trading strategy can positively impact the returns generated compared to using many technical indicators. We found that there was no statistically significant difference between using machine learning and using technical analysis. In up market periods, machine learning will outperform technical analysis. However, if the market is a down market it is more beneficial to use technical analysis. Machine

Learning performs better in up markets because it uses momentum to its advantage by calculating the optimal weights that need to be traded on in the market paired with the future direction. On the other hand, technical analysis performs much better at spotting potential drawdowns, especially when using so many different trading strategies it is apparent some work better than others in down markets. For future research, we would recommend examining similar methods over a longer time-period. Because the down market only had 48 observations, it might have decreased the usability of the results.

REFERENCES

1. Ayodele A, Charles A, Marion A, Sunday O. Stock price prediction using neural network with hybridized market indicators. The Journal of Computing, pp: 2-54.
2. Leigh W, Purvis R, Ragusa JM. Forecasting the NYSE composite index with technical analysis, pattern recognizer, neural network, and genetic algorithm: a case study in romantic decision support. Journal of Finance, pp: 10-112.
3. Abarbanell J, Bushee B. Fundamental analysis, future earnings, and stock prices. Journal of Accounting Research, pp: 8-45.
4. Freeman JA, Skapura DM (1991) Neural networks: algorithms, applications and programming techniques. Addison Wesley Longman, pp: 18-44.
5. Vikas A, Naik NY (2004) Risk and portfolio decisions involving hedge funds. Review of Financial Studies 17: 63-98.
6. Karazoglou A. Supper vector machines in R. Journal of statistical software, pp: 12-28.
7. Andrew A, Gorovyy S, van Inwegen GB (2011) Hedge fund leverage. Journal of Financial Economics 102: 102-126.
8. Heckerling PS, Canaris G, Flach SD, Tape TG, Wigton RS,et al. (2007) Predictors of urinary tract infection based on artificial neural networks and genetic algorithms. International Journal of Medical Informatics 76: 289-296.
9. Watkins C (2000) Dynamic alignment kernels. In: Smola A, Bartlett PL, Sch¨olkopf B, Schuurmans D (eds.), Advances in large margin classifiers. MIT Press, Cambridge, MA, pp: 39-50.
10. Clifford A, Krail R, Liew J (2001) Do hedge funds hedge? Journal of Portfolio Management 28: 6-19.
11. Ali A, Magnor O, Schultalbers M (2009) Misfire detection using a neural network based pattern recognition. International Conference on Artificial Intelligence and Computational Intelligence.
12. Anand MV (1994) S&P 500 trading strategies and stock betas. Review of Financial Studies 7: 215-251.

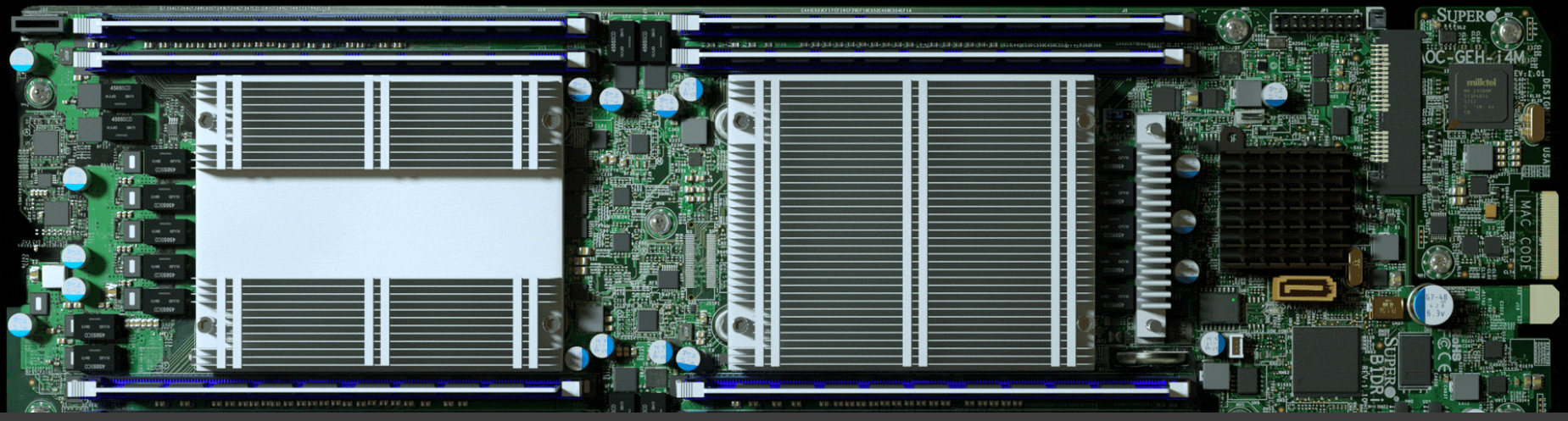
13. Dimitri V, Woolley P (2013) An institutional theory of momentum and reversal. Review of Financial Studies 26: 1087-1145.
14. Dybowski R, Gant V (2007) Clinical applications of artificial neural networks. Cambridge University Press, pp: 2-33.
15. Gil D, Johnsson M, Garicia Chemizo JM, Paya AS, Fernandez DR (2009) Application of artificial neural networks in the diagnosis of urological dysfunctions. Expert Systems with Applications 36: 5754-5760.
16. Wang Y-G, Li H-P (2010) Remote sensing image classification based on artificial neural network. International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE).
17. R Development Core Team (2008) R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria.
18. ISO/IEC (2014) ISO International Standard ISO/IEC 14882:2014(E) - Programming Language C++. Working draft, Geneva, International Organization for Standardization (ISO), Switzerland.
19. Van Rossum G. Python tutorial, Technical Report CS-R9526, Centrum voor Wiskunde en Informatica (CWI), Amsterdam, May 1995. Python Software Foundation. Python Language Reference, version 2.7.
20. MATLAB and Signal Processing Toolbox Release 2012. The Math Works, Inc., Natick, Massachusetts, United States.
21. IBM Corp (2013) IBM SPSS Statistics for Windows, Version 22.0. Armonk. IBM Corp, NY.
22. SAS Institute Inc. Cary, NC, 1989-2007.
23. Friedrich A, Lutz VC (1950) Monetary and foreign exchange policy in Italy.
24. Schlesinger ER (1952) Multiple exchange rates and economic development.
25. White WR (2000) What have we learnt from recent financial crises and policy responses? BIS Working Papers.
26. Bloomberg (2012) Bloomberg Professional.
27. CRSP/Compustat Merged (2012) CRSP/Compustat Merged. Center for Research in Security Prices.
28. Thomson One Banker (2012) Thomson One Banker. Thomson Reuters.
29. Bloomberg LP (2006) Stock price graph for SPDR® SPY ETF.
30. Widrow B, Lehr M (1990) 30 Years of Adaptive Neural Networks: Perceptron, Madaline and Backpropagation. Proceedings of the IEEE 78: 1420-1442.
31. Anderson J, Rosenfeld E (1988) Neurocomputing: Foundations of Research. MIT Press, Cambridge, MA.
32. Arrowsmith D, Place C (1990) An introduction to dynamical systems. Cambridge University Press, Cambridge, UK.
33. Dittman DJ, Khoshgoftaar TM, Napolitano A. Selecting the appropriate ensemble learning approach for balanced bioinformatics data.

34. Khoshgoftaar TM, Dittman DJ, Wald R, Fazelpour A (2012) First order statistics based feature selection: A diverse and powerful family of feature selection techniques. Proceedings of the Eleventh International Conference on Machine Learning and Applications (ICMLA): Health Informatics Workshop, pp: 151-157.

October 4, 2018, 5:00 AM EDT

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.



In 2015, Amazon.com Inc. began quietly evaluating a startup called Elemental Technologies, a potential acquisition to help with a major expansion of its streaming video service, known today as Amazon Prime Video. Based in Portland, Ore., Elemental made software for compressing massive video files and formatting them for different devices. Its technology had helped stream the Olympic Games online, communicate with the International Space Station, and funnel drone footage to the Central Intelligence Agency. Elemental's national security contracts weren't the main reason for the proposed acquisition, but they fit nicely with Amazon's government businesses, such as the highly secure cloud that Amazon Web Services (AWS) was building for the CIA.

To help with due diligence, AWS, which was overseeing the prospective acquisition, hired a third-party company to scrutinize Elemental's security, according to one person familiar with the process. The first pass uncovered troubling issues, prompting AWS to take a closer look at Elemental's main product: the expensive servers that customers installed in their networks to handle the video compression. These servers were assembled for Elemental by Super Micro Computer Inc., a San Jose-based company (commonly known as Supermicro) that's also one of the world's biggest suppliers of server motherboards, the fiberglass-mounted clusters of chips and capacitors that act as the neurons of data centers large and small. In late

▲ Featured in *Bloomberg Businessweek*, Oct. 8, 2018. Subscribe now. PHOTOGRAPHER: VICTOR PRADO FOR BLOOMBERG BUSINESSWEEK

Nested on the servers' motherboards, the testers found a tiny microchip, not much bigger than a grain of rice, that wasn't part of the boards' original design. Amazon reported the discovery to U.S. authorities, sending a shudder through the intelligence community. Elemental's servers could be found in Department of Defense data centers, the CIA's drone operations, and the onboard networks of Navy warships. And Elemental was just one of hundreds of Supermicro customers.

During the ensuing top-secret probe, which remains open more than three years later, investigators determined that the chips allowed the attackers to create a stealth doorway into any network that included the altered machines. Multiple people familiar with the matter say investigators found that the chips had been inserted at factories run by manufacturing subcontractors in China.

This attack was something graver than the software-based incidents the world has grown accustomed to seeing. Hardware hacks are more difficult to pull off and potentially more devastating, promising the kind of long-term, stealth access that spy agencies are willing to invest millions of dollars and many years to get.

"Having a well-done, nation-state-level hardware implant surface

There are two ways for spies to alter the guts of computer equipment. One, known as interdiction, consists of manipulating devices as they're in transit from manufacturer to customer. This approach is favored by U.S. spy agencies, according to documents leaked by former National Security Agency contractor Edward Snowden. The other method involves seeding changes from the very beginning.

One country in particular has an advantage executing this kind of attack: China, which by some estimates makes 75 percent of the world's mobile phones and 90 percent of its PCs. Still, to actually accomplish a seeding attack would mean developing a deep understanding of a product's design, manipulating components at the factory, and ensuring that the doctored devices made it through the global logistics chain to the desired location—a feat akin to throwing a stick in the Yangtze River upstream from Shanghai and ensuring that it washes ashore in Seattle. "Having a well-done, nation-state-level hardware implant surface would be like witnessing a unicorn jumping over a rainbow," says Joe Grand, a hardware hacker and the founder of Grand Idea Studio Inc. "Hardware is just so far off the radar, it's almost treated like black magic."

But that's just what U.S. investigators found: The chips had been inserted during the manufacturing process, two officials say, by operatives from a unit of the People's Liberation Army. In Supermicro, China's spies appear to have found a perfect conduit for what U.S. officials now describe as the most significant supply chain attack known to have been carried out against American companies.

servers in two years for a new global network of data centers. Three senior insiders at Apple say that in the summer of 2015, it, too, found malicious chips on Supermicro motherboards. Apple severed ties with Supermicro the following year, for what it described as unrelated reasons.

In emailed statements, Amazon (which announced its acquisition of Elemental in September 2015), Apple, and Supermicro disputed summaries of *Bloomberg Businessweek*'s reporting. "It's untrue that AWS knew about a supply chain compromise, an issue with malicious chips, or hardware modifications when acquiring Elemental," Amazon wrote. "On this we can be very clear: Apple has never found malicious chips, 'hardware manipulations' or vulnerabilities purposely planted in any server," Apple wrote. "We remain unaware of any such investigation," wrote a spokesman for Supermicro, Perry Hayes. The Chinese government didn't directly address questions about manipulation of Supermicro servers, issuing a statement that read, in part, "Supply chain safety in cyberspace is an issue of common concern, and China is also a victim." The FBI and the Office of the Director of National Intelligence, representing the CIA and NSA, declined to comment.

Related:

- Statements From Amazon, Apple, Supermicro, and Beijing
- The Software Side of China's Supply Chain Attack
- Inside the Chinese Cyberspies' Bag of Tech Tricks

---

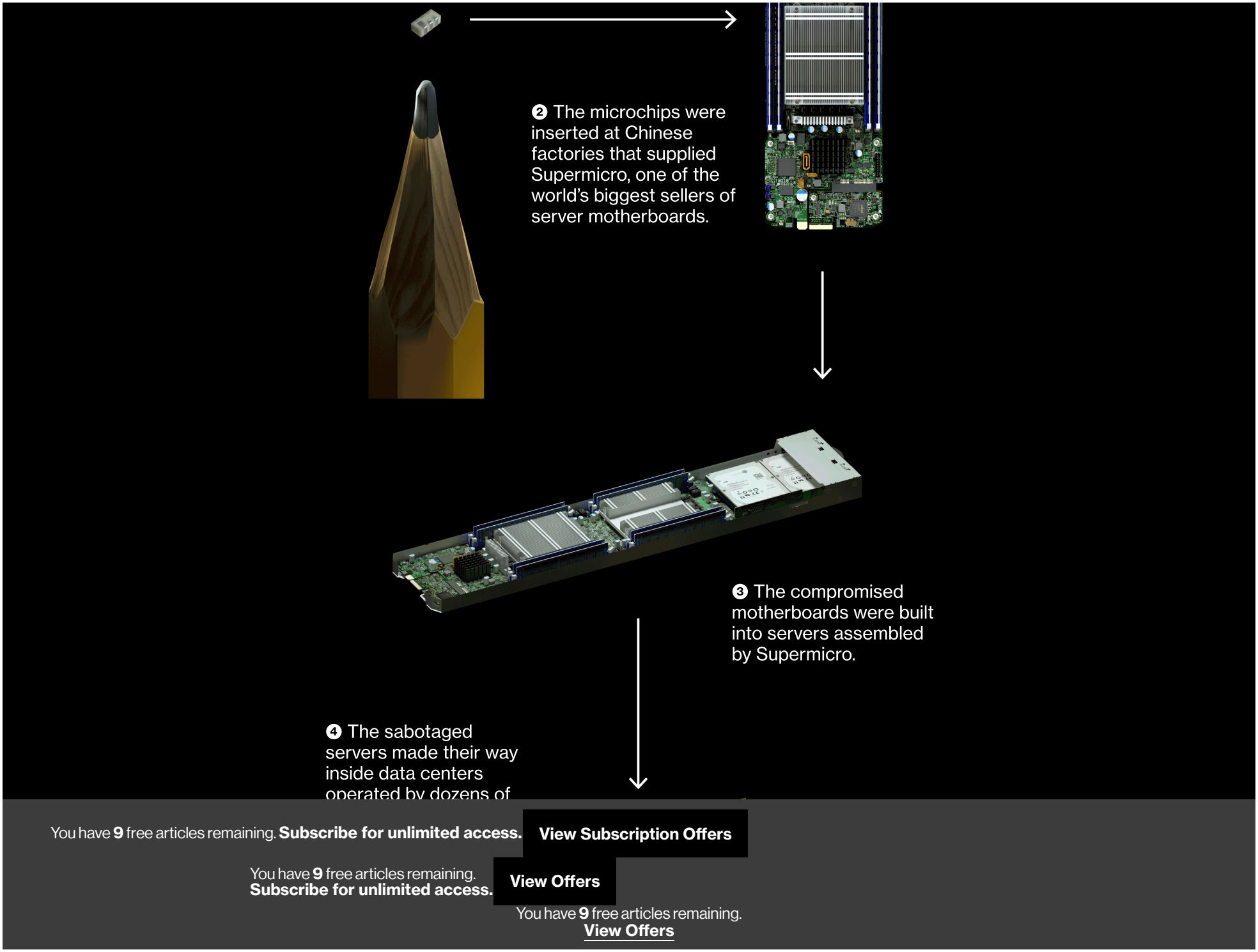
of those officials and two people inside AWS provided extensive information on how the attack played out at Elemental and Amazon; the official and one of the insiders also described Amazon's cooperation with the government investigation. In addition to the three Apple insiders, four of the six U.S. officials confirmed that Apple was a victim. In all, 17 people confirmed the manipulation of Supermicro's hardware and other elements of the attacks. The sources were granted anonymity because of the sensitive, and in some cases classified, nature of the information.

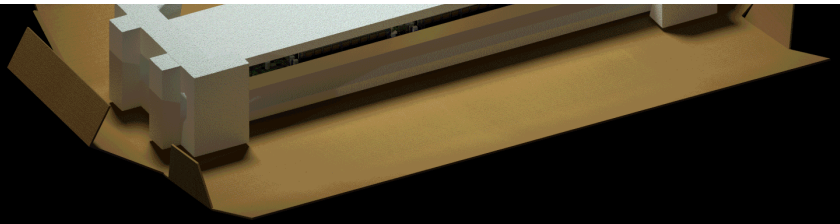
One government official says China's goal was long-term access to high-value corporate secrets and sensitive government networks. No consumer data is known to have been stolen.

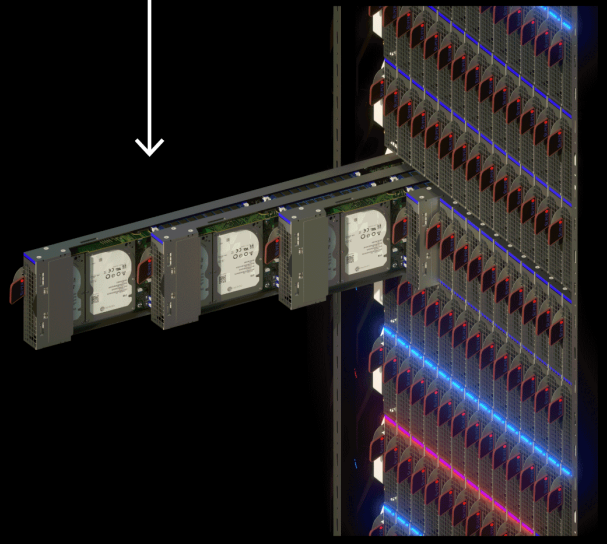
The ramifications of the attack continue to play out. The Trump administration has made computer and networking hardware, including motherboards, a focus of its latest round of trade sanctions against China, and White House officials have made it clear they think companies will begin shifting their supply chains to other countries as a result. Such a shift might assuage officials who have been warning for years about the security of the supply chain—even though they've never disclosed a major reason for their concerns.

How the Hack Worked, According to U.S. Officials

❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of







❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

Illustrator: Scott Gelber

Back in 2006, three engineers in Oregon had a clever idea. Demand for mobile video was about to explode, and they predicted that broadcasters would be desperate to transform programs designed to fit TV screens into the various formats needed for viewing on smartphones, laptops, and other devices. To meet the anticipated demand, the engineers started Elemental

Elemental then loaded the software onto custom-built servers emblazoned with its leprechaun-green logos.

Elemental servers sold for as much as $100,000 each, at profit margins of as high as 70 percent, according to a former adviser to the company. Two of Elemental's biggest early clients were the Mormon church, which used the technology to beam sermons to congregations around the world, and the adult film industry, which did not.

Elemental also started working with American spy agencies. In 2009 the company announced a development partnership with In-Q-Tel Inc., the CIA's investment arm, a deal that paved the way for Elemental servers to be used in national security missions across the U.S. government. Public documents, including the company's own promotional materials, show that the servers have been used inside Department of Defense data centers to process drone and surveillance-camera footage, on Navy warships to transmit feeds of airborne missions, and inside government buildings to enable secure videoconferencing. NASA, both houses of Congress, and the Department of Homeland Security have also been customers. This portfolio made Elemental a target for foreign adversaries.

Supermicro had been an obvious choice to build Elemental's servers. Headquartered north of San Jose's airport, up a smoggy stretch of Interstate 880, the company was founded by Charles Liang, a Taiwanese engineer who attended graduate school in Texas and then moved west to start Supermicro with his wife in 1993. Silicon Valley was then embracing outsourcing, forging a pathway from Taiwanese, and later Chinese,

Today, Supermicro sells more server motherboards than almost anyone else. It also dominates the $1 billion market for boards used in special-purpose computers, from MRI machines to weapons systems. Its motherboards can be found in made-to-order server setups at banks, hedge funds, cloud computing providers, and web-hosting services, among other places. Supermicro has assembly facilities in California, the Netherlands, and Taiwan, but its motherboards—its core product—are nearly all manufactured by contractors in China.

The company's pitch to customers hinges on unmatched customization, made possible by hundreds of full-time engineers and a catalog encompassing more than 600 designs. The majority of its workforce in San Jose is Taiwanese or Chinese, and Mandarin is the preferred language, with *hanzi* filling the whiteboards, according to six former employees. Chinese pastries are delivered every week, and many routine calls are done twice, once for English-only workers and again in Mandarin. The latter are more productive, according to people who've been on both. These overseas ties, especially the widespread use of Mandarin, would have made it easier for China to gain an understanding of Supermicro's operations and potentially to infiltrate the company. (A U.S. official says the government's probe is still examining whether spies were planted inside Supermicro or other American companies to aid the attack.)

With more than 900 customers in 100 countries by 2015, Supermicro offered inroads to a bountiful collection of sensitive targets. "Think of Supermicro as the Microsoft of the hardware world," says a former U.S.

The security of the global technology supply chain had been compromised, even if consumers and most companies didn't know it yet

Well before evidence of the attack surfaced inside the networks of U.S. companies, American intelligence sources were reporting that China's spies had plans to introduce malicious microchips into the supply chain. The sources weren't specific, according to a person familiar with the information they provided, and millions of motherboards are shipped into the U.S. annually. But in the first half of 2014, a different person briefed on high-level discussions says, intelligence officials went to the White House with something more concrete: China's military was preparing to insert the chips into Supermicro motherboards bound for U.S. companies.

The specificity of the information was remarkable, but so were the challenges it posed. Issuing a broad warning to Supermicro's customers could have crippled the company, a major American hardware maker, and it wasn't clear from the intelligence whom the operation was targeting or what its ultimate aims were. Plus, without confirmation that anyone had been attacked, the FBI was limited in how it could respond. The White

problems, according to a person familiar with the timeline. Two of the senior Apple insiders say the company reported the incident to the FBI but kept details about what it had detected tightly held, even internally. Government investigators were still chasing clues on their own when Amazon made its discovery and gave them access to sabotaged hardware, according to one U.S. official. This created an invaluable opportunity for intelligence agencies and the FBI—by then running a full investigation led by its cyber- and counterintelligence teams—to see what the chips looked like and how they worked.

The chips on Elemental servers were designed to be as inconspicuous as possible, according to one person who saw a detailed report prepared for Amazon by its third-party security contractor, as well as a second person who saw digital photos and X-ray images of the chips incorporated into a later report prepared by Amazon's security team. Gray or off-white in color, they looked more like signal conditioning couplers, another common motherboard component, than microchips, and so they were unlikely to be detectable without specialized equipment. Depending on the board model, the chips varied slightly in size, suggesting that the attackers had supplied different factories with different batches.

Officials familiar with the investigation say the primary role of implants such as these is to open doors that other attackers can go through. "Hardware attacks are about access," as one former senior official puts it. In simplified terms, the implants on Supermicro hardware manipulated the core operating instructions that tell the server what to do as data move

a way that allowed it to effectively edit this information queue, injecting its own code or altering the order of the instructions the CPU was meant to follow. Deviously small changes could create disastrous effects.

Since the implants were small, the amount of code they contained was small as well. But they were capable of doing two very important things: telling the device to communicate with one of several anonymous computers elsewhere on the internet that were loaded with more complex code; and preparing the device's operating system to accept this new code. The illicit chips could do all this because they were connected to the baseboard management controller, a kind of superchip that administrators use to remotely log in to problematic servers, giving them access to the most sensitive code even on machines that have crashed or are turned off.

This system could let the attackers alter how the device functioned, line by line, however they wanted, leaving no one the wiser. To understand the power that would give them, take this hypothetical example: Somewhere in the Linux operating system, which runs in many servers, is code that authorizes a user by verifying a typed password against a stored encrypted one. An implanted chip can alter part of that code so the server won't check for a password—and presto! A secure machine is open to any and all users. A chip can also steal encryption keys for secure communications, block security updates that would neutralize the attack, and open up new pathways to the internet. Should some anomaly be noticed, it would likely be cast as an unexplained oddity. "The hardware opens whatever door it wants," says Joe FitzPatrick, founder of Hardware Security Resources LLC, a

security of the global technology supply chain had been compromised, even if consumers and most companies didn't know it yet. What remained for investigators to learn was how the attackers had so thoroughly infiltrated Supermicro's production process—and how many doors they'd opened into American targets.

Unlike software-based hacks, hardware manipulation creates a real-world trail. Components leave a wake of shipping manifests and invoices. Boards have serial numbers that trace to specific factories. To track the corrupted chips to their source, U.S. intelligence agencies began following Supermicro's serpentine supply chain in reverse, a person briefed on evidence gathered during the probe says.

As recently as 2016, according to *DigiTimes*, a news site specializing in supply chain research, Supermicro had three primary manufacturers constructing its motherboards, two headquartered in Taiwan and one in Shanghai. When such suppliers are choked with big orders, they sometimes parcel out work to subcontractors. In order to get further down the trail, U.S. spy agencies drew on the prodigious tools at their disposal. They sifted through communications intercepts, tapped informants in Taiwan and China, even tracked key individuals through their phones, according to the person briefed on evidence gathered during the probe. Eventually, that person says, they traced the malicious chips to four subcontracting factories that had been building Supermicro motherboards for at least two years.

suggesting a connection to the government. The middlemen would request changes to the motherboards' original designs, initially offering bribes in conjunction with their unusual requests. If that didn't work, they threatened factory managers with inspections that could shut down their plants. Once arrangements were in place, the middlemen would organize delivery of the chips to the factories.

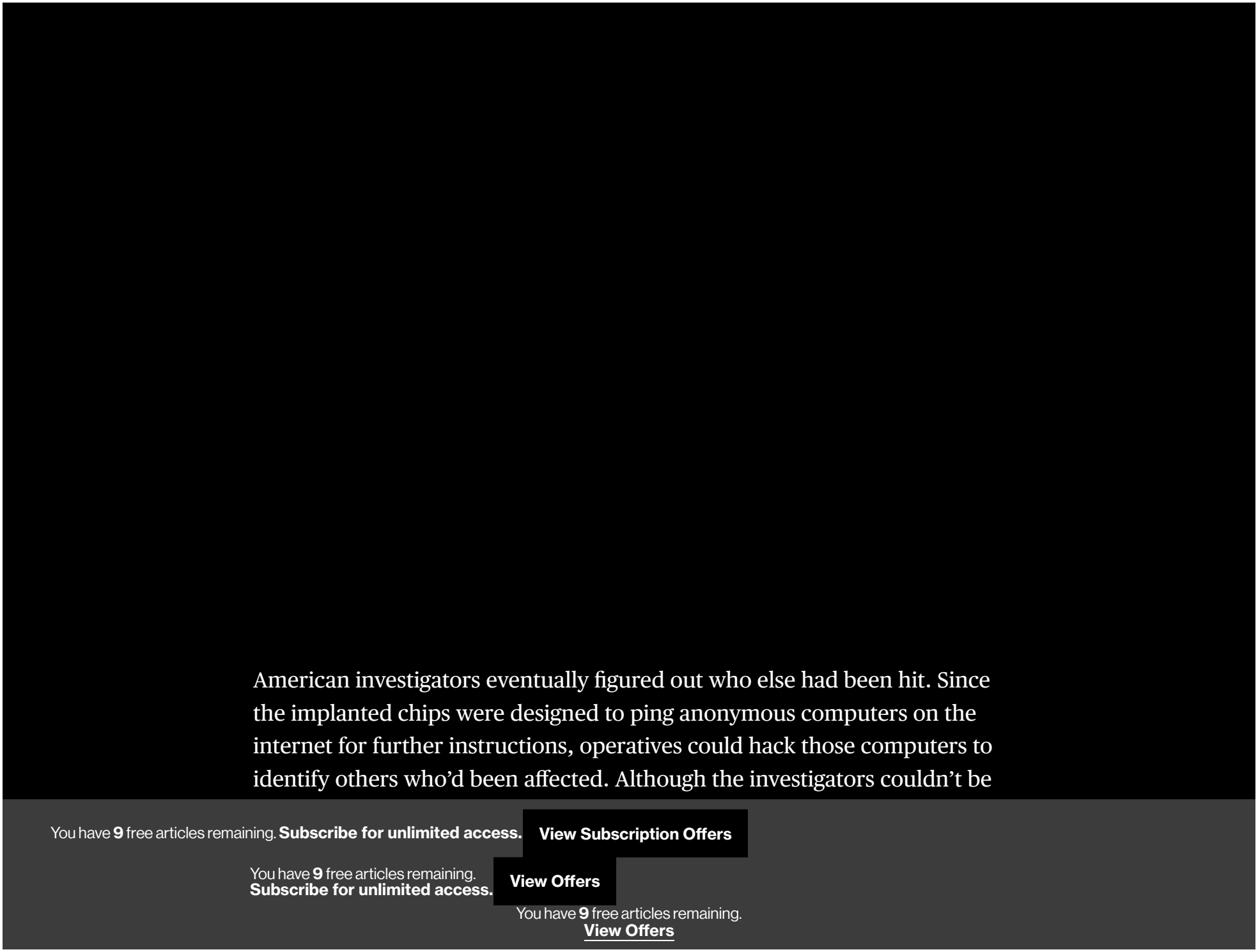
The investigators concluded that this intricate scheme was the work of a People's Liberation Army unit specializing in hardware attacks, according to two people briefed on its activities. The existence of this group has never been revealed before, but one official says, "We've been tracking these guys for longer than we'd like to admit." The unit is believed to focus on high-priority targets, including advanced commercial technology and the computers of rival militaries. In past attacks, it targeted the designs for high-performance computer chips and computing systems of large U.S. internet providers.

Provided details of *Businessweek*'s reporting, China's Ministry of Foreign Affairs sent a statement that said "China is a resolute defender of cybersecurity." The ministry added that in 2011, China proposed international guarantees on hardware security along with other members of the Shanghai Cooperation Organization, a regional security body. The statement concluded, "We hope parties make less gratuitous accusations and suspicions but conduct more constructive talk and collaboration so that we can work together in building a peaceful, safe, open, cooperative and orderly cyberspace."

relationship intensified after 2013, when Apple acquired a startup called Topsy Labs, which created superfast technology for indexing and searching vast troves of internet content. By 2014, the startup was put to work building small data centers in or near major global cities. This project, known internally as Ledbelly, was designed to make the search function for Apple's voice assistant, Siri, faster, according to the three senior Apple insiders.

Documents seen by *Businessweek* show that in 2014, Apple planned to order more than 6,000 Supermicro servers for installation in 17 locations, including Amsterdam, Chicago, Hong Kong, Los Angeles, New York, San Jose, Singapore, and Tokyo, plus 4,000 servers for its existing North Carolina and Oregon data centers. Those orders were supposed to double, to 20,000, by 2015. Ledbelly made Apple an important Supermicro customer at the exact same time the PLA was found to be manipulating the vendor's hardware.

Project delays and early performance problems meant that around 7,000 Supermicro servers were humming in Apple's network by the time the company's security team found the added chips. Because Apple didn't, according to a U.S. official, provide government investigators with access to its facilities or the tampered hardware, the extent of the attack there remained outside their view.



American investigators eventually figured out who else had been hit. Since the implanted chips were designed to ping anonymous computers on the internet for further instructions, operatives could hack those computers to identify others who'd been affected. Although the investigators couldn't be

giants, Huawei Corp. and ZTE Corp., was subject to Chinese government manipulation. (Both Huawei and ZTE have said no such tampering has occurred.) But a similar public alert regarding a U.S. company was out of the question. Instead, officials reached out to a small number of important Supermicro customers. One executive of a large web-hosting company says the message he took away from the exchange was clear: Supermicro's hardware couldn't be trusted. "That's been the nudge to everyone—get that crap out," the person says.

Amazon, for its part, began acquisition talks with an Elemental competitor, but according to one person familiar with Amazon's deliberations, it reversed course in the summer of 2015 after learning that Elemental's board was nearing a deal with another buyer. Amazon announced its acquisition of Elemental in September 2015, in a transaction whose value one person familiar with the deal places at $350 million. Multiple sources say that Amazon intended to move Elemental's software to AWS's cloud, whose chips, motherboards, and servers are typically designed in-house and built by factories that Amazon contracts from directly.

A notable exception was AWS's data centers inside China, which were filled with Supermicro-built servers, according to two people with knowledge of AWS's operations there. Mindful of the Elemental findings, Amazon's security team conducted its own investigation into AWS's Beijing facilities and found altered motherboards there as well, including more sophisticated designs than they'd previously encountered. In one case, the

denies that AWS knew of servers found in China containing malicious chips.)

China has long been known to monitor banks, manufacturers, and ordinary citizens on its own soil, and the main customers of AWS's China cloud were domestic companies or foreign entities with operations there. Still, the fact that the country appeared to be conducting those operations inside Amazon's cloud presented the company with a Gordian knot. Its security team determined that it would be difficult to quietly remove the equipment and that, even if they could devise a way, doing so would alert the attackers that the chips had been found, according to a person familiar with the company's probe. Instead, the team developed a method of monitoring the chips. In the ensuing months, they detected brief check-in communications between the attackers and the sabotaged servers but didn't see any attempts to remove data. That likely meant either that the attackers were saving the chips for a later operation or that they'd infiltrated other parts of the network before the monitoring began. Neither possibility was reassuring.

When in 2016 the Chinese government was about to pass a new cybersecurity law—seen by many outside the country as a pretext to give authorities wider access to sensitive data—Amazon decided to act, the person familiar with the company's probe says. In August it transferred operational control of its Beijing data center to its local partner, Beijing Sinnet, a move the companies said was needed to comply with the incoming law. The following November, Amazon sold the entire

As for Apple, one of the three senior insiders says that in the summer of 2015, a few weeks after it identified the malicious chips, the company started removing all Supermicro servers from its data centers, a process Apple referred to internally as "going to zero." Every Supermicro server, all 7,000 or so, was replaced in a matter of weeks, the senior insider says. (Apple denies that any servers were removed.) In 2016, Apple informed Supermicro that it was severing their relationship entirely—a decision a spokesman for Apple ascribed in response to *Businessweek*'s questions to an unrelated and relatively minor security incident.

That August, Supermicro's CEO, Liang, revealed that the company had lost two major customers. Although he didn't name them, one was later identified in news reports as Apple. He blamed competition, but his explanation was vague. "When customers asked for lower price, our people did not respond quickly enough," he said on a conference call with analysts. Hayes, the Supermicro spokesman, says the company has never been notified of the existence of malicious chips on its motherboards by either customers or U.S. law enforcement.

Concurrent with the illicit chips' discovery in 2015 and the unfolding investigation, Supermicro has been plagued by an accounting problem, which the company characterizes as an issue related to the timing of certain revenue recognition. After missing two deadlines to file quarterly and annual reports required by regulators, Supermicro was delisted from the Nasdaq on Aug. 23 of this year. It marked an extraordinary stumble for a company whose annual revenue had risen sharply in the previous four

One Friday in late September 2015, President Barack Obama and Chinese President Xi Jinping appeared together at the White House for an hourlong press conference headlined by a landmark deal on cybersecurity. After months of negotiations, the U.S. had extracted from China a grand promise: It would no longer support the theft by hackers of U.S. intellectual property to benefit Chinese companies. Left out of those pronouncements, according to a person familiar with discussions among senior officials across the U.S. government, was the White House's deep concern that China was willing to offer this concession because it was already developing far more advanced and surreptitious forms of hacking founded on its near monopoly of the technology supply chain.

In the weeks after the agreement was announced, the U.S. government quietly raised the alarm with several dozen tech executives and investors at a small, invite-only meeting in McLean, Va., organized by the Pentagon. According to someone who was present, Defense Department officials briefed the technologists on a recent attack and asked them to think about creating commercial products that could detect hardware implants. Attendees weren't told the name of the hardware maker involved, but it was clear to at least some in the room that it was Supermicro, the person says.

The problem under discussion wasn't just technological. It spoke to decisions made decades ago to send advanced production work to Southeast Asia. In the intervening years, low-cost Chinese manufacturing had come to underpin the business models of many of America's largest

Over the decades, the security of the supply chain became an article of faith despite repeated warnings by Western officials. A belief formed that China was unlikely to jeopardize its position as workshop to the world by letting its spies meddle in its factories. That left the decision about where to build commercial systems resting largely on where capacity was greatest and cheapest. "You end up with a classic Satan's bargain," one former U.S. official says. "You can have less supply than you want and guarantee it's secure, or you can have the supply you need, but there will be risk. Every organization has accepted the second proposition."

In the three years since the briefing in McLean, no commercially viable way to detect attacks like the one on Supermicro's motherboards has emerged—or has looked likely to emerge. Few companies have the resources of Apple and Amazon, and it took some luck even for them to spot the problem. "This stuff is at the cutting edge of the cutting edge, and there is no easy technological solution," one of the people present in McLean says. "You have to invest in things that the world wants. You cannot invest in things that the world is not ready to accept yet."

Bloomberg LP has been a Supermicro customer. According to a Bloomberg LP spokesperson, the company has found no evidence to suggest that it has been affected by the hardware issues raised in the article.

109 S.Ct. 693, 102 L.Ed.2d 835, 57 USLW 4126

109 S.Ct. 693
Supreme Court of the United States

FLORIDA, Petitioner,
v.
Michael A. **RILEY**.

No. 87–764.
|
Argued Oct. 3, 1988.
|
Decided Jan. 23, **1989**.
|
Rehearing Denied April 3, **1989**.
|
See 490 U.S. 1014, **109 S.Ct**. 1659.

Synopsis

Defendant moved to suppress marijuana plants seized pursuant to execution of search warrant, which was based on aerial observations by police officer in helicopter 400 feet above defendant's greenhouse. The Circuit Court, Pasco County, W. Lowell Bray, Jr., J., granted motion to suppress, and State appealed. The District Court of Appeal, 476 So.2d 1354, reversed, and defendant appealed. The **Florida** Supreme Court, 511 So.2d 282, reversed and remanded, and State's petition for certiorari was granted. The Supreme Court, Justice White, held that officer's observation, with his naked eye, of interior of partially covered greenhouse in residential backyard from vantage point of helicopter circling 400 feet above did not constitute a "search" for which a warrant was required.

Reversed.

Justice O'Connor concurred in the judgment and filed an opinion.

Justice Brennan filed a dissenting opinion in which Justices Marshall and Stevens joined.

Justice Blackmun filed a dissenting opinion.

****694** Opinion on remand, 549 So.2d 673.

West Headnotes (1)

[1] **Searches and Seizures**
Aerial surveillance

Officer's observation, with his naked eye, of interior of partially covered greenhouse in residential backyard from vantage point of helicopter circling 400 feet above did not constitute a "search" for which a warrant was required. (Per Justice White with the Chief Justice and two Justices concurring, and one Justice concurring in the judgment.) U.S.C.A. Const.Amend. 4.

215 Cases that cite this headnote

Syllabus *

***445** A **Florida** county sheriff's office received an anonymous tip that marijuana was being grown on respondent's property. When an investigating officer discovered that he could not observe from ground level the contents of a greenhouse on the property—which was enclosed on two sides and obscured from view on the other, open sides by trees, shrubs, and respondent's nearby home—he circled twice over the property in a helicopter at the height of 400 feet and made naked-eye observations through openings in the greenhouse roof and its open sides of what he concluded were marijuana plants. After a search pursuant to a warrant obtained on the basis of these observations revealed marijuana growing in the greenhouse, respondent was charged with possession of that substance under **Florida** law. The trial court granted his motion to suppress the evidence. Although reversing, the State Court of Appeals certified the case to the State Supreme Court on the question whether the helicopter surveillance from 400 feet constituted a "search" for which a warrant was required under the Fourth Amendment. Answering that question in the affirmative, the court

quashed the Court of Appeals' decision and reinstated the trial court's suppression order.

Held: The judgment is reversed.

511 So.2d 282, (Fla.1987) reversed.

Justice WHITE, joined by THE CHIEF JUSTICE, Justice SCALIA, and Justice KENNEDY, concluded that the Fourth Amendment does not require the police traveling in the public airways at an altitude of 400 feet to obtain a warrant in order to observe what is visible to the naked eye. *California v. Ciraolo,* 476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210—which held that a naked-eye police inspection of the backyard of a house from a fixed-wing aircraft at 1,000 feet was not a "search"—is controlling. Thus, respondent could not reasonably have expected that the contents of his greenhouse were protected from public or official inspection from the air, since he left the greenhouse's sides and roof partially open. The fact that the inspection was made from a helicopter is irrelevant, since, as in the case of fixed-wing planes, private and commercial flight by helicopter is routine. Nor, on the facts of this case, does it make a difference for Fourth Amendment purposes that the helicopter was flying below 500 feet, the Federal Aviation Administration's lower limit upon the navigable airspace for fixed-wing craft. Since the FAA permits helicopters to fly ***446** below that limit, the helicopter here was not violating the law, and any member of the public or the police could legally have observed respondent's greenhouse from that altitude. Although an aerial ****695** inspection of a house's curtilage may not always pass muster under the Fourth Amendment simply because the aircraft is within the navigable airspace specified by law, there is nothing in the record here to suggest that helicopters flying at 400 feet are sufficiently rare that respondent could have reasonably anticipated that his greenhouse would not be observed from that altitude. Moreover, there is no evidence that the helicopter interfered with respondent's normal use of his greenhouse or other parts of the curtilage, that intimate details connected with the use of the home or curtilage, were observed, or that there was undue noise, wind, dust, or threat of injury. Pp. 696–697.

Justice O'CONNOR concluded that the plurality's approach rests the scope of Fourth Amendment protection too heavily on compliance with FAA regulations, which are intended to promote air safety and not to protect the right to be secure against unreasonable searches and seizures. Whether respondent had a reasonable expectation of privacy from aerial observation of his curtilage does not depend on whether the helicopter was where it had a right to be, but, rather, on whether it was in the public airways at an altitude at which members of the public travel with sufficient regularity that respondent's expectation was not one that society is prepared to recognize as "reasonable." Because there is reason to believe that there is considerable public use of airspace at altitudes of 400 feet and above, and because respondent introduced no evidence to the contrary before the state courts, it must be concluded that his expectation of privacy here was not reasonable. However, public use of altitudes lower than 400 feet—particularly public observations from helicopters circling over the curtilage of a home—may be sufficiently rare that police surveillance from such altitudes would violate reasonable expectations of privacy, despite compliance with FAA regulations. Pp. 698–699.

WHITE, J., announced the judgment of the Court and delivered an opinion in which REHNQUIST, C.J., and SCALIA and KENNEDY, JJ., joined. O'CONNOR, J., filed an opinion concurring in the judgment, *post,* p. 698. BRENNAN, J., filed a dissenting opinion, in which MARSHALL and STEVENS, JJ., joined, *post,* p. 699. BLACKMUN, J., filed a dissenting opinion, *post,* p. 705.

Attorneys and Law Firms

Parker D. Thomson, Special Assistant Attorney General of Florida, argued the cause for petitioner. With him on the briefs were *Robert A. Butterworth,* Attorney General, ***447** *Candace M. Sunderland,* and *Peggy A. Quince,* Assistant Attorneys General, and *Cloyce L. Mangas, Jr.,* Special Assistant Attorney General.

Marc H. Salton argued the cause and filed a brief for respondent.*

* Briefs of *amici curiae* urging reversal were filed for the State of Indiana et al. by *Linley E. Pearson,* Attorney General of Indiana, and *Lisa M. Paunicka,* Deputy Attorney General, *Don Siegelman,* Attorney General of

Alabama, *Robert K. Corbin,* Attorney General of Arizona, *John Steven Clark,* Attorney General of Arkansas, *John J. Kelly,* Chief State's Attorney of Connecticut, *Charles M. Oberly,* Attorney General of Delaware, *Warren Price III,* Attorney General of Hawaii, *Jim Jones,* Attorney General of Idaho, *Neil F. Hartigan,* Attorney General of Illinois, *Robert T. Stephan,* Attorney General of Kansas, *Frederic J. Cowan,* Attorney General of Kentucky, *Frank J. Kelley,* Attorney General of Michigan, *Hubert H. Humphrey III,* Attorney General of Minnesota, *William L. Webster,* Attorney General of Missouri, *Robert M. Spire,* Attorney General of Nebraska, *Lacy H. Thornburg,* Attorney General of North Carolina, *Anthony J. Celebrezze, Jr.,* Attorney General of Ohio, *Dave Frohnmayer,* Attorney General of Oregon, *Travis Medlock,* Attorney General of South Carolina, *Roger A. Tellinghuisen,* Attorney General of South Dakota, *David L. Wilkinson,* Attorney General of Utah, *Jeffrey Amestoy,* Attorney General of Vermont, *Don Hanaway,* Attorney General of Wisconsin, and *Joseph B. Meyer,* Attorney General of Wyoming; and for the Airborne Law Enforcement Association, Inc., by *Ellen M. Condon* and *Paul J. Marino.*

Briefs of *amici curiae* urging affirmance were filed for the American Civil Liberties Union et al. by *Kent L. Richland, Pamela Victorine, John A. Powell, Steve R. Shapiro, Paul Hoffman, Joan W. Howarth,* and *James K. Green;* for Community Outreach to Vietnam Era Returnees, Inc., by *Deborah C. Wyatt;* and for the National Association of Criminal Defense Lawyers by *Milton Hirsch.*

Ronald M. Sinoway filed a brief for the California Attorneys for Criminal Justice et al. as *amici curiae.*

Opinion

Justice WHITE announced the judgment of the Court and delivered an opinion, in which THE CHIEF JUSTICE, Justice SCALIA, and Justice KENNEDY join.

On certification to it by a lower state court, the **Florida** Supreme Court addressed the following question: "Whether surveillance of the interior of a partially covered greenhouse ***448** in a residential backyard from the vantage point of a helicopter located 400 feet above the greenhouse constitutes a 'search' for which a warrant is required under the Fourth Amendment and Article I, § 12 of the **Florida** Constitution." 511 So.2d 282 (1987). The court answered the question in the affirmative, and we granted the State's petition for certiorari challenging that conclusion. 484 U.S. 1058, 108 **S.Ct**. 1011, 98 L.Ed.2d 977 (1988). [1]

Respondent **Riley** lived in a mobile home located on five acres of rural property. A ****696** greenhouse was located 10 to 20 feet behind the mobile home. Two sides of the greenhouse were enclosed. The other two sides were not enclosed but the contents of the greenhouse were obscured from view from surrounding property by trees, shrubs, and the mobile home. The greenhouse was covered by corrugated roofing panels, some translucent and some opaque. At the time relevant to this case, two of the panels, amounting to approximately 10% of the roof area, were missing. A wire fence surrounded the mobile home and the greenhouse, and the property was posted with a "DO NOT ENTER" sign.

This case originated with an anonymous tip to the Pasco County Sheriff's office that marijuana was being grown on respondent's property. When an investigating officer discovered that he could not see the contents of the greenhouse from the road, he circled twice over respondent's property in a helicopter at the height of 400 feet. With his naked eye, he was able to see through the openings in the roof and one or more of the open sides of the greenhouse and to identify what he thought was marijuana growing in the structure. A warrant ***449** was obtained based on these observations, and the ensuing search revealed marijuana growing in the greenhouse. Respondent was charged with possession of marijuana under **Florida** law. The trial court granted his motion to suppress; the **Florida** Court of Appeals reversed but certified the case to the **Florida** Supreme Court, which quashed the decision of the Court of Appeals and reinstated the trial court's suppression order.

We agree with the State's submission that our decision in *California v. Ciraolo,* 476 U.S. 207, 106 **S.Ct**. 1809, 90 L.Ed.2d 210 (1986), controls this case. There, acting on a tip, the police inspected the back-yard of a particular house while flying in a fixed-wing aircraft at 1,000 feet. With the naked eye the officers saw what they concluded was marijuana growing in the yard. A search warrant was obtained on the strength of this airborne inspection, and

marijuana plants were found. The trial court refused to suppress this evidence, but a state appellate court held that the inspection violated the Fourth and Fourteenth Amendments to the United States Constitution, and that the warrant was therefore invalid. We in turn reversed, holding that the inspection was not a search subject to the Fourth Amendment. We recognized that the yard was within the curtilage of the house, that a fence shielded the yard from observation from the street, and that the occupant had a subjective expectation of privacy. We held, however, that such an expectation was not reasonable and not one "that society is prepared to honor." *Id.,* at 214, 106 S.Ct., at 1813. Our reasoning was that the home and its curtilage are not necessarily protected from inspection that involves no physical invasion. " 'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.' " *Id.,* at 213, 106 S.Ct., at 1812, quoting *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 511, 19 L.Ed.2d 576 (1967). As a general proposition, the police may see what may be seen "from a public vantage point where [they have] a right to be," 476 U.S., at 213, 106 S.Ct., at 1812. Thus the police, like the public, would have been free to inspect the backyard garden from ***450** the street if their view had been unobstructed. They were likewise free to inspect the yard from the vantage point of an aircraft flying in the navigable airspace as this plane was. "In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet. The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye." *Id.,* at 215, 106 S.Ct., at 1813–1814.

We arrive at the same conclusion in the present case. In this case, as in *Ciraolo,* ****697** the property surveyed was within the curtilage of respondent's home. Riley no doubt intended and expected that his greenhouse would not be open to public inspection, and the precautions he took protected against ground-level observation. Because the sides and roof of his greenhouse were left partially open, however, what was growing in the greenhouse was subject to viewing from the air. Under the holding in *Ciraolo,* Riley could not reasonably have expected the contents of his greenhouse to be immune from examination by an officer seated in a fixed-wing aircraft flying in navigable airspace at an altitude of 1,000 feet or, as the Florida Supreme Court seemed to recognize, at an altitude of 500 feet, the lower limit of the navigable airspace for such an aircraft. 511 So.2d, at 288. Here, the inspection was made from a helicopter, but as is the case with fixed-wing planes, "private and commercial flight [by helicopter] in the public airways is routine" in this country, *Ciraolo, supra,* 476 U.S., at 215, 106 S.Ct., at 1813, and there is no indication that such flights are unheard of in Pasco County, Florida.[2] Riley could not reasonably ***451** have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing aircraft.

Nor on the facts before us, does it make a difference for Fourth Amendment purposes that the helicopter was flying at 400 feet when the officer saw what was growing in the greenhouse through the partially open roof and sides of the structure. We would have a different case if flying at that altitude had been contrary to law or regulation. But helicopters are not bound by the lower limits of the navigable airspace allowed to other aircraft.[3] Any member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse. The police officer did no more. This is not to say that an inspection of the curtilage of a house from an aircraft will always pass muster under the Fourth Amendment simply because the plane is within the navigable airspace specified by law. But it is of obvious importance that the helicopter in this case was *not* violating the law, and there is nothing in the record or before us to suggest that helicopters flying at 400 feet are sufficiently rare in this country to lend substance to respondent's claim that he reasonably anticipated that his greenhouse would not be subject to ***452** observation from that altitude. Neither is there any intimation here that the helicopter interfered with respondent's normal use of the greenhouse or of other parts of the curtilage. As far as this record reveals, no intimate details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury. In these circumstances, there was no violation of the Fourth Amendment.

The judgment of the Florida Supreme Court is accordingly reversed.

So ordered.

****698** Justice O'CONNOR, concurring in the judgment. I concur in the judgment reversing the Supreme Court of Florida because I agree that police observation of the greenhouse in Riley's curtilage from a helicopter passing at an altitude of 400 feet did not violate an expectation of privacy "that society is prepared to recognize as 'reasonable.' " *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 517, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). I write separately, however, to clarify the standard I believe follows from *California v. Ciraolo,* 476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986). In my view, the plurality's approach rests the scope of Fourth Amendment protection too heavily on compliance with FAA regulations whose purpose is to promote air safety, not to protect "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., Amdt. 4.

Ciraolo involved observation of curtilage by officers flying in an airplane at an altitude of 1,000 feet. In evaluating whether this observation constituted a search for which a warrant was required, we acknowledged the importance of curtilage in Fourth Amendment doctrine: "The protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened." 476 U.S., at 212–213, 106 S.Ct., at 1812. Although the curtilage is an area to which the private activities ***453** of the home extend, all police observation of the curtilage is not necessarily barred by the Fourth Amendment. As we observed: "The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." *Id.,* at 213, 106 S.Ct., at 1812. In *Ciraolo,* we likened observation from a plane traveling in "public navigable airspace" at 1,000 feet to observation by police "passing by a home on public thoroughfares." We held that "[i]n an age where private and commercial flight in the public airways is routine," it is unreasonable to expect the curtilage to be constitutionally protected from aerial observation with the naked eye from an altitude of 1,000 feet. *Id.,* at 215, 106 S.Ct., at 1813.

Ciraolo's expectation of privacy was unreasonable not because the airplane was operating where it had a "right to be," but because public air travel at 1,000 feet is a sufficiently routine part of modern life that it is unreasonable for persons on the ground to expect that their curtilage will not be observed from the air at that altitude. Although "helicopters are not bound by the lower limits of the navigable airspace allowed to other aircraft," *ante,* at 699, there is no reason to assume that compliance with FAA regulations alone determines " 'whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment.' " *Ciraolo, supra,* at 212, 106 S.Ct., at 1812 (quoting *Oliver v. United States,* 466 U.S. 170, 182–183, 104 S.Ct.1735, 1743, 80 L.Ed.2d 214 (1984)). Because the FAA has decided that helicopters can lawfully operate at virtually any altitude so long as they pose no safety hazard, it does not follow that the expectations of privacy "society is prepared to recognize as 'reasonable' " simply mirror the FAA's safety concerns.

Observations of curtilage from helicopters at very low altitudes are not perfectly analogous to ground-level observations from public roads or sidewalks. While in both cases the police may have a legal right to occupy the physical space from which their observations are made, the two situations ***454** are not necessarily comparable in terms of whether expectations of privacy from such vantage points should be considered reasonable. Public roads, even those less traveled by, are clearly demarked public thoroughfares. Individuals who seek privacy can take precautions, tailored to the location of the road, to avoid ****699** disclosing private activities to those who pass by. They can build a tall fence, for example, and thus ensure private enjoyment of the curtilage without risking public observation from the road or sidewalk. If they do not take such precautions, they cannot reasonably expect privacy from public observation. In contrast, even individuals who have taken effective precautions to ensure against ground-level observations cannot block off all conceivable aerial views of their outdoor patios and yards without entirely giving up their enjoyment of those areas. To require individuals to completely cover and enclose their curtilage is to demand more than the

"precautions customarily taken by those seeking privacy." *Rakas v. Illinois,* 439 U.S. 128, 152, 99 S.Ct. 421, 435, 58 L.Ed.2d 387 (1978) (Powell, J., concurring). The fact that a helicopter could conceivably observe the curtilage at virtually any altitude or angle, without violating FAA regulations, does not in itself mean that an individual has no reasonable expectation of privacy from such observation.

In determining whether Riley had a reasonable expectation of privacy from aerial observation, the relevant inquiry after *Ciraolo* is not whether the helicopter was where it had a right to be under FAA regulations. Rather, consistent with *Katz,* we must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not "one that society is prepared to recognize as 'reasonable.' " *Katz, supra,* 389 U.S., at 361, 88 S.Ct., at 516. Thus, in determining " 'whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment,' " *Ciraolo, supra,* 476 U.S., at 212, 106 S.Ct., at 1812 (quoting *Oliver, supra,* 466 U.S., at 182–183, 104 S.Ct., at 1743), it is not conclusive to observe, ***455** as the plurality does, that "[a]ny member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse." *Ante,* at 696–698. Nor is it conclusive that police helicopters may often fly at 400 feet. If the public rarely, if ever, travels overhead at such altitudes, the observation cannot be said to be from a vantage point generally used by the public and Riley cannot be said to have "knowingly expose[d]" his greenhouse to public view. However, if the public can generally be expected to travel over residential backyards at an altitude of 400 feet, Riley cannot reasonably expect his curtilage to be free from such aerial observation.

In my view, the defendant must bear the burden of proving that his expectation of privacy was a reasonable one, and thus that a "search" within the meaning of the Fourth Amendment even took place. Cf. *Jones v. United States,* 362 U.S. 257, 261, 80 S.Ct. 725, 731, 4 L.Ed.2d 697 (1960) ("Ordinarily, then, it is entirely proper to require of one who seeks to challenge the legality of a search as the basis for suppressing relevant evidence that he allege, and if the allegation be disputed that he establish, that he himself was the victim of an invasion of privacy"); *Nardone v. United States,* 308 U.S. 338, 341, 60 S.Ct. 266, 267–268, 84 L.Ed. 307 (1939).

Because there is reason to believe that there is considerable public use of airspace at altitudes of 400 feet and above, and because Riley introduced no evidence to the contrary before the Florida courts, I conclude that Riley's expectation that his curtilage was protected from naked-eye aerial observation from that altitude was not a reasonable one. However, public use of altitudes lower than that—particularly public observations from helicopters circling over the curtilage of a home—may be sufficiently rare that police surveillance from such altitudes would violate reasonable expectations of privacy, despite compliance with FAA air safety regulations.

***456** Justice BRENNAN, with whom Justice MARSHALL and Justice STEVENS, join, dissenting.

The Court holds today that police officers need not obtain a warrant based on ****700** probable cause before circling in a helicopter 400 feet above a home in order to investigate what is taking place behind the walls of the curtilage. I cannot agree that the Fourth Amendment to the Constitution, which safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," tolerates such an intrusion on privacy and personal security.

I

The opinion for a plurality of the Court reads almost as if *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), had never been decided. Notwithstanding the disclaimers of its final paragraph, the opinion relies almost exclusively on the fact that the police officer conducted his surveillance from a vantage point where, under applicable Federal Aviation Administration regulations, he had a legal right to be. *Katz* teaches, however, that the relevant inquiry is whether the police surveillance "violated the privacy upon which [the defendant] justifiably relied," *id.,* at 353, 88 S.Ct.,

at 512—or, as Justice Harlan put it, whether the police violated an "expectation of privacy ... that society is prepared to recognize as 'reasonable.' " *Id.,* at 361, 88 S.Ct., at 516 (concurring opinion). The result of that inquiry in any given case depends ultimately on the judgment "whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society." Amsterdam, Perspectives on the Fourth Amendment, 58 Minn.L.Rev. 349, 403 (1974); see also 1 W. LaFave, Search and Seizure § 2.1(d), pp. 310–314 (2d ed.1987).

The plurality undertakes no inquiry into whether low-level helicopter surveillance by the police of activities in an enclosed ***457** backyard is consistent with the "aims of a free and open society." Instead, it summarily concludes that Riley's expectation of privacy was unreasonable because "[a]ny member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse." *Ante,* at 696–698. This observation is, in turn, based solely on the fact that the police helicopter was within the airspace within which such craft are allowed by federal safety regulations to fly.

I agree, of course, that "[w]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection." *Katz, supra,* at 351, 88 S.Ct., at 511. But I cannot agree that one "knowingly exposes [an area] to the public" solely because a helicopter may legally fly above it. Under the plurality's exceedingly grudging Fourth Amendment theory, the expectation of privacy is defeated if a single member of the public could conceivably position herself to see into the area in question without doing anything illegal. It is defeated whatever the difficulty a person would have in so positioning herself, and however infrequently anyone would in fact do so. In taking this view the plurality ignores the very essence of *Katz.* The reason why there is no reasonable expectation of privacy in an area that is exposed to the public is that little diminution in "the amount of privacy and freedom remaining to citizens" will result from police surveillance of something that any passerby readily sees. To pretend, as the plurality opinion does, that the same is true when the police use a helicopter to peer over high fences is, at best, disingenuous. Notwithstanding the plurality's statistics about the number of helicopters registered in this country, can it seriously be questioned that Riley enjoyed virtually complete privacy in his backyard greenhouse, and that that privacy was invaded solely by police helicopter surveillance? Is the theoretical possibility that any member of the public (with sufficient means) could also have hired a helicopter and looked over Riley's fence of any relevance at all in determining ***458** whether Riley suffered a serious loss of ****701** privacy and personal security through the police action?

In *California v. Ciraolo,* 476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986), we held that whatever might be observed from the window of an airplane flying at 1,000 feet could be deemed unprotected by any reasonable expectation of privacy. That decision was based on the belief that airplane traffic at that altitude was sufficiently common that no expectation of privacy could inure in anything on the ground observable with the naked eye from so high. Indeed, we compared those airways to "public thoroughfares," and made the obvious point that police officers passing by a home on such thoroughfares were not required by the Fourth Amendment to "shield their eyes." *Id.,* at 213, 106 S.Ct., at 1812. Seizing on a reference in *Ciraolo* to the fact that the police officer was in a position "where he ha[d] a right to be," *ibid.,* today's plurality professes to find this case indistinguishable because FAA regulations do not impose a minimum altitude requirement on helicopter traffic; thus, the officer in this case too made his observations from a vantage point where he had a right to be. [1]

It is a curious notion that the reach of the Fourth Amendment can be so largely defined by administrative regulations issued for purposes of flight safety. [2] It is more curious still ***459** that the plurality relies to such an extent on the legality of the officer's act, when we have consistently refused to equate police violation of the law with infringement of the Fourth Amendment. [3] But the plurality's willingness to end its inquiry when it finds that the officer was in a position he had a right to be in is misguided for an even more ****702** fundamental reason. Finding determinative the fact that the officer was where he had a right to be is, at bottom, an attempt to analogize

surveillance from a helicopter to surveillance by a police officer standing on a public road and viewing evidence of crime through an open window or a gap in a fence. In such a situation, the occupant of the home may be said to lack any ***460** reasonable expectation of privacy in what can be seen from that road—even if, in fact, people rarely pass that way.

The police officer positioned 400 feet above **Riley's** backyard was not, however, standing on a public road. The vantage point he enjoyed was not one any citizen could readily share. His ability to see over **Riley's** fence depended on his use of a very expensive and sophisticated piece of machinery to which few ordinary citizens have access. In such circumstances it makes no more sense to rely on the legality of the officer's position in the skies than it would to judge the constitutionality of the wiretap in *Katz* by the legality of the officer's position outside the telephone booth. The simple inquiry whether the police officer had the legal right to be in the position from which he made his observations cannot suffice, for we cannot assume that **Riley's** curtilage was so open to the observations of passersby in the skies that he retained little privacy or personal security to be lost to police surveillance. The question before us must be not whether the police were where they had a right to be, but whether public observation of **Riley's** curtilage was so commonplace that **Riley's** expectation of privacy in his backyard could not be considered reasonable. To say that an invasion of **Riley's** privacy from the skies was not impossible is most emphatically not the same as saying that his expectation of privacy within his enclosed curtilage was not "one that society is prepared to recognize as 'reasonable.' " *Katz,* 389 U.S., at 361, 88 **S.Ct**., at 517 (Harlan, J., concurring).[4] While, as we held in *Ciraolo,* air traffic at elevations of 1,000 feet or more may be so common that whatever could be seen with the naked eye from that elevation is unprotected by the Fourth Amendment, it is a large step from there to say that the Amendment offers no protection against low-level helicopter surveillance of enclosed curtilage ***461** areas. To take this step is error enough. That the plurality does so with little analysis beyond its determination that the police complied with FAA regulations is particularly unfortunate.

II

Equally disconcerting is the lack of any meaningful limit to the plurality's holding. It is worth reiterating that the FAA regulations the plurality relies on as establishing that the officer was where he had a right to be set no minimum flight altitude for helicopters. It is difficult, therefore, to see what, if any, helicopter surveillance would run afoul of the plurality's rule that there exists no reasonable expectation of privacy as long as the helicopter is where it has a right to be.

Only in its final paragraph does the plurality opinion suggest that there might be some limits to police helicopter surveillance beyond those imposed by FAA regulations:

> "Neither is there any intimation here that the helicopter interfered with respondent's normal use of the greenhouse or of other parts of the curtilage. As far as this record reveals, no intimate details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury. In these circumstances, there was no violation of the Fourth Amendment." *Ante,* at 697.[5]

****703** I will deal with the "intimate details" below. For the rest, one wonders what the plurality believes the purpose of the Fourth Amendment to be. If through noise, wind, dust, and threat of injury from helicopters the State "interfered with respondent's normal use of the greenhouse or of other parts ***462** of the curtilage," **Riley** might have a cause of action in inverse condemnation, but that is not what the Fourth Amendment is all about. Nowhere is this better stated than in Justice WHITE's opinion for the Court in *Camara v. Municipal Court,* 387 U.S. 523, 528, 87 **S.Ct**. 1727, 1730–1731, 18 L.Ed.2d 930 (1967): "The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." See also *Marshall v. Barlow's, Inc.,* 436 U.S. 307, 312, 98 **S.Ct**. 1816, 1820, 56 L.Ed.2d 305 (1978) (same); *Schmerber v. California,* 384 U.S. 757, 767, 86 **S.Ct**. 1826, 1833–1834, 16 L.Ed.2d 908 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and

dignity against unwarranted intrusion by the State"); *Wolf v. Colorado,* 338 U.S. 25, 27, 69 S.Ct. 1359, 1361, 93 L.Ed. 1782 (1949) ("The security of one's privacy against arbitrary intrusion by the police ... is at the core of the Fourth Amendment ..."), overruled on other grounds, *Mapp v. Ohio,* 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961); *Boyd v. United States,* 116 U.S. 616, 630, 6 S.Ct. 524, 532, 29 L.Ed. 746 (1886) ("It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security ...").

If indeed the purpose of the restraints imposed by the Fourth Amendment is to "safeguard the privacy and security of individuals," then it is puzzling why it should be the helicopter's noise, wind, and dust that provides the measure of whether this constitutional safeguard has been infringed. Imagine a helicopter capable of hovering just above an enclosed courtyard or patio without generating any noise, wind, or dust at all—and, for good measure, without posing any threat of injury. Suppose the police employed this miraculous tool to discover not only what crops people were growing in their greenhouses, but also what books they were reading and who their dinner guests were. Suppose, finally, that the FAA regulations remained unchanged, so that the police were undeniably "where they had a right to be." Would today's ***463** plurality continue to assert that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" was not infringed by such surveillance? Yet that is the logical consequence of the plurality's rule that, so long as the police are where they have a right to be under air traffic regulations, the Fourth Amendment is offended only if the aerial surveillance interferes with the use of the backyard as a garden spot. Nor is there anything in the plurality's opinion to suggest that any different rule would apply were the police looking from their helicopter, not into the open curtilage, but through an open window into a room viewable only from the air.

III

Perhaps the most remarkable passage in the plurality opinion is its suggestion that the case might be a different one had any "intimate details connected with the use of the home or curtilage [been] observed." *Ante,* at 697. What, one wonders, is meant by "intimate details"? If the police had observed **Riley** embracing his wife in the backyard greenhouse, would we then say that his reasonable expectation of privacy had been infringed? Where in the Fourth ****704** Amendment or in our cases is there any warrant for imposing a requirement that the activity observed must be "intimate" in order to be protected by the Constitution?

It is difficult to avoid the conclusion that the plurality has allowed its analysis of **Riley's** expectation of privacy to be colored by its distaste for the activity in which he was engaged. It is indeed easy to forget, especially in view of current concern over drug trafficking, that the scope of the Fourth Amendment's protection does not turn on whether the activity disclosed by a search is illegal or innocuous. But we dismiss this as a "drug case" only at the peril of our own liberties. Justice Frankfurter once noted that "[i]t is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very ***464** nice people," *United States v. Rabinowitz,* 339 U.S. 56, 69, 70 S.Ct. 430, 436, 94 L.Ed. 653 (1950) (dissenting opinion), and nowhere is this observation more apt than in the area of the Fourth Amendment, whose words have necessarily been given meaning largely through decisions suppressing evidence of criminal activity. The principle enunciated in this case determines what limits the Fourth Amendment imposes on aerial surveillance of any person, for any reason. If the Constitution does not protect **Riley's** marijuana garden against such surveillance, it is hard to see how it will prohibit the government from aerial spying on the activities of a law-abiding citizen on her fully enclosed outdoor patio. As Professor Amsterdam has eloquently written: "The question is not whether you or I must draw the blinds before we commit a crime. It is whether you and I must discipline ourselves to draw the blinds every time we enter a room, under pain of surveillance if we do not." 58 Minn.L.Rev., at 403. [6]

IV

I find little to disagree with Justice O'CONNOR's concurrence, apart from its closing paragraphs. A majority of the Court thus agrees that the fundamental inquiry is not whether the police were where they had a right to be under FAA regulations, but rather whether Riley's expectation of privacy was rendered illusory by the extent of ***465** public observation of his backyard from aerial traffic at 400 feet.

What separates me from Justice O'CONNOR is essentially an empirical matter concerning the extent of public use of the airspace at that altitude, together with the question of how to resolve that issue. I do not think the constitutional claim should fail simply because "there is reason to believe" that there is "considerable" public flying this close to earth or because Riley "introduced no evidence to the contrary before the Florida courts." *Ante,* at 699 (O'CONNOR, J., concurring in judgment). I should think that this might be an apt occasion for the application of Professor Davis' distinction between "adjudicative" and "legislative" facts. See Davis, An Approach to Problems of Evidence in the Administrative Process, 55 Harv.L.Rev. 364, 402–410 (1942); see also Advisory Committee's Notes on Fed.Rule Evid. 201, 28 U.S.C.App., pp. 683–684. If so, I think we could take judicial notice that, while there may be an occasional privately owned helicopter that flies over populated areas at an altitude of 400 feet, such flights are a rarity and are almost entirely limited to approaching or leaving airports or to reporting traffic congestion near major roadways. And, as the concurrence agrees, ****705** *ante,* at 699, the extent of police surveillance traffic cannot serve as a bootstrap to demonstrate public use of the airspace.

If, however, we are to resolve the issue by considering whether the appropriate party carried its burden of proof, I again think that Riley must prevail. Because the State has greater access to information concerning customary flight patterns and because the coercive power of the State ought not be brought to bear in cases in which it is unclear whether the prosecution is a product of an unconstitutional, warrantless search, cf. *Bumper v. North Carolina,* 391 U.S. 543, 548, 88 S.Ct. 1788, 1791–1792, 20 L.Ed.2d 797 (1968) (prosecutor has burden of proving consent to search), the burden of proof properly rests with the State and ***466** not with the individual defendant. The State quite clearly has not carried this burden. [7]

V

The issue in this case is, ultimately, "how tightly the Fourth Amendment permits people to be driven back into the recesses of their lives by the risk of surveillance." Amsterdam, *supra,* at 402. The Court today approves warrantless helicopter surveillance from an altitude of 400 feet. While Justice O'CONNOR's opinion gives reason to hope that this altitude may constitute a lower limit, I find considerable cause for concern in the fact that a plurality of four Justices would remove virtually all constitutional barriers to police surveillance from the vantage point of helicopters. The Fourth Amendment demands that we temper our efforts to apprehend criminals with a concern for the impact on our fundamental liberties of the methods we use. I hope it will be a matter of concern to my colleagues that the police surveillance methods they would sanction were among those described 40 years ago in George Orwell's dread vision of life in the 1980's:

> "The black-mustachio'd face gazed down from every commanding corner. There was one on the house front immediately opposite. BIG BROTHER IS WATCHING YOU, the caption said.... In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the Police Patrol, snooping into people's windows." Nineteen Eighty–Four 4 (1949).

***467** Who can read this passage without a shudder, and without the instinctive reaction that it depicts life in some country other than ours? I respectfully dissent.

Justice BLACKMUN, dissenting.

The question before the Court is whether the helicopter surveillance over Riley's property constituted a "search" within the meaning of the Fourth Amendment. Like Justice BRENNAN, Justice MARSHALL, Justice STEVENS, and Justice O'CONNOR, I believe that answering this question depends upon whether Riley

has a "reasonable expectation of privacy" that no such surveillance would occur, and does not depend upon the fact that the helicopter was flying at a lawful altitude under FAA regulations. A majority of this Court thus agrees to at least this much.

The inquiry then becomes how to determine whether **Riley's** expectation was a reasonable one. Justice BRENNAN, the two Justices who have joined him, and Justice O'CONNOR all believe that the reasonableness of **Riley's** expectation depends, in large measure, on the frequency of nonpolice helicopter flights at an altitude of 400 feet. Again, I agree.

How is this factual issue to be decided? Justice BRENNAN suggests that we may ****706** resolve it ourselves without any evidence in the record on this point. I am wary of this approach. While I, too, suspect that for most American communities it is a rare event when nonpolice helicopters fly over one's curtilage at an altitude of 400 feet, I am not convinced that we should establish a *per se* rule for the entire Nation based on judicial suspicion alone. See Coffin, Judicial Balancing, 63 N.Y.U.L.Rev. 16, 37 (1988).

But we need not abandon our judicial intuition entirely. The opinions of both Justice BRENNAN and Justice O'CONNOR, by their use of "cf." citations, implicitly recognize that none of our prior decisions tells us who has the burden of proving whether **Riley's** expectation of privacy was reasonable. In the absence of precedent on the point, it is appropriate for us to take into account our estimation of the ***468** frequency of nonpolice helicopter flights. See 4 W. LaFave, Search and Seizure § 11.2(b), p. 228 (2d ed. 1987) (burdens of proof relevant to Fourth Amendment issues may be based on a judicial estimate of the probabilities involved). Thus, because I believe that private helicopters rarely fly over curtilages at an altitude of 400 feet, I would impose upon the prosecution the burden of proving contrary facts necessary to show that **Riley** lacked a reasonable expectation of privacy. Indeed, I would establish this burden of proof for any helicopter surveillance case in which the flight occurred below 1,000 feet—in other words, for any aerial surveillance case not governed by the Court's decision in *California v. Ciraolo,* 476 U.S. 207, 106 **S.Ct**. 1809, 90 L.Ed.2d 210 (1986).

In this case, the prosecution did not meet this burden of proof, as Justice BRENNAN notes. This failure should compel a finding that a Fourth Amendment search occurred. But because our prior cases gave the parties little guidance on the burden of proof issue, I would remand this case to allow the prosecution an opportunity to meet this burden.

The order of this Court, however, is not to remand the case in this manner. Rather, because Justice O'CONNOR would impose the burden of proof on **Riley** and because she would not allow **Riley** an opportunity to meet this burden, she joins the plurality's view that no Fourth Amendment search occurred. The judgment of the Court, therefore, is to reverse outright on the Fourth Amendment issue. Accordingly, for the reasons set forth above, I respectfully dissent.

All Citations

488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835, 57 USLW 4126

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Lumber Co.,* 200 U.S. 321, 337, 26 **S.Ct**. 282, 287, 50 L.Ed. 499.

1 The **Florida** Supreme Court mentioned the State Constitution in posing the question, once in the course of its opinion, and again in finally concluding that the search violated the Fourth Amendment and the State Constitution. The bulk of the discussion, however, focused exclusively on federal cases dealing with the Fourth Amendment, and there being no indication that the decision "clearly and expressly ... is alternatively based on bona fide separate, adequate, and independent grounds," we have jurisdiction. *Michigan v. Long,* 463 U.S. 1032, 1041, 103 **S.Ct**. 3469, 3476–3477, 77 L.Ed.2d 1201 (1983).

109 S.Ct. 693, 102 L.Ed.2d 835, 57 USLW 4126

2 The first use of the helicopter by police was in New York in 1947, and today every State in the country uses helicopters in police work. As of 1980, there were 1,500 such aircraft used in police work. E. Brown, The Helicopter in Civil Operations 79 (1981). More than 10,000 helicopters, both public and private, are registered in the United States. Federal Aviation Administration, Census of U.S. Civil Aircraft, Calendar Year 1987, p. 12. See also 1988 Helicopter Annual 9. And there are an estimated 31,697 helicopter pilots. Federal Aviation Administration, Statistical Handbook of Aviation, Calendar Year 1986, p. 147.

3 While Federal Aviation Administration regulations permit fixed-wing-aircraft to be operated at an altitude of 1,000 feet while flying over congested areas and at an altitude of 500 feet above the surface in other than congested areas, helicopters may be operated at less than the minimums for fixed-wing-aircraft "if the operation is conducted without hazard to persons or property on the surface. In addition, each person operating a helicopter shall comply with routes or altitudes specifically prescribed for helicopters by the [FAA] Administrator." 14 CFR § 91.79 (1988).

1 What the plurality now states as a firm rule of Fourth Amendment jurisprudence appeared in *Ciraolo,* 476 U.S., at 213, 106 **S.Ct**., at 1812–1813, as a passing comment: "Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible. *E.g., United States v. Knotts,* 460 U.S. 276, 282 [103 **S.Ct**. 1081, 1085–1086, 75 L.Ed.2d 55] (1983)." This rule for determining the constitutionality of aerial surveillance thus derives ultimately from *Knotts,* a case in which the police officers' feet were firmly planted on the ground. What is remarkable is not that one case builds on another, of course, but rather that a principle based on terrestrial observation was applied to airborne surveillance without any consideration whether that made a difference.

2 The plurality's use of the FAA regulations as a means for determining whether **Riley** enjoyed a reasonable expectation of privacy produces an incredible result. Fixed-wing aircraft may not be operated below 500 feet (1,000 feet over congested areas), while helicopters may be operated below those levels. See *ante,* at 701, n. 3. Therefore, whether **Riley's** expectation of privacy is reasonable turns on whether the police officer at 400 feet above his curtilage is seated in an airplane or a helicopter. This cannot be the law.

3 In *Oliver v. United States,* 466 U.S. 170, 104 **S.Ct**. 1735, 80 L.Ed.2d 214 (1984), for example, we held that police officers who trespassed upon posted and fenced private land did not violate the Fourth Amendment, despite the fact that their action was subject to criminal sanctions. We noted that the interests vindicated by the Fourth Amendment were not identical with those served by the common law of trespass. See *id.,* at 183–184, and n. 15, 104 **S.Ct**., at 1744, and n. 15; see also *Hester v. United States,* 265 U.S. 57, 44 **S.Ct**. 445, 68 L.Ed. 898 (1924) (trespass in "open fields" does not violate the Fourth Amendment). In *Olmstead v. United States,* 277 U.S. 438, 466–469, 48 **S.Ct**. 564, 72 L.Ed. 944 (1928), the illegality under state law of a wiretap that yielded the disputed evidence was deemed irrelevant to its admissibility. And of course *Katz v. United States,* 389 U.S. 347, 88 **S.Ct**. 507, 19 L.Ed.2d 576 (1967), which overruled *Olmstead,* made plain that the question whether or not the disputed evidence had been procured by means of a trespass was irrelevant. Recently, in *Dow Chemical Co. v. United States,* 476 U.S. 227, 239, n. 6, 106 **S.Ct**. 1819, 1827, n. 6, 90 L.Ed.2d 226 (1986), we declined to consider trade-secret laws indicative of a reasonable expectation of privacy. Our precedent thus points not toward the position adopted by the plurality opinion, but rather toward the view on this matter expressed some years ago by the Oregon Court of Appeals: "We ... find little attraction in the idea of using FAA regulations because they were not formulated for the purpose of defining the reasonableness of citizens' expectations of privacy. They were designed to promote air safety." *State v. Davis,* 51 Or.App. 827, 831, 627 P.2d 492, 494 (1981).

4 Cf. *California v. Greenwood,* 486 U.S. 35, 54, 108 **S.Ct**. 1625, 1636, 100 L.Ed. 30 (1988) (BRENNAN, J., dissenting) ("The mere *possibility* that unwelcome meddlers *might* open and rummage through the containers does not negate the expectation of privacy in their contents ...").

5 Without actually stating that it makes any difference, the plurality also notes that "there is nothing in the record or before us to suggest" that helicopter traffic at the 400–foot level is so rare as to justify **Riley's** expectation of privacy. *Ante,* at 697. The absence of anything "in the record or before us" to suggest the opposite, however, seems not to give the plurality pause. It appears, therefore, that it is the FAA regulations rather than any empirical inquiry that is determinative.

6 See also *United States v. White,* 401 U.S. 745, 789–790, 91 **S.Ct**. 1122, 1144–1145, 28 L.Ed.2d 453 (1971) (Harlan, J., dissenting):

> "By casting its 'risk analysis' solely in terms of the expectations and risks that 'wrongdoers' or 'one contemplating illegal activities' ought to bear, the plurality opinion, I think, misses the mark entirely.... The interest [protected by the Fourth

> Amendment] is the expectation of the ordinary citizen, who has never engaged in illegal conduct in his life, that he may carry on his private discourse freely, openly, and spontaneously.... Interposition of a warrant requirement is designed not to shield 'wrongdoers,' but to secure a measure of privacy and a sense of personal security throughout our society."

7 The issue in *Jones v. United States,* 362 U.S. 257, 261, 80 **S.Ct**. 725, 731, 4 L.Ed.2d 697 (1960), cited by Justice O'CONNOR, was whether the defendant had standing to raise a Fourth Amendment challenge. While I would agree that the burden of alleging and proving facts necessary to show standing could ordinarily be placed on the defendant, I fail to see how that determination has any relevance to the question where the burden should lie on the merits of the Fourth Amendment claim.

Harnessing machine learning for baggage scans

By Mark Rockwell | May 04, 2018

The Transportation Security Administration is looking to Silicon Valley startups to help it bring machine learning to security screening to improve the accuracy of airport baggage scanners.

MOST POPULAR ARTICLES

Supply chain highlighted in Risk Management Framework update

Tech keeps FINRA on top of the market

How to rethink analytics for citizen-centric government

5 reasons municipalities are getting hit by cyber threats

Science agencies invest in quantum

Through an Other Transaction Solicitation, the Department of Homeland Security's Science & Technology Directorate and TSA's Office of Requirements and Capabilities Analysis are looking for a new way to detect evolving threats carried in airline passenger luggage.

Rapidly changing consumer electronics, the RFI said, are an example of a dynamic threat vector that evolves faster than next-generation detector hardware. TSA personnel looking at baggage scanner images might miss subtle new differences in how newly introduced consumer devices are wired or put together.

The agency wants developers to come up with AI-based methods that could automate detection algorithm training, allowing detection hardware to "intuitively recognize" such subtleties and new objects that come through airports in luggage. If that software can be easily plugged into existing detection gear at airports to identify subtle, but potentially devastating, threats to aircraft, TSA could move away from expensive and proprietary detection capabilities in its luggage screening hardware, while also avoiding labor-intensive hand searches.

The solicitation suggests a system using an image library combined with artificial intelligence could to learn to identify new items and distinguish between benign objects and potential threats.

The OTS would fund development efforts in four three- to six-month $200,000 sprints. TSA is holding an industry day in Menlo Park, Calif., on May 4.

Meanwhile, TSA is also investigating incorporating machine learning into the computer tomography scanners that are starting to be used at airport security checkpoints.

This article was first posted to FCW, a sibling site to GCN.

About the Author

Mark Rockwell is a senior staff writer at FCW, whose beat focuses on acquisition, the Department of Homeland Security and the Department of Energy.

Before joining FCW, Rockwell was Washington correspondent for Government Security News, where he covered all aspects of homeland security from IT to detection dogs and border security. Over the last 25 years in Washington as a reporter, editor and correspondent, he has covered an increasingly wide array of high-tech issues for publications like Communications Week, Internet Week, Fiber Optics News, tele.com magazine and Wireless Week.

Rockwell received a Jesse H. Neal Award for his work covering telecommunications issues, and is a graduate of James Madison University.

Click here for previous articles by Rockwell. Contact him at mrockwell@fcw.com or follow him on Twitter at @MRockwell4.

E-Mail this page Printable Format

RELATED ARTICLES

- Worst storm ever? NOAA maps 170 years of hurricane data
- SSA seeks virtual assistants to help with boomer retirements
- ICE seeks robust video evidence management
- NOAA fine-tunes its cloud-based Big Data Project
- OMB, DLA join ranks of bot-friendly agencies
- Blockchain for trade certificate management
- Drone deterrence: Easy to buy, tricky to use legally
- State of AI: Beneficial, but challenges persist

INSIDE GCN

How state governments bolster cybersecurity

READER COMMENTS

Please post your comments here. Comments are moderated, so they may not appear immediately after submitting. We will not post comments that we consider abusive or off-topic.

Name: (Optional)

Email: (Optional)

Location: (Optional)

Your Comment:

Please type the letters/numbers you see above

SUBMIT MESSAGE

More from 1105 Public Sector Media Group

Federal SOUP

- Republican lawmaker says deal has been reached on fed pay raise
- VA relaunches website; focuses on customer service
- Federal scientists pen letter to Congress opposing USDA reorg

FCW

- OPM targets improved job satisfaction scores
- U.S. indicts Russian hackers in global conspiracy
- House Republicans agree to give feds pay raise

Washington Technology

- BluVector's quiet win speaks plenty about cyber opportunity
- Air Force may require agile for all acquisitions
- GD taps small business team for $465M Army training contract

Defense Systems

- 'Kessel Run' could set standard for Air Force IT
- At Navy PEO EIS, the change keeps coming
- Navy awards 'C5ISR' tech services contract

8251 Greensboro Drive, Suite 510
McLean, VA 22102
703-876-5100

PUBLIC SECTOR MEDIA GROUP

For more information about the PIA report, or doing the associated PIA, contact:

Rebecca Herold
rebeccaherold@rebeccaherold.com
www.privacyguidance.com
www.compliancehelper.com

<Name>
Privacy Impact Assessment
Full Report

[CLIENT LOGO]

Prepared by Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI
<date>

Table of Contents

Executive Summary

<Intro/background>

1. **Company information security and privacy administration**	Findings summary
2. **Corporate leadership**	Findings summary
3. **Data collection and processing**	Findings summary
4. **Data retention**	Findings summary
5. **Openness and transparency**	Findings summary
6. **Responsiveness**	Findings summary
7. **Hardware and software physical security**	Findings summary
8. **Customer control**	Findings summary
9. **Consent and opt-in/opt-out controls**	Findings summary
10. **Privacy Enhancing Practices & Technology**	Findings summary
11. **Privacy Invading Practices & Technology**	Findings summary
Assessment & Justification	Findings summary

LEGEND:

- **Green:** **Privacy-friendly and privacy enhancing**
- **Blue:** **Generally privacy aware but could be improved upon**
- **Yellow:** **Generally aware of privacy issues and requirements, but notable lapses exist**
- **Red:** **Substantial and comprehensive privacy threats**
- **Black:** **Significant lack of security for PII**

Table 1 – <Company X>PIA summary

<Company X>PIA Report

<Intro/background>

A. Summary of PIA Findings

<Info>

B. Purpose of a PIA

<Info>

C. <Company X><PIA scope> Description

<Description>

Data Item	Data Item Description
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	

Table 2 – Data Within <Company X><PIA scope> Processing

<Add additional details, flow diagrams, tables, illustrations, etc. describing the PIA scope here>

D. GAPP Alignment

1. Management, Accountability & Training

<Put findings here>

Information Security and Privacy Training and Awareness Practices

<Put findings here>

2. Notice & Purpose for PII Use

<Put findings here>

3. Choice & Consent to use PII

<Put findings here>

4. Collection of PII

<Put findings here>

5. Use and Retention of PII

<Put findings here>

6. Individual access

<Put findings here>

7. Disclosure and Limiting Use of PII

<Put findings here>

8. Security and Safeguards

<Put findings here>

9. Accuracy & Quality of PII

<Put findings here>

10. Openness, Monitoring & Challenging Compliance

<Put findings here>

E. PCI DSS Compliance <Include section only if applicable>

<Put findings here>

F. HIPAA/HITECH Compliance <Include section only if applicable>

<Put findings here>

G. <Put regulation/standard/etc. as applicable > <Include section only if applicable>

<Put findings here>

Work Papers

<Background info>

The recommendations include:

<Put recommendations here>

NOTE: This report is not, and should not be construed as, a legal opinion.

1. Project Scope

<Description>

2. <Company X><PIA scope> process

Figure 1 shows the <Company X>online <Company X><PIA scope> process.

<Put diagram here>

Figure 1 – <Company X><PIA scope> processing

Personally Identifiable Information (PII)

<Description>

Data Item	Data Item Description
14.	
15.	
16.	
17.	
18.	
19.	
20.	
21.	
22.	
23.	
24.	
25.	
26.	

Figure 2 – Data Within <Company X><PIA scope> Processing

Areas of concern

<fill in>

Recommendations

<fill in>

3. Privacy Complaints and Incidents

<Put description of review and work here>.

Areas of concern
<fill in>

Recommendations
<fill in>

4. Privacy Policies and Practices

<Description>

4.1 Website Privacy Policies

<Put description of work and review here>

Areas of concern

<fill in>

Recommendations
<fill in>

4.2 Internal Information Security and Privacy Policies

<Describe importance of policies and procedures here>

<Describe work, research and findings here>

Areas of concern
<fill in>

Recommendations
<fill in>

5. Privacy Programs and Executive Support

<Company X> <provide applicable information here>

Areas of concern
<fill in>

Recommendations
<fill in>

6. Awareness and Training

<Company X> <provide applicable information here>

Areas of concern
<fill in>

Recommendations
<fill in>

7. PII Collection and Access

<Background>

7.1 Customer PII Collection

Customer PII is collected within **<Company X>**through the **<Company X><PIA scope>**.

- The **<Company X><PIA scope>** **<provide applicable information here>** The data items are listed in Table 2. PII items are highlighted in green. Information that, when coupled with a PII item, becomes sensitive are highlighted in yellow.

Data Item	Data Item Description
1.	
2.	
3.	
4.	
5.	

6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	

Table 2 – Data Within <Company X><PIA scope> Processing

<Illustrations> **<Company X><PIA scope>** looks on a website.

<Include diagrams, illustrations, screen prints, etc. as appropriate to the PIA scope.>

<Describe all types of PII collection activities here>

Areas of concern
<fill in>

Recommendations

<fill in>

7.2 Use Limitation & Sharing Customer PII With Third Parties

<Background>

<Describe PII sharing practices here>

Areas of concern

<fill in>

Recommendations

<fill in>

7.3 Purpose Specification

<Describe how purposes for PII use are, or are not, provided>

Areas of concern

<fill in>

Recommendations

<fill in>

7.4 Individual Participation

<Describe how individuals can access their own PII>

Areas of concern

<fill in>

Recommendations

<fill in>

8. Customer PII Storage

<Describe PII storage practices and locations>

Areas of concern
<fill in>

Recommendations
<fill in>

9. Laws, Regulations and Contracts

<include an description and appropriate list>

Areas of concern

<fill in>

Recommendations

<fill in>

10. Contractual Obligations

<Description>

Areas of concern

<fill in>

Recommendations

<fill in>

11. Background checks

<Description>

Areas of concern

<fill in>

Recommendations

<fill in>

12. Safeguards & Data Integrity

<Company X>has <**include information here as appropriate>**

Areas of concern

<fill in>

Recommendations

<fill in>

13. Data Quality

The **<Company X><PIA scope>** **<include information here as appropriate>**

Areas of concern
<fill in>

Recommendations

<fill in>

14. Customer PII Used for Test Purposes

Currently production **<Company X>**customer PII is **<provide details as applicable here>**

Areas of concern

<fill in>

Recommendations

<fill in>

15. Limiting access within applications and systems

<Company X>controls access to customer PII through **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16. Oversight, Maintenance & Evaluation

16.1 Accountability

The **<Company X>** **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.2 Openness

<Company X>has **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.3 Customer PII Retention

<Company X> **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.4 Customer PII Disposal

The **<Company X>** **<include applicable information here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.5 Compliance and enforcement

<Company X> **<include applicable information here>**

Areas of concern

<fill in>

Recommendations

<fill in>

Appendix A – <Company X>Privacy Survey Responses

<Put verbatim copies of completed PIA surveys here>

Appendix B – Existing <Company X>Information Security and Privacy Policies

<Fill in as appropriate>

Appendix C – Recommended Information Security and Privacy Policies & Supporting Documents

<Fill in as appropriate>

Appendix D – <Company X>PIA Project Meeting Notes

<Copy all PIA meeting notes here>

Appendix E –U.S. State Breach Notice Laws

Appendix F – <Company X>Website Privacy Policies

<Copy here verbatim>

Appendix G - Data Protection (Privacy) Laws

<Describe applicable laws here>

Appendix H - <Company X>Information Security and Privacy Training and Awareness Program

<Fill in as appropriate>

Appendix I - Recommended <Company X>Website Privacy Policy

<Fill in appropriately>

Appendix J - Updated <Company X>Website Privacy Policy

<Fill in as applicable>

Appendix K – <Change to PIA Specific Issue>

Appendix L – <Change to PIA Specific Issue>

Appendix M – Updated <Company X>Security Policies

<Change appropriately>

KeyCite Yellow Flag - Negative Treatment
Declined to Extend by Florida v. Jardines, U.S.Fla., March 26, 2013

121 S.Ct. 2038
Supreme Court of the United States

Danny Lee **KYLLO**, Petitioner,
v.
UNITED STATES.

No. 99–8508.
|
Argued Feb. 20, 2001.
|
Decided June 11, 2001.

Synopsis
After unsuccessfully moving to suppress evidence, defendant entered conditional guilty plea to manufacturing marijuana and appealed. Following remand, 37 F.3d 526, the United States District Court for the District of Oregon, Helen J. Frye, J., again denied suppression motion, and defendant appealed. The Ninth Circuit Court of Appeals, 190 F.3d 1041, affirmed. Certiorari was granted. The United States Supreme Court, Justice Scalia, held that: (1) use of sense-enhancing technology to gather any information regarding interior of home that could not otherwise have been obtained without physical intrusion into constitutionally protected area constitutes a "search," and (2) use of thermal imaging to measure heat emanating from home was search.

Reversed and remanded.

Justice Stevens filed a dissenting opinion, in which Chief Justice Rehnquist and Justices O'Connor and Kennedy joined.

West Headnotes (7)

[1] Searches and Seizures
Fourth Amendment and reasonableness in general

With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no. U.S.C.A. Const.Amend. 4.

132 Cases that cite this headnote

[2] Searches and Seizures
What Constitutes Search or Seizure

Searches and Seizures
Use of electronic devices;tracking devices or "beepers."

Obtaining by sense-enhancing technology any information regarding the interior of a home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a "search"—at least where the technology in question is not in general public use. U.S.C.A. Const.Amend. 4.

179 Cases that cite this headnote

[3] Controlled Substances
Premises, Search of

Searches and Seizures
What Constitutes Search or Seizure

Police engaged in unlawful "search" when they used thermal imaging device without warrant to scan home to determine whether heat emanating from home was consistent with use of high-intensity lamps employed in indoor marijuana growing operation. U.S.C.A. Const.Amend. 4.

104 Cases that cite this headnote

[4] Searches and Seizures
What Constitutes Search or Seizure

Use of thermal imaging devices to gather information about heat in home's interior is not removed from scope of Fourth Amendment search merely because device captures only heat radiating from external surface of house, and thus involves "off-

the-wall" rather than "through-the-wall" observation. U.S.C.A. Const.Amend. 4.

220 Cases that cite this headnote

[5] Searches and Seizures

What Constitutes Search or Seizure

Information gathered through use of thermal imaging to measure heat emanating from exterior of home is product of a search even if relevant information regarding heat use in interior of home must be inferred from information provided by device. U.S.C.A. Const.Amend. 4.

50 Cases that cite this headnote

[6] Controlled Substances

Premises, Search of

Searches and Seizures

Nature and source of information in general;suspicion or conjecture

Prohibition against warrantless use of thermal imaging devices is not limited to "intimate details" regarding home; such limitation would be wrong in principle, in that Fourth Amendment's protection of home has never been tied to measurement of quality of information obtained, and impracticable in application, in that it would not provide a workable accommodation between law enforcement needs and Fourth Amendment interests, and would require development of jurisprudence specifying which home activities are "intimate" and which are not. U.S.C.A. Const.Amend. 4.

322 Cases that cite this headnote

[7] Searches and Seizures

What Constitutes Search or Seizure

Searches and Seizures

Use of electronic devices;tracking devices or "beepers."

Searches and Seizures

Nature and source of information in general;suspicion or conjecture

Where the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search"and is presumptively unreasonable without a warrant. U.S.C.A. Const.Amend. 4.

192 Cases that cite this headnote

****2039** *Syllabus* [*]

***27** Suspicious that marijuana was being grown in petitioner **Kyllo's** home in a triplex, agents used a thermal-imaging device to scan the triplex to determine if the amount of heat emanating from it was consistent with the high-intensity lamps typically used for indoor marijuana growth. The scan showed that **Kyllo's** garage roof and a side wall were relatively hot compared to the rest of his home and substantially warmer than the neighboring units. Based in part on the thermal imaging, a Federal Magistrate Judge issued a warrant to search **Kyllo's** home, where the agents found marijuana growing. After **Kyllo** was indicted on a federal drug charge, he unsuccessfully moved to suppress the evidence seized from his home and then entered a conditional guilty plea. The Ninth Circuit ultimately affirmed, upholding the thermal imaging on the ground that **Kyllo** had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home. Even if he had, ruled the court, there was no objectively reasonable expectation of privacy because the thermal imager did not expose any intimate details of **Kyllo's** life, only amorphous hot spots on his home's exterior.

Held: Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant. Pp. 2041–2047.

(a) The question whether a warrantless search of a home is reasonable and hence constitutional must be answered no in most instances, but the antecedent question whether a Fourth Amendment "search" has occurred is not so simple. This Court has approved warrantless visual surveillance of a home, see *California v. Ciraolo,* 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210, ruling that visual observation is no "search" at all, see *Dow Chemical Co. v. United States,* 476 U.S. 227, 234–235, 239, 106 S.Ct. 1819, 90 L.Ed.2d 226. In assessing when a search is not a search, the Court has adapted a principle first enunciated in *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576: A "search" does not occur—even when its object is a house explicitly protected by ****2040** the Fourth Amendment—unless the individual manifested a subjective ***28** expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable, see, *e.g., California v. Ciraolo, supra,* at 211, 106 S.Ct. 1809. Pp. 2041–2043.

(b) While it may be difficult to refine the *Katz* test in some instances, in the case of the search of a home's interior —the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists,* and that is acknowledged to be *reasonable.* To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. Thus, obtaining by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman v. United States,* 365 U.S. 505, 512, 81 S.Ct. 679, 5 L.Ed.2d 734, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. P. 2043.

(c) Based on this criterion, the information obtained by the thermal imager in this case was the product of a search. The Court rejects the Government's argument that the thermal imaging must be upheld because it detected only heat radiating from the home's external surface. Such a mechanical interpretation of the Fourth Amendment was rejected in *Katz,* where the eavesdropping device in question picked up only sound waves that reached the exterior of the phone booth to which it was attached. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. Also rejected is the Government's contention that the thermal imaging was constitutional because it did not detect "intimate details." Such an approach would be wrong in principle because, in the sanctity of the home, *all* details are intimate details. See, *e.g., United States v. Karo,* 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530; *Dow Chemical, supra,* at 238, 106 S.Ct. 1819, distinguished. It would also be impractical in application, failing to provide a workable accommodation between law enforcement needs and Fourth Amendment interests. See *Oliver v. United States,* 466 U.S. 170, 181, 104 S.Ct. 1735, 80 L.Ed.2d 214. Pp. 2044–2046.

(d) Since the imaging in this case was an unlawful search, it will remain for the District Court to determine whether, without the evidence it provided, the search warrant was supported by probable cause—and if not, whether there is any other basis for supporting admission of that evidence. Pp. 2046–2047.

190 F.3d 1041, reversed and remanded.

***29** SCALIA, J., delivered the opinion of the Court, in which SOUTER, THOMAS, GINSBURG, and BREYER, JJ., joined. STEVENS, J., filed a dissenting opinion, in which REHNQUIST, C.J., and O'CONNOR and KENNEDY, JJ., joined, *post,* p. 2047.

Attorneys and Law Firms

Kenneth Lerner, for petitioner.

Michael R. Dreeben, Washington, DC, for respondent.

Opinion

Justice SCALIA delivered the opinion of the Court.

This case presents the question whether the use of a thermal-imaging device aimed at a private home from a public street to ****2041** detect relative amounts of heat

within the home constitutes a "search" within the meaning of the Fourth Amendment.

I

In 1991 Agent William Elliott of the United States Department of the Interior came to suspect that marijuana was being grown in the home belonging to petitioner Danny **Kyllo**, part of a triplex on Rhododendron Drive in Florence, Oregon. Indoor marijuana growth typically requires high-intensity lamps. In order to determine whether an amount of heat was emanating from petitioner's home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex. Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth—black ***30** is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images. The scan of **Kyllo's** home took only a few minutes and was performed from the passenger seat of Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house, which indeed he was. Based on tips from informants, utility bills, and the thermal imaging, a Federal Magistrate Judge issued a warrant authorizing a search of petitioner's home, and the agents found an indoor growing operation involving more than 100 plants. Petitioner was indicted on one count of manufacturing marijuana, in violation of 21 U.S.C. § 841(a)(1). He unsuccessfully moved to suppress the evidence seized from his home and then entered a conditional guilty plea.

The Court of Appeals for the Ninth Circuit remanded the case for an evidentiary hearing regarding the intrusiveness of thermal imaging. On remand the District Court found that the Agema 210 "is a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house"; it "did not show any people or activity within the walls of the structure"; "[t]he device used cannot penetrate walls or windows to reveal conversations or human activities"; and "[n]o intimate details of the home were observed." Supp.App. to Pet. for Cert. 39–40. Based on these findings, the District Court upheld the validity of the warrant that relied in part upon the thermal imaging, and reaffirmed its denial of the motion to suppress. A divided Court of Appeals initially reversed, 140 F.3d 1249 (1998), but that ***31** opinion was withdrawn and the panel (after a change in composition) affirmed, 190 F.3d 1041 (1999), with Judge Noonan dissenting. The court held that petitioner had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home, *id.,* at 1046, and even if he had, there was no objectively reasonable expectation of privacy because the imager "did not expose any intimate details of **Kyllo's** life," only "amorphous 'hot spots' on the roof and exterior wall," *id.,* at 1047. We granted certiorari. 530 **U.S.** 1305, **121** **S.Ct.** 29, 147 L.Ed.2d 1052 (2000).

II

[1] The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." "At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." ****2042** *Silverman v. United States,* 365 **U.S.** 505, 511, 81 **S.Ct.** 679, 5 L.Ed.2d 734 (1961). With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no. See *Illinois v. Rodriguez,* 497 **U.S.** 177, 181, 110 **S.Ct.** 2793, 111 L.Ed.2d 148 (1990); *Payton v. New York,* 445 **U.S.** 573, 586, 100 **S.Ct.** 1371, 63 L.Ed.2d 639 (1980).

On the other hand, the antecedent question whether or not a Fourth Amendment "search" has occurred is not so simple under our precedent. The permissibility of ordinary visual surveillance of a home used to be clear because, well into the 20th century, our Fourth Amendment

jurisprudence was tied to common-law trespass. See, *e.g., Goldman v. United States,* 316 U.S. 129, 134–136, 62 S.Ct. 993, 86 L.Ed. 1322 (1942); *Olmstead v. United States,* 277 U.S. 438, 464–466, 48 S.Ct. 564, 72 L.Ed. 944 (1928). Cf. *Silverman v. United States, supra,* at 510–512, 81 S.Ct. 679 (technical trespass not necessary for Fourth Amendment violation; it suffices if there is "actual intrusion into a constitutionally protected area"). Visual surveillance was unquestionably lawful because " 'the ***32** eye cannot by the laws of England be guilty of a trespass.' " *Boyd v. United States,* 116 U.S. 616, 628, 6 S.Ct. 524, 29 L.Ed. 746 (1886) (quoting *Entick v. Carrington,* 19 How. St. Tr. 1029, 95 Eng. Rep. 807 (K.B.1765)). We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property, see *Rakas v. Illinois,* 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978), but the lawfulness of warrantless visual surveillance of a home has still been preserved. As we observed in *California v. Ciraolo,* 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986), "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."

One might think that the new validating rationale would be that examining the portion of a house that is in plain public view, while it is a "search" [1] despite the absence of trespass, is not an "unreasonable" one under the Fourth Amendment. See *Minnesota v. Carter,* 525 U.S. 83, 104, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (BREYER, J., concurring in judgment). But in fact we have held that visual observation is no "search" at all—perhaps in order to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional. See *Dow Chemical Co. v. United States,* 476 U.S. 227, 234–235, 239, 106 S.Ct. 1819, 90 L.Ed.2d 226 (1986). In assessing when a search is not a search, we have applied somewhat in reverse the principle first enunciated in *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). *Katz* involved eavesdropping by means of an electronic listening device placed on the outside of a telephone booth —a location not within the catalog ("persons, houses, papers, and effects") that the Fourth Amendment protects against unreasonable searches. We held that the ***33** Fourth Amendment nonetheless protected Katz from the warrantless eavesdropping because he "justifiably relied" upon the privacy of the telephone booth. *Id.,* at 353, 88 S.Ct. 507. As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. See *id.,* at 361, 88 S.Ct. 507. We have subsequently applied this principle to hold that a Fourth Amendment search does *not* occur—even when the explicitly protected location of a *house* is concerned—unless "the individual manifested a subjective expectation of privacy ****2043** in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable." *Ciraolo, supra,* at 211, 106 S.Ct. 1809. We have applied this test in holding that it is not a search for the police to use a pen register at the phone company to determine what numbers were dialed in a private home, *Smith v. Maryland,* 442 U.S. 735, 743–744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), and we have applied the test on two different occasions in holding that aerial surveillance of private homes and surrounding areas does not constitute a search, *Ciraolo, supra; Florida v. Riley,* 488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989).

The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much. While we upheld enhanced aerial photography of an industrial complex in *Dow Chemical,* we noted that we found "it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened," 476 U.S., at 237, n. 4, 106 S.Ct. 1819 (emphasis in original).

III

It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been ***34** entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. See *Ciraolo, supra,* at 215, 106 S.Ct. 1809. The question we confront today is what limits there

are upon this power of technology to shrink the realm of guaranteed privacy.

[2] **[3]** The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable. See 1 W. LaFave, Search and Seizure § 2.1(d), pp. 393–394 (3d ed.1996); Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 S.Ct. Rev. 173, 188; *Carter, supra,* at 97, 119 S.Ct. 469 (SCALIA, J., concurring). But see *Rakas, supra,* at 143–144, n. 12, 99 S.Ct. 421. While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences is at issue, in the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists,* and that is acknowledged to be *reasonable.* To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman,* 365 U.S., at 512, 81 S.Ct. 679, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the ***35** information obtained by the thermal imager in this case was the product of a search. [2]

****2044** **[4]** **[5]** The Government maintains, however, that the thermal imaging must be upheld because it detected "only heat radiating from the external surface of the house," Brief for United States 26. The dissent makes this its leading point, see *post,* at 2047, contending that there is a fundamental difference between what it calls "off-the-wall" observations and "through-the-wall surveillance." But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house-and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz,* where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human ***36** activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development. [3] The dissent's reliance on the distinction between "off-the-wall" and "through-the-wall" observation is entirely incompatible with the dissent's belief, which we discuss below, that thermal-imaging observations of the intimate details of a home are impermissible. The most sophisticated thermal-imaging devices continue to measure heat "off-the-wall" rather than "through-the-wall"; the dissent's disapproval of those more sophisticated thermal-imaging devices, see *post,* at 2051, is an acknowledgement that there is no substance to this distinction. As for the dissent's extraordinary assertion that anything learned through "an inference" cannot be a search, see *post,* at 2048–2049, that would validate even the "through-the-wall" technologies that the dissent purports to disapprove. Surely the dissent does not believe that the through-the-wall radar or ultrasound technology produces an 8–by–10 Kodak glossy that needs no analysis (*i.e.,* the making of inferences). And, of course, the novel proposition that inference insulates a search is blatantly contrary to *United States v. Karo,* 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), where the police "inferred" from the activation of a beeper that a certain can of ether was in the home. The police activity ***37** was held to be a search, and the search was held unlawful. [4]

****2045** **[6]** The Government also contends that the thermal imaging was constitutional because it did not "detect private activities occurring in private areas," Brief for United States 22. It points out that in *Dow Chemical* we observed that the enhanced aerial photography did not reveal any "intimate details." 476 U.S., at 238, 106 S.Ct. 1819. *Dow Chemical,* however, involved enhanced aerial photography of an industrial complex, which does not share the Fourth Amendment sanctity of the home. The

Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained. In *Silverman,* for example, we made clear that any physical invasion of the structure of the home, "by even a fraction of an inch," was too much, 365 U.S., at 512, 81 S.Ct. 679, and there is certainly no exception to the warrant requirement for the officer who barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor. In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes. Thus, in *Karo, supra,* the only thing detected was a can of ether in the ***38** home; and in *Arizona v. Hicks,* 480 U.S. 321, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987), the only thing detected by a physical search that went beyond what officers lawfully present could observe in "plain view" was the registration number of a phonograph turntable. These were intimate details because they were details of the home, just as was the detail of how warm—or even how relatively warm—**Kyllo** was heating his residence. [5]

Limiting the prohibition of thermal imaging to "intimate details" would not only be wrong in principle; it would be impractical in application, failing to provide "a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment," *Oliver v. United States,* 466 U.S. 170, 181, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984). To begin with, there is no necessary connection between the sophistication of the surveillance equipment and the "intimacy" of the details that it observes—which means that one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful. The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider "intimate"; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on. We could not, in other words, develop a rule approving only that through-the-wall surveillance which identifies objects no smaller than 36 by 36 inches, but would have to develop a jurisprudence specifying which ***39** home activities are "intimate" and which are not. ****2046** And even when (if ever) that jurisprudence were fully developed, no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up "intimate" details—and thus would be unable to know in advance whether it is constitutional.

The dissent's proposed standard—whether the technology offers the "functional equivalent of actual presence in the area being searched," *post,* at 2050—would seem quite similar to our own at first blush. The dissent concludes that *Katz* was such a case, but then inexplicably asserts that if the same listening device only revealed the volume of the conversation, the surveillance would be permissible, *post,* at 2051. Yet if, without technology, the police could not discern volume without being actually present in the phone booth, Justice STEVENS should conclude a search has occurred. Cf. *Karo,* 468 U.S., at 735, 104 S.Ct. 3296 (STEVENS, J., concurring in part and dissenting in part) ("I find little comfort in the Court's notion that no invasion of privacy occurs until a listener obtains some significant information by use of the device .... A bathtub is a less private area when the plumber is present even if his back is turned"). The same should hold for the interior heat of the home if only a person present in the home could discern the heat. Thus the driving force of the dissent, despite its recitation of the above standard, appears to be a distinction among different types of information—whether the "homeowner would even care if anybody noticed," *post,* at 2051. The dissent offers no practical guidance for the application of this standard, and for reasons already discussed, we believe there can be none. The people in their houses, as well as the police, deserve more precision. [6]

[7] ***40** We have said that the Fourth Amendment draws "a firm line at the entrance to the house," *Payton,* 445 U.S., at 590, 100 S.Ct. 1371. That line, we think, must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no "significant" compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.

> "The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and

rights of individual citizens." *Carroll v. United States,* 267 U.S. 132, 149, 45 S.Ct. 280, 69 L.Ed. 543 (1925).

Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.

Since we hold the Thermovision imaging to have been an unlawful search, it will remain for the District Court to determine whether, without the evidence it provided, the search warrant issued in this case was supported by probable cause—and if not, whether there is any other basis for supporting admission of the evidence that the search pursuant to the warrant produced.

**2047 *41 * * *

The judgment of the Court of Appeals is reversed; the case is remanded for further proceedings consistent with this opinion.

It is so ordered.

Justice STEVENS, with whom THE CHIEF JUSTICE, Justice O'CONNOR, and Justice KENNEDY join, dissenting.

There is, in my judgment, a distinction of constitutional magnitude between "through-the-wall surveillance" that gives the observer or listener direct access to information in a private area, on the one hand, and the thought processes used to draw inferences from information in the public domain, on the other hand. The Court has crafted a rule that purports to deal with direct observations of the inside of the home, but the case before us merely involves indirect deductions from "off-the-wall" surveillance, that is, observations of the exterior of the home. Those observations were made with a fairly primitive thermal imager that gathered data exposed on the outside of petitioner's home but did not invade any constitutionally protected interest in privacy. [1] Moreover, I believe that the supposedly "bright-line" rule the Court has created in response to its concerns about future technological developments is unnecessary, unwise, and inconsistent with the Fourth Amendment.

I

There is no need for the Court to craft a new rule to decide this case, as it is controlled by established principles from *42 our Fourth Amendment jurisprudence. One of those core principles, of course, is that "searches and seizures *inside a home* without a warrant are presumptively unreasonable." *Payton v. New York,* 445 U.S. 573, 586, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980) (emphasis added). But it is equally well settled that searches and seizures of property in plain view are presumptively reasonable. See *id.,* at 586–587, 100 S.Ct. 1371. [2] Whether that property is residential or commercial, the basic principle is the same: " 'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.' " *California v. Ciraolo,* 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (quoting *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)); see *Florida v. Riley,* 488 U.S. 445, 449–450, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989); *California v. Greenwood,* 486 U.S. 35, 40–41, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988); *Dow Chemical Co. v. United States,* 476 U.S. 227, 235–236, 106 S.Ct. 1819, 90 L.Ed.2d 226 (1986); **2048 *Air Pollution Variance Bd. of Colo. v. Western Alfalfa Corp.,* 416 U.S. 861, 865, 94 S.Ct. 2114, 40 L.Ed.2d 607 (1974). That is the principle implicated here.

While the Court "take[s] the long view" and decides this case based largely on the potential of yet-to-be-developed technology that might allow "through-the-wall surveillance," *ante,* at 2045–2046; see *ante,* at 2044, n. 3, this case involves nothing more than off-the-wall surveillance by law enforcement officers to gather information exposed to the general public from the outside of petitioner's home. All that the infrared camera did in this case was passively measure heat emitted *43 from the exterior surfaces of petitioner's home; all that those measurements showed were relative differences in emission levels, vaguely indicating that some areas of the roof and outside walls were warmer than others. As still images from the infrared scans show, see Appendix, *infra,* no details regarding the interior of petitioner's home

were revealed. Unlike an x-ray scan, or other possible "through-the-wall" techniques, the detection of infrared radiation emanating from the home did not accomplish "an unauthorized physical penetration into the premises," *Silverman v. United States,* 365 U.S. 505, 509, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961), nor did it "obtain information that it could not have obtained by observation from outside the curtilage of the house," *United States v. Karo,* 468 U.S. 705, 715, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984).

Indeed, the ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from a building, particularly if it is vented, as was the case here. Additionally, any member of the public might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces. Such use of the senses would not convert into an unreasonable search if, instead, an adjoining neighbor allowed an officer onto her property to verify her perceptions with a sensitive thermometer. Nor, in my view, does such observation become an unreasonable search if made from a distance with the aid of a device that merely discloses that the exterior of one house, or one area of the house, is much warmer than another. Nothing more occurred in this case.

Thus, the notion that heat emissions from the outside of a dwelling are a private matter implicating the protections of the Fourth Amendment (the text of which guarantees the right of people "to be secure *in* their ... houses" against unreasonable searches and seizures (emphasis added)) is not only unprecedented but also quite difficult to take seriously. Heat waves, like aromas that are generated in a kitchen, or ***44** in a laboratory or opium den, enter the public domain if and when they leave a building. A subjective expectation that they would remain private is not only implausible but also surely not "one that society is prepared to recognize as 'reasonable.' " *Katz,* 389 U.S., at 361, 88 S.Ct. 507 (Harlan, J., concurring).

To be sure, the homeowner has a reasonable expectation of privacy concerning what takes place within the home, and the Fourth Amendment's protection against physical invasions of the home should apply to their functional equivalent. But the equipment in this case did not penetrate the walls of petitioner's home, and while it did pick up "details of the home" that were exposed to the public, *ante,* at 2045, it did not obtain "any information regarding the *interior* of the home," *ante,* at 2043 (emphasis added). In the Court's own words, based on what the thermal imager "showed" regarding the outside of petitioner's home, the officers "concluded" that petitioner was engaging in illegal activity inside the home. *Ante,* at 2041. It would be quite absurd to characterize their thought processes as "searches," regardless of whether they inferred (rightly) that petitioner was growing marijuana in his house, or (wrongly) that "the lady of the house [was taking] her daily sauna and bath." *Ante,* at 2045. In either case, the only conclusions the officers reached concerning the interior of the home were at least as indirect as those that might have ****2049** been inferred from the contents of discarded garbage, see *California v. Greenwood,* 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988), or pen register data, see *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), or, as in this case, subpoenaed utility records, see 190 F.3d 1041, 1043 (C.A.9 1999). For the first time in its history, the Court assumes that an inference can amount to a Fourth Amendment violation. See *ante,* at 2044–2045. [3]

***45** Notwithstanding the implications of today's decision, there is a strong public interest in avoiding constitutional litigation over the monitoring of emissions from homes, and over the inferences drawn from such monitoring. Just as "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public," *Greenwood,* 486 U.S., at 41, 108 S.Ct. 1625, so too public officials should not have to avert their senses or their equipment from detecting emissions in the public domain such as excessive heat, traces of smoke, suspicious odors, odorless gases, airborne particulates, or radioactive emissions, any of which could identify hazards to the community. In my judgment, monitoring such emissions with "sense-enhancing technology," *ante,* at 2043, and drawing useful conclusions from such monitoring, is an entirely reasonable public service.

On the other hand, the countervailing privacy interest is at best trivial. After all, homes generally are insulated to keep heat in, rather than to prevent the detection of heat going out, and it does not seem to me that society will

suffer from a rule requiring the rare homeowner who both intends to engage in uncommon activities that produce extraordinary amounts of heat, and wishes to conceal that production from outsiders, to make sure that the surrounding area is well insulated. Cf. *United States v. Jacobsen,* 466 U.S. 109, 122, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well ***46** justified, that certain facts will not come to the attention of the authorities"). The interest in concealing the heat escaping from one's house pales in significance to "the chief evil against which the wording of the Fourth Amendment is directed," the "physical entry of the home," *United States v. United States Dist. Court for Eastern Dist. of Mich.,* 407 U.S. 297, 313, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972), and it is hard to believe that it is an interest the Framers sought to protect in our Constitution.

Since what was involved in this case was nothing more than drawing inferences from off-the-wall surveillance, rather than any "through-the-wall" surveillance, the officers' conduct did not amount to a search and was perfectly reasonable. [4]

****2050** II

Instead of trying to answer the question whether the use of the thermal imager in this case was even arguably unreasonable, the Court has fashioned a rule that is intended to provide essential guidance for the day when "more sophisticated systems" gain the "ability to 'see' through walls and other opaque barriers." *Ante,* at 2044, and n. 3. The newly minted rule encompasses "obtaining [1] by sense-enhancing technology [2] any information regarding the interior of the home [3] that could not otherwise have been obtained without physical intrusion into a constitutionally protected area ... [4] at least where (as here) the technology in question is not in general public use." *Ante,* at 2043 (internal quotation marks omitted). In my judgment, the ***47** Court's new rule is at once too broad and too narrow, and is not justified by the Court's explanation for its adoption. As I have suggested, I would not erect a constitutional impediment to the use of sense-enhancing technology unless it provides its user with the functional equivalent of actual presence in the area being searched.

Despite the Court's attempt to draw a line that is "not only firm but also bright," *ante,* at 2046, the contours of its new rule are uncertain because its protection apparently dissipates as soon as the relevant technology is "in general public use," *ante,* at 2043. Yet how much use is general public use is not even hinted at by the Court's opinion, which makes the somewhat doubtful assumption that the thermal imager used in this case does not satisfy that criterion. [5] In any event, putting aside its lack of clarity, this criterion is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available.

It is clear, however, that the category of "sense-enhancing technology" covered by the new rule, *ibid.,* is far too broad. It would, for example, embrace potential mechanical substitutes for dogs trained to react when they sniff narcotics. But in *United States v. Place,* 462 U.S. 696, 707, 103 S.Ct. 2637, 77 L.Ed.2d 110 (1983), we held that a dog sniff that "discloses only the presence or absence of narcotics" does "not constitute a 'search' within the meaning of the Fourth Amendment," and it must follow that sense-enhancing equipment that identifies nothing but illegal ***48** activity is not a search either. Nevertheless, the use of such a device would be unconstitutional under the Court's rule, as would the use of other new devices that might detect the odor of deadly bacteria or chemicals for making a new type of high explosive, even if the devices (like the dog sniffs) are "so limited both in the manner in which" they obtain information and "in the content of the information" they reveal. *Ibid.* If nothing more than that sort of information could be obtained by using the devices in a public place to monitor emissions from a house, then their use would be no more objectionable than the use of the thermal imager in this case.

The application of the Court's new rule to "any information regarding the interior of the home," *ante,* at 2043, is also unnecessarily broad. If it takes sensitive equipment to detect an odor that identifies criminal conduct and nothing else, the fact that the odor emanates

from the interior of a **2051 home should not provide it with constitutional protection. See *supra,* at 2050 and this page. The criterion, moreover, is too sweeping in that information "regarding" the interior of a home apparently is not just information obtained through its walls, but also information concerning the outside of the building that could lead to (however many) inferences "regarding" what might be inside. Under that expansive view, I suppose, an officer using an infrared camera to observe a man silently entering the side door of a house at night carrying a pizza might conclude that its interior is now occupied by someone who likes pizza, and by doing so the officer would be guilty of conducting an unconstitutional "search" of the home.

Because the new rule applies to information regarding the "interior" of the home, it is too narrow as well as too broad. Clearly, a rule that is designed to protect individuals from the overly intrusive use of sense-enhancing equipment should not be limited to a home. If such equipment *49 did provide its user with the functional equivalent of access to a private place—such as, for example, the telephone booth involved in *Katz,* or an office building—then the rule should apply to such an area as well as to a home. See *Katz,* 389 U.S., at 351, 88 S.Ct. 507 ("[T]he Fourth Amendment protects people, not places").

The final requirement of the Court's new rule, that the information "could not otherwise have been obtained without physical intrusion into a constitutionally protected area," *ante,* at 2043 (internal quotation marks omitted), also extends too far as the Court applies it. As noted, the Court effectively treats the mental process of analyzing data obtained from external sources as the equivalent of a physical intrusion into the home. See *supra,* at 2048–2049. As I have explained, however, the process of drawing inferences from data in the public domain should not be characterized as a search.

The two reasons advanced by the Court as justifications for the adoption of its new rule are both unpersuasive. First, the Court suggests that its rule is compelled by our holding in *Katz,* because in that case, as in this, the surveillance consisted of nothing more than the monitoring of waves emanating from a private area into the public domain. See *ante,* at 2044. Yet there are critical differences between the cases. In *Katz,* the electronic listening device attached to the outside of the phone booth allowed the officers to pick up the content of the conversation inside the booth, making them the functional equivalent of intruders because they gathered information that was otherwise available only to someone inside the private area; it would be as if, in this case, the thermal imager presented a view of the heat-generating activity inside petitioner's home. By contrast, the thermal imager here disclosed only the relative amounts of heat radiating from the house; it would be as if, in *Katz,* the listening device disclosed only the relative *50 volume of sound leaving the booth, which presumably was discernible in the public domain.[6] Surely, there is a significant difference between the general and well-settled expectation that strangers will not have direct access to the contents of private communications, on the one hand, and the rather theoretical expectation that an occasional homeowner would even care if anybody noticed the relative amounts of heat emanating from the walls of his house, on the other. It is pure hyperbole for the Court to suggest that refusing to extend the holding of *Katz* to this case would leave the homeowner at the mercy of "technology that could discern all human activity in the home." *Ante,* at 2044.

**2052 Second, the Court argues that the permissibility of "through-the-wall surveillance" cannot depend on a distinction between observing "intimate details" such as "the lady of the house [taking] her daily sauna and bath," and noticing only "the nonintimate rug on the vestibule floor" or "objects no smaller than 36 by 36 inches." *Ante,* at 2045–2046. This entire argument assumes, of course, that the thermal imager in this case could or did perform "through-the-wall surveillance" that could identify any detail "that would previously have been unknowable without physical intrusion." *Ante,* at 2046. In fact, the device could not, see n. 1, *supra,* and did not, see Appendix, *infra,* enable its user to identify either the lady of the house, the rug on the vestibule floor, or anything else inside the house, whether smaller or larger than 36 by 36 inches. Indeed, the vague thermal images of petitioner's home that are reproduced in the Appendix were submitted by him to the District Court as part of an expert report raising the question whether the device could even take "accurate, consistent infrared images" of the *51 *outside*

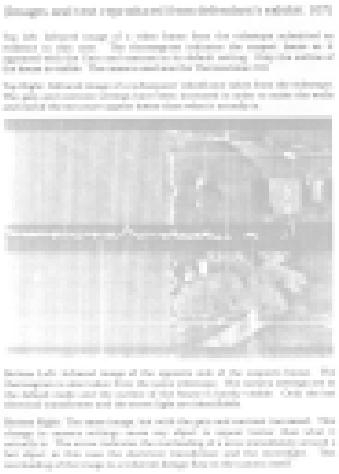
of his house. Defendant's Exh. 107, p. 4. But even if the device could reliably show extraordinary differences in the amounts of heat leaving his home, drawing the inference that there was something suspicious occurring inside the residence—a conclusion that officers far less gifted than Sherlock Holmes would readily draw—does not qualify as "through-the-wall surveillance," much less a Fourth Amendment violation.

III

Although the Court is properly and commendably concerned about the threats to privacy that may flow from advances in the technology available to the law enforcement profession, it has unfortunately failed to heed the tried and true counsel of judicial restraint. Instead of concentrating on the rather mundane issue that is actually presented by the case before it, the Court has endeavored to craft an all-encompassing rule for the future. It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.

I respectfully dissent.

**2053 *52 APPENDIX



All Citations

533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94, 01 Cal. Daily Op. Serv. 4749, 2001 Daily Journal D.A.R. 5879, 14 Fla. L. Weekly Fed. S 329, 2001 DJCAR 2926

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.,* 200 **U.S**. 321, 337, 26 **S.Ct**. 282, 50 L.Ed. 499.

1 When the Fourth Amendment was adopted, as now, to "search" meant "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief." N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed.1989).

2 The dissent's repeated assertion that the thermal imaging did not obtain information regarding the interior of the home, *post,* at 2048 (opinion of STEVENS, J.), is simply inaccurate. A thermal imager reveals the relative heat of various rooms in the home. The dissent may not find that information particularly private or important, see *post,* at 2048, 2049, 2051, but there is no basis for saying it is not information regarding the interior of the home. The dissent's comparison of the thermal imaging to various circumstances in which outside observers might be able to perceive, without technology, the heat of the home—for example, by observing snowmelt on the roof, *post,* at 2048—is quite irrelevant. The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment. The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful. In any event, on the night of January 16, 1992, no outside observer could have discerned the relative heat of **Kyllo's** home without thermal imaging.

3 The ability to "see" through walls and other opaque barriers is a clear, and scientifically feasible, goal of law enforcement research and development. The National Law Enforcement and Corrections Technology Center, a program within the United States Department of Justice, features on its Internet Website projects that include a "Radar–Based Through–the–Wall Surveillance System," "Handheld Ultrasound Through the Wall Surveillance," and a "Radar Flashlight" that "will

enable law enforcement officers to detect individuals through interior building walls." www.nlectc.org/techproj/ (visited May 3, 2001). Some devices may emit low levels of radiation that travel "through-the-wall," but others, such as more sophisticated thermal-imaging devices, are entirely passive, or "off-the-wall" as the dissent puts it.

4 The dissent asserts, *post,* at 2049, n. 3, that we have misunderstood its point, which is not that inference *insulates* a search, but that inference alone is *not* a search. If we misunderstood the point, it was only in a good-faith effort to render the point germane to the case at hand. The issue in this case is not the police's allegedly unlawful inferencing, but their allegedly unlawful thermal-imaging measurement of the emanations from a house. We say such measurement is a search; the dissent says it is not, because an inference is not a search. We took that to mean that, since the technologically enhanced emanations had to be the basis of inferences before anything inside the house could be known, the use of the emanations could not be a search. But the dissent certainly knows better than we what it intends. And if it means only that an inference is not a search, we certainly agree. That has no bearing, however, upon whether hi-tech measurement of emanations from a house is a search.

5 The Government cites our statement in *California v. Ciraolo,* 476 **U.S**. 207, 106 **S.Ct**. 1809, 90 L.Ed.2d 210 (1986), noting apparent agreement with the State of California that aerial surveillance of a house's curtilage could become " 'invasive' " if " 'modern technology' " revealed " 'those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens.' " *Id.,* at 215, n. 3, 106 **S.Ct**. 1809 (quoting Brief for State of California 14–15). We think the Court's focus in this secondhand dictum was not upon intimacy but upon otherwise-imperceptibility, which is precisely the principle we vindicate today.

6 The dissent argues that we have injected potential uncertainty into the constitutional analysis by noting that whether or not the technology is in general public use may be a factor. See *post,* at 2050. That quarrel, however, is not with **us** but with this Court's precedent. See *Ciraolo, supra,* at 215, 106 **S.Ct**. 1809 ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet"). Given that we can quite confidently say that thermal imaging is not "routine," we decline in this case to reexamine that factor.

1 After an evidentiary hearing, the District Court found:

"[T]he use of the thermal imaging device here was not an intrusion into **Kyllo's** home. No intimate details of the home were observed, and there was no intrusion upon the privacy of the individuals within the home. The device used cannot penetrate walls or windows to reveal conversations or human activities. The device recorded only the heat being emitted from the home." Supp.App. to Pet. for Cert. 40.

2 Thus, for example, we have found consistent with the Fourth Amendment, even absent a warrant, the search and seizure of garbage left for collection outside the curtilage of a home, *California v. Greenwood,* 486 **U.S**. 35, 108 **S.Ct**. 1625, 100 L.Ed.2d 30 (1988); the aerial surveillance of a fenced-in backyard from an altitude of 1,000 feet, *California v. Ciraolo,* 476 **U.S**. 207, 106 **S.Ct**. 1809, 90 L.Ed.2d 210 (1986); the aerial observation of a partially exposed interior of a residential greenhouse from 400 feet above, *Florida v. Riley,* 488 **U.S**. 445, 109 **S.Ct**. 693, 102 L.Ed.2d 835 (1989); the aerial photography of an industrial complex from several thousand feet above, *Dow Chemical Co. v. United States,* 476 **U.S**. 227, 106 **S.Ct**. 1819, 90 L.Ed.2d 226 (1986); and the observation of smoke emanating from chimney stacks, *Air Pollution Variance Bd. of Colo. v. Western Alfalfa Corp.,* 416 **U.S**. 861, 94 **S.Ct**. 2114, 40 L.Ed.2d 607 (1974).

3 Although the Court credits **us** with the "novel proposition that inference insulates a search," *ante,* at 2044, our point simply is that an inference cannot *be* a search, contrary to the Court's reasoning. See *supra,* at 2048 and this page. Thus, the Court's use of *United States v. Karo,* 468 **U.S**. 705, 104 **S.Ct**. 3296, 82 L.Ed.2d 530 (1984), to refute a point we do not make underscores the fact that the Court has no real answer (either in logic or in law) to the point we do make. Of course, *Karo* itself does not provide any support for the Court's view that inferences can amount to unconstitutional searches. The illegality in that case was "the monitoring of a beeper in a private residence" to obtain information that "could not have [been] obtained by observation from outside," *id.,* at 714–715, 104 **S.Ct**. 3296, rather than any thought processes that flowed from such monitoring.

4 This view comports with that of all the Courts of Appeals that have resolved the issue. See 190 F.3d 1041 (C.A.9 1999); *United States v. Robinson,* 62 F.3d 1325 (C.A.11 1995) (upholding warrantless use of thermal imager); *United States v. Myers,* 46 F.3d 668 (C.A.7 1995) (same); *United States v. Ishmael,* 48 F.3d 850 (C.A.5 1995) (same); *United States v. Pinson,* 24 F.3d 1056 (C.A.8 1994) (same). But see *United States v. Cusumano,* 67 F.3d 1497 (C.A.10 1995) (warrantless

use of thermal imager violated Fourth Amendment), vacated and decided on other grounds, 83 F.3d 1247 (C.A.10 1996) (en banc).

5 The record describes a device that numbers close to a thousand manufactured units; that has a predecessor numbering in the neighborhood of 4,000 to 5,000 units; that competes with a similar product numbering from 5,000 to 6,000 units; and that is "readily available to the public" for commercial, personal, or law enforcement purposes, and is just an 800–number away from being rented from "half a dozen national companies" by anyone who wants one. App. 18. Since, by virtue of the Court's new rule, the issue is one of first impression, perhaps it should order an evidentiary hearing to determine whether these facts suffice to establish "general public use."

6 The use of the latter device would be constitutional given *Smith v. Maryland,* 442 U.S. 735, 741, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), which upheld the use of pen registers to record numbers dialed on a phone because, unlike "the listening device employed in *Katz* ... pen registers do not acquire the *contents* of communications."

NVIDIA

TITAN

TITAN V

VOLTA DESIGN SPECS GALLERY BUY NOW

NVIDIA TITAN V

NVIDIA's SUPERCOMPUTING GPU ARCHITECTURE, NOW FOR YOUR PC

NVIDIA TITAN V is the most powerful Volta-based graphics card ever created for the PC. NVIDIA's supercomputing GPU architecture is now here for your PC, and fueling breakthroughs in every industry.

$ 2,999.00

ADD TO CART

Free Shipping

Limit 2 per customer

WATCH FULL VIDEO

POWERED BY NVIDIA VOLTA

Volta GPU architecture pairs NVIDIA ® CUDA ® and Tensor Cores to deliver new levels of performance in a desktop PC GPU.

LEARN MORE

STUNNING DESIGN, UNEQUALLED PERFORMANCE

GROUNDBREAKING CAPABILITY

NVIDIA TITAN V has the power of 12 GB HBM2 memory and 640 Tensor Cores, delivering 110 TeraFLOPS of performance. Plus, it features Volta-optimized NVIDIA CUDA for maximum results.

	NVIDIA TITAN V
Architecture	**NVIDIA Volta**
Frame Buffer	**12 GB HBM2**
Boost Clock	**1455 MHz**
Tensor Cores	**640**

NVIDIA

TITAN

VOLTA DESIGN SPECS GALLERY BUY NOW

NVIDIA TITAN users now have free access to GPU-optimized deep learning software on NVIDIA GPU Cloud.

LEARN MORE

GALLERY

NVIDIA

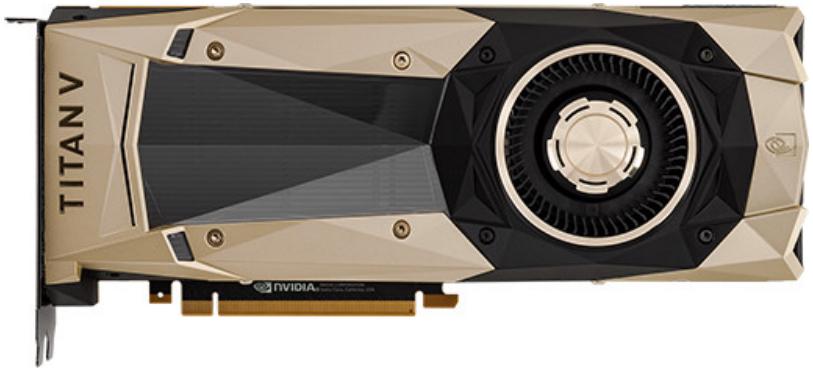
TITAN

VOLTA DESIGN SPECS GALLERY

BUY NOW

SHOP NOW

NVIDIA TITAN V



$ 2,999.00

ADD TO CART

Free Shipping

Limit 2 per customer

Resources

Deep Learning Blogs
AI Newsletter
GPU Technology Conference
Customer Stories
Deep Learning Jobs

UNITED STATES v. CAREY

United States Court of Appeals,Tenth Circuit.

UNITED STATES of America, Plaintiff-Appellee, v. Patrick CAREY, Defendant-Appellant.

No. 98-3077.

Decided: April 14, 1999

Before PORFILIO, McWILLIAMS, and BALDOCK, Circuit Judges.John V. Wachtel, Klenda, Mitchell, Austerman & Zuercher, L.L.C., Wichita, KS, for Defendant-Appellant. Thomas G. Luedke, Assistant United States Attorney (Jackie N. Williams, United States Attorney, with him on the briefs), Topeka, Kansas, for Plaintiff-Appellee.

Patrick J. Carey was charged with one count of possessing a computer hard drive that contained three or more images of child pornography produced with materials shipped in interstate commerce. See 18 U.S.C. § 2252A(a)(5)(B) (1996).[1] Following a conditional plea of guilty, he appeals an order of the district court denying his motion to suppress the material seized from his computer on grounds it was taken as the result of a general, warrantless search. He also contends his sentence was illegal and the district court erred in failing to depart downward from the guideline range, but we do not reach these issues. We conclude the motion to suppress should have been granted and reverse.

I.

Mr. Carey had been under investigation for some time for possible sale and possession of cocaine. Controlled buys had been made from him at his residence, and six weeks after the last purchase, police obtained a warrant to arrest him. During the course of the arrest, officers observed in plain view a “bong,” a device for smoking marijuana, and what appeared to be marijuana in defendant's apartment.

Alerted by these items, a police officer asked Mr. Carey to consent to a search of his apartment. The officer said he would get a search warrant if Mr. Carey refused permission. After considerable discussion with the

officer, Mr. Carey verbally consented to the search and later signed a formal written consent at the police station. Because he was concerned that officers would "trash" his apartment during the search, Mr. Carey gave them instructions on how to find drug related items.

The written consent to search authorized Sergeant William Reece "to have conducted a complete search of the premises and property located at 3225 Canterbury # 10, Manhattan, KS 66503." It further provided, "I do freely and voluntarily consent and agree that any property under my control . may be removed by the officers . if said property shall be essential in the proof of the commission of any crime in violation of the Laws of the United States." Armed with this consent, the officers returned to the apartment that night and discovered quantities of cocaine, marijuana, and hallucinogenic mushrooms. They also discovered and took two computers, which they believed would either be subject to forfeiture or evidence of drug dealing.

The computers were taken to the police station and a warrant was obtained by the officers allowing them to search the files on the computers for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." Detective Lewis and a computer technician searched the contents of the computers, first viewing the directories of both computers' hard drives. They then downloaded onto floppy disks and printed the directories. Included in the directories were numerous files with sexually suggestive titles and the label "JPG." [2] Lewis then inserted the disks into another computer and began searching the files copied from Mr. Carey's computers. His method was to enter key words such as, "money, accounts, people, so forth" into the computer's explorer to find "text-based" files containing those words. This search produced no files "related to drugs."

Undaunted, Detective Lewis continued to explore the directories and encountered some files he "was not familiar with." Unable to view these files on the computer he was using, he downloaded them to a disk which he placed into another computer. He then was "immediately" able to view what he later described as a "JPG file." Upon opening this file, he discovered it contained child pornography.

Detective Lewis downloaded approximately two hundred forty-four JPG or image files. These files were transferred to nineteen disks, only portions of which were viewed to determine that they contained child pornography. Although none of the disks was viewed in its entirety, Detective Lewis looked at "about five to seven" files on each disk. Then, after viewing the contents of the nineteen disks in that fashion, he returned to the computers to pursue his original task of looking for evidence of drug transactions.

Mr. Carey moved to suppress the computer files containing child pornography. During the hearing on the motion, Detective Lewis stated although the discovery of the JPG files was completely inadvertent, when he saw the first picture containing child pornography, he developed probable cause to believe the same kind of material was present on the other image files. When asked why, therefore, he did not obtain a warrant to search the remaining image files for child pornography, he stated, "that question did arise, [a]nd my captain took care of that through the county attorney's office." No warrant was obtained, but the officer nonetheless continued his search because he believed he "had to search these files as well as any other files contained [in the computer]."

Upon further questioning by the government, Detective Lewis retrenched and stated until he opened each file, he really did not know its contents. Thus, he said, he did not believe he was restricted by the search warrant from opening each JPG file. Yet, after viewing a copy of the hard disk directory, the detective admitted there was a "phalanx" of JPG files listed on the directory of the hard drive.[3] He downloaded and viewed these files knowing each of them contained pictures. He claimed, however, "I wasn't conducting a search for child pornography, that happened to be what these turned out to be."

At the close of the hearing, the district court ruled from the bench. Without any findings, the court denied the motion, saying: "[a]t this point, the Court feels that the . Defendant's Motion to Suppress . would be-should be denied. And that will be the order of the Court, realizing that they are close questions." No subsequent written order containing findings of fact or conclusions of law was filed.

II.

We review the denial of a motion to suppress for clear error. See United States v. Griffin, 7 F.3d 1512, 1516 (10th Cir.1993). Reasonableness of a search is reviewed de novo. See United States v. Eylicio-Montoya, 18 F.3d 845, 848 (10th Cir.1994). Mr. Carey complains: (1) search of the computers exceeded the scope of the warrant, (2) he did not consent to the search of his apartment, and (3) seizure of the computers was unlawful because the officers lacked probable cause. We address only the first issue.

Mr. Carey argues the search of the computers transformed the warrant into a "general warrant" and resulted in a general and illegal search of the computers and their files. The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings. See Marron v. United States, 275 U.S. 192, 196, 48 S.Ct. 74, 76, 72 L.Ed. 231 (1927) ("The requirement that warrants shall particularly describe things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is to be left to the discretion of the officer executing the warrant."). As we have instructed:

The essential inquiry when faced with challenges under the Fourth Amendment is whether the search or seizure was reasonable-reasonableness is analyzed in light of what was reasonable at the time of the Fourth Amendment's adoption. It is axiomatic that the 4th Amendment was adopted as a directed response to the evils of the general warrants in England and the writs of assistance in the Colonies.

O'Rourke v. City of Norman, 875 F.2d 1465, 1472 (10th Cir.1989) (citations omitted).

Mr. Carey argues that examined against history and case law, the search constituted general rummaging in "flagrant disregard" for the terms of the warrant and in violation of the Fourth Amendment. United States v. Foster, 100 F.3d 846, 849-50 (10th Cir.1996). Despite the specificity of the search warrant, files not pertaining to the sale or distribution of controlled substances were opened and searched, and according to Mr. Carey, these files should have been suppressed. See id. at 849.

The government responds that the plain view doctrine authorized the police search. See Coolidge v. New Hampshire, 403 U.S. 443, 465, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). A police officer may properly seize evidence of a crime without a warrant if:

(1) the officer was lawfully in a position from which to view the object seized in plain view; (2) the object's incriminating character was immediately apparent-i.e., the officer had probable cause to believe the object was contraband or evidence of a crime; and (3) the officer had a lawful right of access to the object itself.

United States v. Soussi, 29 F.3d 565, 570 (10th Cir.1994) (citing Horton v. California, 496 U.S. 128, 134, 110 S.Ct. 2301, 2307, 110 L.Ed.2d 112 (1990)).

According to the government, "a computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet, pursuant to a valid search warrant, and instead finding child pornography." Just as if officers has seized pornographic photographs from a file cabinet, seizure of the

pornographic computer images was permissible because officers had a valid warrant, the pornographic images were in plain view, and the incriminating nature was readily apparent as the photographs depicted children under the age of twelve engaged in sexual acts. The warrant authorized the officer to search any file because "any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information." See Erickson v. Commissioner of Internal Revenue, 937 F.2d 1548, 1554 (10th Cir.1991) (drug trafficking activity is often concealed or masked by deceptive records). Further, the government states the defendant's consent to search of the apartment overrides all of these questions because it extended to the search of every file on both computers.

The Supreme Court has instructed, "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." Coolidge, 403 U.S. at 466, 91 S.Ct. 2022. The warrant obtained for the specific purpose of searching defendant's computers permitted only the search of the computer files for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." The scope of the search was thus circumscribed to evidence pertaining to drug trafficking. The government's argument the files were in plain view is unavailing because it is the contents of the files and not the files themselves which were seized. Detective Lewis could not at first distinguish between the text files and the JPG files upon which he did an unsuccessful word search. Indeed, he had to open the first JPG file and examine its contents to determine what the file contained. Thus, until he opened the first JPG file, he stated he did not suspect he would find child pornography. At best, he says he suspected the files might contain pictures of some activity relating to drug dealing.

In his own words, however, his suspicions changed immediately upon opening the first JPG file. After viewing the contents of the first file, he then had "probable cause" to believe the remaining JPG files contained similar erotic material. Thus, because of the officer's own admission, it is plainly evident each time he opened a subsequent JPG file, he expected to find child pornography and not material related to drugs. Armed with this knowledge, he still continued to open every JPG file to confirm his expectations. Under these circumstances, we cannot say the contents of each of those files were inadvertently discovered. Moreover, Detective Lewis made clear as he opened each of the JPG files he was not looking for evidence of drug trafficking. He had temporarily abandoned that search to look for more child pornography, and only "went back" to searching for drug-related documents after conducting a five hour search of the child pornography files.

We infer from his testimony Detective Lewis knew he was expanding the scope of his search when he sought to open the JPG files. Moreover, at that point, he was in the same position as the officers had been when they first wanted to search the contents of the computers for drug related evidence. They were aware they had to obtain a search warrant and did so. These circumstances suggest Detective Lewis knew clearly he was acting without judicial authority when he abandoned his search for evidence of drug dealing.

Although the question of what constitutes "plain view" in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, we do not need to reach it here. Judging this case only by its own facts, we conclude the items seized were not authorized by the warrant. Further, they were in closed files and thus not in plain view.[4]

We do note the recent decision in United States v. Turner, 169 F.3d 84, 1999 WL 90209 (1st Cir. Feb.26, 1999) [5] affirming the district court's suppression of several images of child pornography found on the defendant's computer. In Turner, the defendant's neighbor was the victim of a nighttime assault in her apartment, and

police officers obtained the defendant's consent to search his apartment for signs of the intruder and for evidence of the assault itself. While searching the apartment, an officer noticed the defendant's computer screen suddenly illuminate with a photograph of a nude woman resembling the assault victim. He then sat at the computer and itemized the files most recently accessed. Several of the files had the "suffix '.jpg,' denoting a file containing a photograph." Id. at 86. The officer opened these files and found photographs of nude blonde women in bondage. After calling the district attorney's office for guidance, the officer copied these adult pornography files onto a floppy disk and then searched the computer hard drive for other incriminating files. He opened a folder labeled "G-Images" and "noted several files with names such as 'young' and 'young with breasts.' " Id. After opening one of these files and observing child pornography, the officer shut down and seized the computer, and the defendant was charged in a single count of possessing child pornography. The government contended the "consent was so broad-authorizing search of all [the defendant's] 'personal property' that it necessarily encompassed a comprehensive search of his computer files." Id. But the First Circuit affirmed the suppression of the computer files on grounds "the consent did not authorize the search of the computer" because "an objectively reasonable person assessing in context the exchange between [the defendant] and these detectives would have understood that the police intended to search only in places where an intruder hastily might have disposed of any physical evidence of the . assault .." Id. at 88. The court also held:

We cannot accept the government's contention that the sexually suggestive image which suddenly came into "plain view" on the computer screen rendered [the defendant]'s computer files "fair game" under a consensual search simply because the [neighbor's] assault had a sexual component. The critical consideration in this regard is that the detectives never announced, before [the defendant] gave his consent, that they were investigating a sexual assault or attempted rape.

Id.

As in Turner, the government argues here the consent Mr. Carey gave to the search of his apartment carried over to the contents of his computer files. We disagree. The arresting officer sought permission to search only the "premises and property located at 3225 Canterbury # 10." Thus, the scope of the consensual search was confined to the apartment itself. The seizure of the computer was permitted by Mr. Carey's consent "that any property under my control . may be removed by the officers . if said property shall be essential in the proof of the commission of any crime." This agreement, by its own terms, did not permit the officer to open the files contained in the computer, a fact he obviously recognized because he obtained a proper warrant to search for drug related evidence before he began opening files.

The warrant constrained the officer to search for items it listed. See United States v. Reyes, 798 F.2d 380, 383 (10th Cir.1986). In our judgment, the case turns upon the fact that each of the files containing pornographic material was labeled "JPG" and most featured a sexually suggestive title. Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware-in advance of opening the remaining files-what the label meant. When he opened the subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant, just like the officer in Turner knew he was not going to find evidence of an assault as authorized by the consent.

At oral argument the government suggested this situation is similar to an officer having a warrant to search a file cabinet containing many drawers. Although each drawer is labeled, he had to open a drawer to find out whether the label was misleading and the drawer contained the objects of the search. While the scenario is likely, it is not representative of the facts of this case. This is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer

before discovering its contents. Even if we employ the file cabinet theory, the testimony of Detective Lewis makes the analogy inapposite because he stated he knew, or at least had probable cause to know, each drawer was properly labeled and its contents were clearly described in the label.

Further, because this case involves images stored in a computer, the file cabinet analogy may be inadequate. "Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information." Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994). Relying on analogies to closed containers or file cabinets may lead courts to "oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage." Id. Alternatively, courts can acknowledge computers often contain "intermingled documents." See United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir.1982).6 Under this approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. See id. at 596.7 The magistrate should then require officers to specify in a warrant which type of files are sought.8

Because in Mr. Carey's case, officers had removed the computers from his control, there was no "exigent circumstance or practical reason to permit officers to rummage through all of the stored data regardless of its relevance or its relation to the information specified in the warrant." Winick, 8 Harv. J.L. & Tech. at 105.9 With the computers and data in their custody, law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory. See id. at 107. In this case, Detective Lewis and the computer technician did list files on the directory and also performed a key word search, but they did not use the information gained to limit their search to items specified in the warrant, nor did they obtain a new warrant authorizing a search for child pornography.

III.

We must conclude Detective Lewis exceeded the scope of the warrant in this case. His seizure of the evidence upon which the charge of conviction was based was a consequence of an unconstitutional general search, and the district court erred by refusing to suppress it. Having reached that conclusion, however, we are quick to note these results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result.10

Although other errors have been raised, we do not reach them because of our conclusion the seizure of evidence was beyond the scope of the warrant. We specifically do not reach the issue of whether Mr. Carey voluntarily consented to the search of his apartment. The district court made no findings on this question, and we are not wont to opine on what would be an immaterial point in this appeal.

REVERSED and REMANDED for further proceedings in accordance with this opinion.

I join in the court's opinion, but write separately to emphasize that the questions presented in this case are extremely close calls and, in my opinion, are totally fact driven.

First, absent Detective Lewis' testimony, I would not suppress the evidence. "The plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." Coolidge v. New Hampshire, 403 U.S. 443, 466, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). In light of

Detective Lewis' testimony, just this sort of impermissible general rummaging occurred in this case. The detective's testimony makes clear that from the time he found the first image of child pornography, he switched from his authorized search for drug-related evidence to another subject-child pornography. At this point, the detective should have ceased his search and obtained a warrant to search the computer files for evidence of child pornography. As Detective Lewis testified, it was clear to him that after he discovered the first image, he had probable cause to believe the computer contained additional images of child pornography, and no exigent circumstances existed because the computer had been removed to the police station.

In contrast, if the record showed that Detective Lewis had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, I think a different result would be required. That is not what happened here, however.

Second, while agreeing with the majority that Defendant's consent to the search of his apartment did not carry over to his computer hard drive, I write separately to explain why I think the scope of Defendant's consent is limited to evidence of drug-related activity. The scope of a consensual search is "generally defined by its expressed object." Florida v. Jimeno, 500 U.S. 248, 251, 111 S.Ct. 1801, 114 L.Ed.2d 297 (1991). To determine the breadth of the consent given by Mr. Carey, we consider what "the typical reasonable person would have understood by the exchange between the officer and the [defendant]." United States v. Elliott, 107 F.3d 810, 815 (10th Cir.1997). Resolution of this issue requires a detailed inquiry into the facts.

The waiver signed by Defendant granted the officers permission to search the "premises and property located at 3255 Canterbury # 10" and authorized the officers to remove any property "if said property shall be essential in the proof of the commission of any crime." The officer testified that after he arrested Defendant, he told him that "based on what I had just observed in his apartment that I was going to apply for a search warrant." The officer had just found, in plain view, a bong typically used for smoking marijuana and a small quantity of what appeared to be marijuana. The officer then explained to Defendant that he could consent to a search instead of the officer obtaining a warrant. Defendant told the officer he was unsure. En route to the police station, Defendant asked several questions about the search. Upon arrival at the station, Defendant indicated that he wished to consent. He also told the officer where he would find additional drugs, a scale, a firearm and cash. In addition, Defendant told him where he would find a pornographic videotape. The officer responded that he "couldn't care less about his pornographic videotapes" and "that wasn't of concern to me."

In light of the officer's conversations with Defendant, a reasonable person would conclude that the statements by the officer limited the scope of the request to drugs and drug-related items in the apartment. See Elliott, 107 F.3d at 815; see also, United States v. Dichiarinte, 445 F.2d 126, 129 (7th Cir.1971) (consent to search after officers repeated references to narcotics did not grant officers a license to conduct a general exploratory search). As in United States v. Turner, 169 F.3d 84 (1st Cir.1999), the Defendant's consent did not include permission to search the hard drive of Defendant's computer for pornographic or any other type of files, a fact, as the majority points out, the officer recognized because he obtained a proper warrant to search for drug-related evidence before he began opening computer files. Thus, I think the record supports a finding that Defendant's consent did not extend to a search for pornographic material on the hard drive of his computer. Of course, the officer's search of the computer hard drive for "evidence pertaining to the sale and distribution of controlled substances" was lawful, in that the officer obtained a valid search warrant to do so.

ORDER ON PETITION FOR REHEARING

April 30, 1999.

This matter is before the court on the government's petition for rehearing by the panel. Because the government contends we failed to properly follow Horton v. California, 496 U.S. 128, 130 (1990), we recognize inadvertance is not a Fourth Amendment requirement. We note, however, "inadvertance is a characteristic of most legitimate 'plain-view' seizures." Id. As such, the fact that Detective Lewis did not inadvertently come across the pornographic files is certainly relevant to our inquiry. Our holding is based, however, on the fact that Detective Lewis impermissibly expanded the scope of his search when he abandoned the search for drug-related evidence to search for evidence of child pornography. The petition for rehearing is denied.

FOOTNOTES

1. As amended in 1998, the statute now applies to any person who knowingly possesses a computer disk "that contains an image of child pornography" produced with materials shipped in interstate commerce. See 18 U.S.C. § 2252A(a)(5)(B) (1998). Because Mr. Carey was charged on August 6, 1997, the 1996 version of the statute applies in this case.

2. Detective Lewis later testified at the time he discovered the first JPG or image file, he did not know what it was nor had he ever experienced an occasion in which the label "JPG" was used by drug dealers to disguise text files. He stated, however, image files could contain evidence pertinent to a drug investigation such as pictures of "a hydroponic growth system and how it's set up to operate."

3. We note the JPG files shown on Detective Lewis' directory printout featured sexually suggestive or obscene names, many including the word "teen" or "young." The detective testified drug dealers often obscure or disguise evidence of their drug activity.

4. Given the officer's testimony that he inadvertently discovered the first image during his search for documents relating to drug activity, our holding is confined to the subsequent opening of numerous files the officer knew, or at least expected, would contain images of child pornography.

5. See also United States v. Maxwell, 45 M.J. 406, 422 (U.S. Armed Forces 1996) (Where a colonel used a personal computer to transport obscenity and child pornography, the plain view doctrine did not apply to the search of computer files under a screen name not listed in the warrant. Because the warrant did not authorize search of those files, view was obtained as a result of improper governmental opening, not as a result of seeing what was legitimately in plain view.). Cf. United States v. Abbell, 914 F.Supp. 519, 520-21 (S.D.Fla.1995) (In a criminal prosecution where a large volume of computer generated data was seized from the defendant's law office, a special master would determine whether documents and data were responsive to the search warrant or fell within an exception to the search warrant requirement such as the plain view doctrine.).

6. United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir.1982), held seizure of all of a corporation's documents during a relevant time period, rather than limiting seizure to categories of documents described in a search warrant, was unreasonable despite the government's contention irrelevant documents were intermingled with described documents. Although this case did not arise in the context of a computer search, we find the concept of "intermingled documents" helpful here.

7. The government contends Mr. Carey would have been "equally guilty had he possessed this material in the form of a book, a magazine, or a film." And in United States v. Reyes, 798 F.2d 380, 383 (10th Cir.1986), we explained "in the age of modern technology and the commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take" because drug records might be found in cassettes, leases and accounts cards, or cancelled checks. We have stated our belief that the storage capacity of computers requires a special approach, and we do not intend to comment on

the particularity requirement as it applies to all contemporary media. Rather, our discussion applies specifically to searches of files of computers held in law enforcement custody.

8. See Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 108 (1994) ("Computer programs store information in a wide variety of formats. For example, most financial spreadsheets store information in a completely different format than do word processing programs. Similarly, an investigator reasonably familiar with computers should be able to distinguish database programs, electronic mail files, telephone lists and stored visual or audio files from each other. Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought. Where relying on the type of computer files fails to narrow the scope of the search sufficiently, the magistrate should review the search methods proposed by the investigating officers."); see also Tamura, 694 F.2d at 596 n. 4. ("[w]e recently approved a procedure whereby law enforcement officers bring in lay experts as consultants to facilitate the on-site search for documents containing complex or technical subject matter") (citations omitted).

9. Cf. United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir.1997) ("Although we are given pause by the wholesale seizure of file cabinets and miscellaneous papers and property not specified in the search warrant, the officers' conduct did not grossly exceed the scope of the warrant. Their conduct was motivated by the impracticability of on-site sorting and the time constraints of executing a daytime search warrant. The officers were authorized to seize ten broad categories of records, and those records were present in every drawer of both file cabinets. No item not specified in the warrant was admitted against [the defendant] at trial. Under these circumstances the officers did not grossly exceed the warrant in concluding they did not need to examine at the site every piece of paper in both cabinets.") (emphasis added).

10. Cf. United States v. Hall, 142 F.3d 988, 993-94 (7th Cir.1998) (Viewing images of child pornography on the defendant's computer by a repair company employee was a private search. Although a police officer then improperly copied the files to a floppy disk without a warrant, a subsequent search of the computer files by the police officer did not require suppression because the employee's statements provided an independent basis for the warrant.).

PORFILIO, Circuit Judge.

237 Fed.Appx. 949
This case was not selected for
publication in the Federal Reporter.
Not for Publication in West's Federal Reporter
See Fed. Rule of Appellate Procedure 32.1
generally governing citation of judicial decisions
issued on or after Jan. 1, **2007**. See also
Fifth Circuit Rules 28.7, 47.5.3, 47.5.4.
(Find CTA5 Rule 28 and Find CTA5 Rule 47)
United States Court of Appeals,
Fifth Circuit.

UNITED STATES of America, Plaintiff-Appellee
v.
Roland Allen **CAMPOS**, Defendant-Appellant.

No. 06-50594.
|
July 17, **2007**.

Synopsis

Background: After his motion to suppress evidence was denied, defendant pled guilty in the United States District Court For the Western District of Texas, Austin Division, to conspiracy to possess cocaine with intent to distribute and possession of cocaine with intent to distribute. Defendant appealed.

Holdings: The Court of Appeals held that:

[1] officer did not exceed scope of lawful traffic stop;

[2] drug dog's positive alert to drugs established probable cause to search van; and

[3] defendant was not entitled to appointment of canine expert; and

[4] defendant was not entitled to continuance for purpose of discovery of evidence concerning dog.

Affirmed.

West Headnotes (4)

[1] Automobiles
Inquiry;License, Registration, or Warrant Checks

That it took officer eight minutes to run records check of defendant's vehicle and driver's license did not exceed scope of lawful traffic stop under *Terry*; defendant's inconsistent statements regarding his travel itinerary, the lack of a valid driver's license, the discovery of $2,000 in cash on defendant's person, and defendant's inability or unwillingness to identify the name of the owner of the van all created suspicion, necessitating further detective efforts by officer. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[2] Controlled Substances
Odor Detection;Use of Dogs

Positive canine alert to drugs inside vehicle was reliable as to afford officer sufficient probable cause to seize and search the van; drug dog's trainer and handler and the dog successfully completed all standard training procedures, dog was certified to detect a variety of narcotics, including cocaine, and, at trial, all but one of the dog's possible previous false alerts were reasonably explained by officer. U.S.C.A. Const.Amend. 4.

3 Cases that cite this headnote

[3] Costs
Expert Witnesses or Assistance in General

Defendant was not entitled to appointment of canine-alert expert without informing district court of requested expert's name, statement of expected expenses, and explanation of what a canine-alert expert was and how one

became such an expert, in prosecution for drug trafficking. 18 U.S.C.A. § 3006A(e)(1).

2 Cases that cite this headnote

[4] **Criminal Law**
Materiality of Evidence in Prosecution for Other Crimes in General

Criminal Law
In Procuring Documentary Evidence

Defendant was not entitled to continuance for purpose of extending discovery concerning drug dog's reliability, in drug trafficking prosecution, where standing discovery order did not require government to produce requested documents, defendant made no discovery requests for documents until the day before the suppression hearing, and evidence at the suppression hearing clearly demonstrated dog's reliability such that any evidence presented by expert would not have affected the finding of dog's reliability.

1 Cases that cite this headnote

Attorneys and Law Firms

***950** Joseph H. Gay, Jr., Assistant **U.S**. Attorney, **U.S**. Attorney's Office, Western District of Texas, San Antonio, TX, for Plaintiff-Appellee.

Joseph Andrew Turner, Law Office of Joseph A. Turner, Austin, TX, for Defendant-Appellant.

Appeal from the United States District Court For the Western District of Texas, Austin Division, 1:05-CR-00246.

Before HIGGINBOTHAM, DAVIS and BARKSDALE, Circuit Judges.

Opinion

PER CURIAM: *

****1** Defendant Roland Allen **Campos** ("**Campos**") appeals his conviction for conspiracy to possess cocaine with intent to distribute ***951** and possession of cocaine with intent to distribute, in violation of 21 U.S.C. §§ 841(a)(1) and 846. **Campos** argues that the district court erred in denying his motion to suppress evidence discovered in a search of the vehicle in which he was traveling, and in denying his application for authorization of expert services and motion for continuance. We AFFIRM.

I. Background

On November 16, 2005, Appellant, Roland Allen **Campos** ("**Campos**"), and a passenger were driving north on I-35 in Round Rock, Texas in a white van. Officers Martin Flores ("Flores") and Eric Mount ("Mount"), both members of the Round Rock Police Department, were patrolling I-35 in separate vehicles. Officer Flores received a call from Officer Mount informing him that Officer Mount observed a red Neon and a white van traveling close together. Officer Mount had already stopped the Neon for failing to maintain an appropriate distance, and wanted Officer Flores to stop the van.

Officer Flores then followed the van, and, after observing **Campos** traveling 69 mph in a 65 mph zone, Officer Flores pulled **Campos** over. **Campos** exited the vehicle. Officer Flores approached the vehicle and asked **Campos** for his driver's license, but **Campos** only produced a Texas identification card. Flores then began to ask **Campos** about his travel plans. **Campos** replied that he was traveling from San Antonio to College Station to buy tickets for the University of Texas versus Texas A & M football game. This was suspicious to Officer Flores because **Campos** had already passed three highways between San Antonio and Round Rock that would have led to College Station.

Next, Officer Flores asked **Campos** for the name of his passenger, but **Campos** had trouble recalling the passenger's name. Officer Flores also asked **Campos** about the owner of the vehicle. Although **Campos** stated that it belonged to his uncle, **Campos's** only response when questioned about his uncle's name was that it was listed on the vehicle's registration. **Campos's** inconsistent

statements made Officer Flores suspicious that Campos was providing false information.

Campos then consented to a pat-down search, in which Officer Flores discovered $2,000 in cash in Campos's pocket. At this time, Campos continued to make inconsistent statements. Campos stated that he was going through Houston to get to College Station, which only added to Officer Flores's suspicions because Campos was traveling away from Houston. In addition, although Campos indicated that he planned on stopping at a rest area to look at a map, Campos passed a rest area less than a mile earlier. Moreover, Campos admitted that he never had a driver's license and he was unable to provide Officer Flores with proof of insurance.

Officer Flores then questioned Campos's passenger, Joe Gomez ("Gomez"). Unlike Campos, Gomez stated that they were heading to Waco, not College Station. Importantly, despite Officer Mount's suggestion that Campos and Gomez were traveling in tandem with the Neon, Gomez told Officer Flores that he and Campos were traveling alone. Based on the inconsistent responses provided by Campos and Gomez, Officer Flores concluded that Campos and Gomez were not traveling to College Station to buy tickets.

**2 Officer Flores then began records checks on Campos and Gomez. At this point, eight minutes had passed since the initial stop. While awaiting the results of the records checks, Officer Flores asked Campos if he had any dope or other illegal drugs in the vehicle, and Campos responded *952 in the negative. Officer Flores then obtained Campos's consent to search the van. During the search, Officer Flores noticed that the bolts holding in both front seats had scratch marks, which, based on his experience as a police officer, [2] indicated that the van was being used for drug trafficking.

Officer Flores learned from Officer Mount that one of the occupants of the Neon lived on the same street as Gomez and that the Neon's driver stated that they were heading to Dallas, not College Station. When Officer Flores confronted Gomez and Campos, they admitted they were traveling with the Neon. Campos explained that they were traveling in separate cars because his friend wanted to drive his own car. However, Officer Flores knew that the Neon was a rental car. During this time, Officer Flores received the return on the records checks, which reported that Joe Campos, a/k/a Roland A. Campos, was wanted for a parole violation.

Officer Flores then told Campos that he believed Campos was engaged in illegal activity. Campos continued to deny any wrongdoing. Although, at this point, Officer Flores testified that he believed he had probable cause to undertake a search, Officer Flores, a certified narcotics-canine handler, decided to use his canine, Tessa, to conduct a dog sniff search. Tessa alerted when entering the rear passenger door and driver's side door of the vehicle. Officer Flores then had the van taken to an auto shop for a more thorough search, where officials located a compartment containing several black bundles of cocaine, weighing 30.08 kilograms, on the underside of the van behind the van's heat shield.

Campos was subsequently indicted for conspiring to possess cocaine with intent to deliver and possessing cocaine with intent to deliver, in violation of 21 U.S.C. §§ 841(a)(1) and 846. Campos moved unsuccessfully to suppress the cocaine discovered during the search of the van. Thereafter, Campos entered a conditional guilty plea, reserving his right to appeal the district court's denial of his motion to suppress.

Campos timely filed a notice of appeal.

II. Discussion

Campos raises three arguments on appeal. He argues that the district court erred by (1) failing to suppress the evidence found in the search of the vehicle; (2) denying his application for authorization of expert services; and (3) denying his motion for continuance. We will address these issues in turn.

A. Suppression of Evidence

When reviewing the denial of a motion to suppress, we review findings of fact for clear error and conclusions of

law de novo.[3] We construe all facts in the light most favorable to the government as the prevailing party.[4]

**3 Campos argues that the cocaine discovered during the search of the van should be suppressed because Officer Flores (1) purposefully delayed running the records checks; and (2) did not have probable cause to search the van because the drug dog was unreliable.

1. Reasonableness of Detention

[1] We evaluate the legality of a traffic stop under *Terry v. Ohio*[5].[6] In determining *953 whether a seizure has exceeded the scope of a permissible *Terry* stop, we undertakes a dual inquiry: (1) whether the officer's action was justified at its inception; and (2) whether it was reasonably related in scope to the circumstances that justified the interference in the first place.[7]

Although in the district court Campos challenged the validity of the initial traffic stop, he no longer argues that the stop of his vehicle for speeding was improper. Rather, Campos argues that the stop was unlawfully prolonged because Officer Flores did not run the records checks until eight minutes into the stop, rendering his detention unreasonable under the Fourth Amendment.

Officer Flores's actions are plainly permissible under our case law. An officer may request a driver's license, insurance papers, vehicle registration, run a computer check, issue a citation, and ask about the purpose and itinerary of a driver's trip.[8] An officer may also undertake similar questioning of the vehicle's occupants to verify the information provided by the driver.[9] In addition, we have specifically held that records checks need not be initiated prior to an officer's initial questioning of a vehicle's occupants.[10]

In *United States v. Brigham,* the officer did not initiate records checks until eight minutes into the initial stop. Prior to running the records checks, the officer asked the driver for his license, insurance papers, questioned him about his travel plans, and sought to verify the driver's story with the car's three passengers. We concluded that the officer's actions were reasonable.

Campos argues that his case is distinguishable from *Brigham* because Officer Flores's testimony indicates that he purposefully engages in delays in initiating records checks so as to extend the amount of time he has for investigation. We reject this argument. "[T]he touchstone of Fourth Amendment analysis is reasonableness," and "[r]easonableness is measured in *objective* terms by examining the totality of the circumstances."[11] Therefore, as long as Officer Flores's investigative methods were objectively reasonable, his subjective motives are irrelevant.[12]

We agree with the district court that Officer Flores's investigative methods were reasonable. Prior to running the records checks, it was permissible for Officer Flores to request Campos's license, conduct a pat-down search of Campos, and question Campos and Gomez about their travel plans.[13] This process required as long as it did for reasons beyond Officer Flores's control.[14] Campos's and Gomez's inconsistent statements regarding their *954 travel itinerary, Campos's lack of a valid driver's license, the discovery of $2,000 in cash on Campos's person, and Campos's inability or unwillingness to identify the name of the owner of the van all created suspicion, necessitating further detective efforts by Officer Flores. In this case, Officer Flores's questioning "exemplified a graduated response to emerging facts."[15]

**4 Because Officer Flores's actions were not unreasonable under the circumstances of this case, the detention of Campos did not violate the Fourth Amendment.

2. Reliability of Drug Dog

[2] Campos argues that Tessa, the drug dog, was unreliable, and thus, Officer Flores did not have probable cause to search and seize the van.[16] After a thorough review of the testimony and evidence before it, the district court found the canine alert to be reliable and concluded

that Officer Flores had sufficient probable cause to seize and search the van.

As Campos concedes, the positive alert of a properly trained drug detecting dog, standing alone, provides probable cause to support a search and seizure.[17] It is undisputed that Officer Flores, Tessa's trainer and handler for nearly two years, and Tessa successfully completed all standard training procedures and that Tessa was certified to detect a variety of narcotics, including cocaine. However, Campos argues that Officer Flores gave subtle "handler cues"[18] to Tessa. According to Campos, the videotape of the incident, which was admitted into evidence, reveals that Officer Flores was not neutral in his handling of Tessa because, even after Tessa seemingly failed three times to alert, Officer Flores took Tessa to the other side of the van to make another attempt at alerting, and when Tessa sat down, Officer Flores exclaimed, "Oh, yeah!" In addition, Campos maintains that Officer Flores is not credible because he testified that Tessa had never made a false positive alert, and Campos subsequently offered evidence showing that Tessa had made three false alerts.

Contrary to Campos's arguments, the district court found that Tessa was reliable. In particular, the district court found that all but one of the possible false alerts by Tessa were reasonably explained away by Officer Flores. In addition, the district court made a determination that Officer Flores was credible, which we will not disturb.[19] Moreover, the district court determined that the videotape demonstrated that Tessa's repeated entries into the van were not merely redundant, and thus, rejected Campos's suggestion that the dog was being cajoled into an alert.

We find no clear error in the district court's factual finding that the canine alert was reliable and therefore uphold the district court's ultimate conclusion that Officer Flores had probable cause to seize and search the van.

***955** B. Application for Authorization of Expert Services

[3] Campos argues that the district court erred in not granting his request under 18 U.S.C. § 3006A(e)(1) for a canine-alert expert. We review the district court's denial of an application for authorization of expert services for abuse of discretion.[20]

On January 31, 2006, Campos filed an application for authorization of the services of a canine-alert expert. On February 3, 2006, the district court denied Campos's application without prejudice to refile his application with the expert's name, a statement of the expected expenses, and information explaining what is a canine-alert expert and how one becomes such an expert. Instead of promptly filing an amended application in compliance with the district court's instructions, Campos waited until February 9, 2006, the day before the suppression hearing (which was set in the January 13, 2006 pre-trial order), to file his amended application. As a result, the district court denied Campos's application as untimely.

****5** Campos alleges that the district court improperly required him to provide information not called for by the statute. Section 3006A(e)(1) provides:

> Counsel for a person who is financially unable to obtain investigative, expert, or other services necessary for adequate representation may request them in an ex parte application. Upon finding, after *appropriate inquiry* in an ex parte proceeding, that the services are necessary and that the person is financially unable to obtain them, the court ... shall authorize counsel to obtain the services [at government expense].[21]

The statute does not define the scope of an "appropriate inquiry" and Campos offers no authority limiting what a district court may request in order to make such an inquiry. Moreover, we have held that "[t]o justify authorization ... under § 3006A(e)(1), a defendant must demonstrate with *specificity,* the reasons why such services are required."[22]

In determining whether the services of a canine-alert expert were necessary, the district court's denial of

Campos's first application and request that Campos provide the above-mentioned information was certainly reasonable.[23] Without such specific information, the district court could not adequately appraise Campos's need for expert services.

In addition, the district court did not abuse its discretion in denying Campos's second application as untimely.[24]

C. Motion for Continuance

[4] Campos argues that the district court erred in denying his motion for continuance. We review the denial of a defendant's motion for continuance for an abuse of discretion resulting in serious prejudice.[25]

Three days before the February 10, 2006, suppression hearing, Campos filed *956 his motion for continuance, alleging that he was not able to complete discovery because records concerning Tessa had not been provided. According to Campos, he made the motion as soon as he became aware that the government did not provide any field-performance or training logs of Tessa. However, the standing discovery order, which was filed in this case on January 13, 2006, did not require the government to produce such documents,[26] and Campos made no discovery complaints for these documents until the day before the suppression hearing.

Campos contends that the denial of his motion prejudiced him because it was essential for him to provide Tessa's training and field logs to his canine-alert expert so that such expert could assess the reliability of Tessa's alert. We reject this contention. Assuming *arguendo* that a defendant can challenge the reliability of a canine alert, once the requested documents were produced, Campos was able to cross-examine Officer Flores regarding the contents of Tessa's field performance records. Furthermore, evidence at the suppression hearing clearly demonstrated Tessa's reliability such that any evidence presented by Campos's expert would not have affected the finding of reliability.[27] Moreover, since the district court subsequently denied Campos's application for authorization of expert services, Campos's argument that he needed the records for such expert is unpersuasive.

**6 The district court's decision to deny Campos's motion for continuance was not an abuse of discretion.

III. Conclusion

For the foregoing reasons, we AFFIRM the district court's judgment.

AFFIRMED.

All Citations

237 Fed.Appx. 949, 2007 WL 2083661

Footnotes

* Pursuant to 5TH CIR. R. 47.5, the Court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5TH CIR. R. 47.5.4.

2 Officer Flores performed hundreds of traffic stops in which drug trafficking was involved, and had found narcotics on previous occasions when there was evidence that someone tampered with seat bolts.

3 *United States v. Gonzalez,* 328 F.3d 755, 758 (5th Cir.2003).

4 *Gonzalez,* 328 F.3d at 758.

5 392 U.S. 1, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968).

6 *United States v. Jenson,* 462 F.3d 399, 403 (5th Cir.2006).

7 *United States v. Brigham,* 382 F.3d 500, 506 (5th Cir.2004) (en banc).

8 *Id.* at 508 (citation omitted); *United States v. Shabazz,* 993 F.2d 431, 437 (5th Cir.1993) (citation omitted).

9 *Brigham,* 382 F.3d at 508 (citation omitted).

10 *Id.* at 510-11.

11 *Id.* at 507 (citations and internal quotations omitted) (emphasis added); *see id.* ("Supreme Court's insistence on reasonableness rather than prescriptions for police conduct").

12 *See United States v. Causey,* 834 F.2d 1179, 1184 (5th Cir.1987) (en banc) ("so long as police do no more than they are objectively authorized to do, their motives in doing so are irrelevant and hence not subject to inquiry").

13 *See Brigham,* 382 F.3d at 508; *United States v. Dortch,* 199 F.3d 193, 198 (5th Cir.1999).

14 *See Brigham,* 382 F.3d at 510; *United States v. Jones,* 234 F.3d 234, 241 (5th Cir.2000).

15 *See Brigham,* 382 F.3d at 509.

16 While Campos urges us to answer the question of whether a defendant can challenge the reliability of a canine alert so as to defeat probable cause based on that alert, we decline to do so here. Campos acknowledges that the district court allowed him to present evidence tending to show that Tessa was unreliable, and thus, the only question before us is whether, on this record, the district court erred in concluding that the canine alert was reliable.

17 *E.g., Gonzalez,* 328 F.3d at 759; *Dortch,* 199 F.3d at 197; *United States v. Dovali-Avila,* 895 F.2d 206, 207 (5th Cir.1990).

18 A "handler cue" is a conscious or unconscious signal that leads a canine to where the handler believes the drugs are located.

19 *See United States v. Lopez,* 74 F.3d 575, 577 (5th Cir.1996).

20 *United States v. Hardin,* 437 F.3d 463, 468 (5th Cir.2006).

21 18 U.S.C. § 3006A(e)(1) (emphasis added).

22 *See United States v. Gadison,* 8 F.3d 186, 191 (5th Cir.1993) (citation omitted) (emphasis in original); *see also Hardin,* 437 F.3d at 469 n. 5.

23 *See Gadison,* 8 F.3d at 191.

24 *See United States v. Scott,* 48 F.3d 1389, 1396 ("The rights established by 18 U.S.C. § 3006A(e) are procedural, and the failure to make a *timely* motion or request waives the necessity for the court's consideration of an appointment of an expert witness." (quotations and citation omitted) (emphasis added)).

25 *United States v. Pollani,* 146 F.3d 269, 272 (5th Cir.1998).

26 The standing order required that the government turn over, *inter alia,* "documents ... that the government intended to use as evidence at trial to prove its case-in-chief...."

27 *See United States v. Diaz,* 25 F.3d 392, 395 (6th Cir.1994) (limited information on which expert's opinion was based, i.e., trial transcripts (and not actual observations of the drug dog), detracted from the expert's testimony).

97 Cal. Daily Op. Serv. 5466, 97 Daily Journal D.A.R. 8856

KeyCite Yellow Flag - Negative Treatment
Declined to Follow by U.S. v. Vig, 8th Cir.(S.D.), February 2, 1999

119 F.3d 742
United States Court of Appeals,
Ninth Circuit.

UNITED STATES of America, Plaintiff–Appellee,
v.
Scott Douglas LACY, Defendant–Appellant.

No. 95–30370.
|
Argued and Submitted June 3, 1996.
|
Submission Vacated Aug. 5, 1996.
|
Resubmitted June 27, **1997**.
|
Decided July 10, **1997**.

Synopsis

Defendant was convicted in the United States District Court for the Western District of Washington, William L. Dwyer, J., of possessing child pornography. Defendant appealed. The Court of Appeals, James R. Browning, Circuit Judge, held that: (1) search warrant affidavit provided probable cause to search defendant's apartment and to seize computer equipment; (2) defendant may be convicted of possessing child pornography only upon showing that he knew matter in question contained unlawful visual depiction; (3) no plain error arose from erroneous scienter and jurisdictional instructions; and (4) jurisdictional element was satisfied.

Affirmed.

West Headnotes (16)

[1] Obscenity
Staleness

Affidavit provided probable cause for issuance of warrant authorizing search of defendant's apartment and seizure of computer equipment, computer records, and documents relating to child pornography computer bulletin board system; affidavit stated that defendant downloaded at least two graphic interchange formats (GIFs) depicting minors engaged in sexual activity, and, even though information relied on was 10 months old, it was not stale, as affiant explained that collectors of child pornography "rarely if ever" dispose of such material, and store it "for long periods" in secure place, typically in their homes. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2252(a)(4)(B).

138 Cases that cite this headnote

[2] Obscenity
Probable Cause

Evidence that defendant has ordered child pornography is insufficient to establish probable cause to believe he possesses such pornography. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2252(a)(4)(B).

18 Cases that cite this headnote

[3] Searches and Seizures
Time for Application or Issuance; Staleness

Search warrant affidavit must be based on facts so closely related to time of issue of warrant as to justify finding of probable cause at that time. U.S.C.A. Const.Amend. 4.

31 Cases that cite this headnote

[4] Searches and Seizures
Time for Application or Issuance; Staleness

Mere lapse of substantial amounts of time is not controlling on question of staleness of information in search warrant affidavit; rather, staleness is evaluated in light of particular facts of case and nature of criminal

activity and property sought. U.S.C.A. Const.Amend. 4.

46 Cases that cite this headnote

[5] Obscenity
Objects or information sought

Warrants authorizing search of child pornography defendant's apartment and seizure of computer equipment and records was not overly general, even though warrants described computer equipment itself in generic terms and subjected it to blanket seizure; government knew defendant had downloaded computerized visual depictions of child pornography, but did not know whether images were stored on hard drive or on one or more of his many computer disks. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2252(a)(4)(B).

67 Cases that cite this headnote

[6] Searches and Seizures
Particularity or generality and overbreadth in general

In gauging search warrant's specificity, court considers whether probable cause exists to seize all items of particular type described in warrant, whether warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not, and whether government was able to describe items more particularly in light of information available to it at time warrant was issued. U.S.C.A. Const.Amend. 4.

13 Cases that cite this headnote

[7] Obscenity
Knowledge or intent

Defendant may be convicted of possessing child pornography only upon showing that he knew matter in question contained unlawful visual depiction. 18 U.S.C.A. § 2252(a)(4)(B).

8 Cases that cite this headnote

[8] Criminal Law
Acts prohibited by statute

Scienter requirement is presumed to apply to each statutory element which criminalizes otherwise innocent conduct, even if this is not most natural grammatical reading of statutory language.

1 Cases that cite this headnote

[9] Obscenity
Possession

Obscenity
Electronic transmission;internet

Telecommunications
Soliciting minor for sex or illegal act; child pornography

"Matter", as used in statute that prohibits knowing possession of 3 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction of minor engaging in sexually explicit conduct, means physical medium that contains visual depiction, such as computer and disks. 18 U.S.C.A. § 2252(a)(4)(B).

17 Cases that cite this headnote

[10] Statutes
Associated terms and provisions; noscitur a sociis

"Noscitur a sociis" means that word is understood by associated words.

3 Cases that cite this headnote

[11] Statutes
General and specific terms and provisions;ejusdem generis

"Ejusdem generis" means that things embraced in general term are of same kind as those denoted by specific terms.

9 Cases that cite this headnote

[12] Statutes

Language

Although canons of construction do not mandate how phrase is to be read, they describe what is usually meant by particular manner of expression.

Cases that cite this headnote

[13] Obscenity

Depiction of minors;child pornography

Instructions that permitted jury to convict defendant of possession of child pornography without finding that he knew his computer hard drive and disks contained unlawful visual depictions was erroneous, in light of claim that, although he knew depictions he downloaded onto his disks and drive were of minors engaged in sexually explicit conduct, he believed he had deleted those depictions. 18 U.S.C.A. § 2252(a)(4)(B).

10 Cases that cite this headnote

[14] Obscenity

Depiction of minors;child pornography

Jurisdictional instruction in prosecution for possession of child pornography on computer hard drive and disks erroneously focused on materials used to produce "matters," i.e., on whether materials used to produce computer hard drive and disks had traveled in interstate commerce, instead of focusing on materials used to produce visual depictions, i.e., on whether computer hard drive and disks themselves had traveled in interstate commerce. 18 U.S.C.A. § 2252(a)(4)(B).

8 Cases that cite this headnote

[15] Criminal Law

Elements of offense and defenses

Erroneous instructions that permitted jury to convict defendant for possession of child pornography without finding that he knew his computer hard drive and disks contained unlawful visual depictions, and which did not ask whether computer hard drive and disks themselves had traveled in interstate commerce, were not plain error; defendant's statements that he attempted to delete depictions in question were contradicted by presence of images on disks, and government offered evidence that defendant's computer equipment traveled in interstate commerce. 18 U.S.C.A. § 2252(a)(4)(B).

24 Cases that cite this headnote

[16] Obscenity

Interstate commerce

Obscenity

Electronic transmission;internet

Telecommunications

Soliciting minor for sex or illegal act; child pornography

Defendant "produced" depiction of minors engaged in sexual acts, for purposes of jurisdictional element in prosecution for possession of child pornography, when he downloading visual depictions from child porn computer bulletin board system, and thus, because his computer hard drive, monitor, and disks had traveled in interstate commerce, jurisdictional element was satisfied; although images on defendant's computer were copies of ones on bulletin board system, they were created —"produced"—when he used his computer to download data. 18 U.S.C.A. § 2252(a)(4)(B).

28 Cases that cite this headnote

97 Cal. Daily Op. Serv. 5466, 97 Daily Journal D.A.R. 8856

Attorneys and Law Firms

***744** C. James Frush, Helsell Fetterman, Seattle, WA, for defendant-appellant.

Kathy L. McClure and Patricia Toth, United States Department of Justice, Washington, DC, for plaintiff-appellee.

Appeal from the United States District Court for the Western District of Washington; William L. Dwyer, District Judge, Presiding. D.C. No. CR–95–00297–1–WLD.

Before: BROWNING, WRIGHT and T.G. NELSON, Circuit Judges.

Opinion

***745** JAMES R. BROWNING, Circuit Judge.

Scott Douglas Lacy appeals his conviction for possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). We affirm.

I.

The United States Customs Service was informed that child pornography from a Danish computer bulletin board system called BAMSE was being brought into the United States by computer. BAMSE's records indicated several people, including a caller from Seattle who identified himself as "Jim Bakker," had received material from BAMSE by telephone.[1] "Bakker" had called BAMSE sixteen times and had downloaded six picture files containing computerized visual depictions known as GIFs.[2] Customs agents traced the caller's phone number to an apartment occupied by a computer analyst named Scott Lacy. Telephone records reflected calls made from Lacy's telephone to BAMSE on the dates shown in BAMSE's records.

A warrant was issued authorizing the search of Lacy's apartment and seizure of computer equipment and records, and documents relating to BAMSE. Customs agents seized Lacy's computer, more than 100 computer disks, and various documents.[3] The computer hard drive and disks contained GIF files depicting minors engaged in sexually explicit activity.

Lacy was indicted for possessing child pornography.[4] Lacy's motion to suppress was denied, with inconsequential exceptions.[5] Lacy was tried and convicted. He appealed, challenging the suppression ruling, the jury instructions, and the sufficiency of the evidence on the crime's jurisdictional element.

II.

[1] Lacy argues the affidavit supporting the application for the warrant was insufficient to establish probable cause because it rested on stale information and demonstrated only that he "might have attempted to order" obscene pictures.

[2] Evidence the defendant has ordered child pornography is insufficient to establish probable cause to believe the defendant possesses such pornography. *See United States v. Weber,* 923 F.2d 1338, 1344 (9th Cir.1990). However, the affidavit stated Lacy downloaded at least two GIFs depicting minors engaged in sexual activity from BAMSE, providing sufficient evidence Lacy actually received computerized visual depictions of child pornography.

[3] **[4]** The information in the affidavit was not stale. An affidavit must be based on facts " 'so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time.' " *Durham v. United States,* 403 F.2d 190, 193 (9th Cir.1968) (quoting *Sgro v. United States,* 287 U.S. 206, 210, 53 S.Ct. 138, 140, 77 L.Ed. 260 (1932)). We held in *Durham* that probable cause was not established by an affidavit relying on events that occurred four months earlier. *Id.* at 194–95. The information relied on in this case was ten months old. However, "[t]he mere lapse of substantial amounts of time is not controlling in a question of staleness." *United States v. Dozier,* 844 F.2d 701, 707 (9th Cir.1988). "We evaluate staleness in light of the particular facts of the case and the nature of the criminal activity and property sought." *United States v. Pitts,* 6 F.3d 1366, 1369 (9th Cir.1993)

(internal quotation omitted). The information offered in support of the application for a *746 search warrant is not stale if "there is sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises." *United States v. Gann,* 732 F.2d 714, 722 (9th Cir.1984).

The affidavit in this case provided ample reason to believe the items sought were still in Lacy's apartment. Based on her training and experience as a Customs agent, the affiant explained that collectors and distributors of child pornography value their sexually explicit materials highly, "rarely if ever" dispose of such material, and store it "for long periods" in a secure place, typically in their homes.[6] *Cf. United States v. Rabe,* 848 F.2d 994, 995–96 (9th Cir.1988). We are unwilling to assume that collectors of child pornography keep their materials indefinitely, but the nature of the crime, as set forth in this affidavit, provided "good reason[ ]" to believe the computerized visual depictions downloaded by Lacy would be present in his apartment when the search was conducted ten months later. *See Gann,* 732 F.2d at 722; *cf. Dozier,* 844 F.2d at 707 (long-term nature of marijuana cultivation justified magistrate's reliance on information that was five months old).

[5] [6] Lacy also argues the warrant was too general because it authorized the seizure of his entire computer system.[7] Lacy relies primarily upon *United States v. Kow,* 58 F.3d 423 (9th Cir.1995), in which we invalidated a warrant authorizing seizure of all the defendant's computer hardware and software, as well as "essentially all" of its "records ... files, ledgers, and invoices." *See id.* at 425. Unlike the affidavit in *Kow,* the affidavit in this case established probable cause to believe Lacy's entire computer system was "likely to evidence criminal activity." *See id.* at 427. And while the warrant in *Kow* "contained no limits on which documents within each category could be seized or suggested how they related to specific criminal activity," *id.,* the Lacy warrant contained objective limits to help officers determine which items they could seize—allowing seizure only of documents linked to BAMSE, for example.

Both warrants described the computer equipment itself in generic terms and subjected it to blanket seizure. However, this type of generic classification is acceptable "when a more precise description is not possible," *United States v. Cardwell,* 680 F.2d 75, 78 (9th Cir.1982) (internal quotation omitted); *see also United States v. Kimbrough,* 69 F.3d 723, 727 (5th Cir.1995), and in this case no more specific description of the computer equipment sought was possible. The government knew Lacy had downloaded computerized visual depictions of child pornography, but did not know whether the images were stored on the hard drive or on one or more of his many computer disks. In the affidavit supporting the search warrant application, a Customs agent explained there was *747 no way to specify what hardware and software had to be seized to retrieve the images accurately.

We conclude that Lacy's challenge to the district court's suppression ruling is without merit.

III.

Lacy contends the district court improperly instructed the jury on the *mens rea* and jurisdictional elements of § 2252(a)(4)(B).

A. Mens Rea

Lacy argues the instructions were improper because they omitted a necessary *mens rea* element. The instructions required the jury to find that Lacy knowingly possessed "the matters charged" and that those "matters contained a visual depiction of a minor engaging in sexually explicit conduct," but the instructions did not require a finding Lacy *knew* the matters contained the visual depictions. The omission was critical, Lacy contends, because his defense was that he had attempted to erase the illegal images from his computer disks and believed he had succeeded. He argues the instruction allowed the jury to convict him without finding he knew the computer hard drive and disks in his possession contained pornographic visual depictions that violated § 2252(a)(4)(B).

The government responds that the instruction was correct as given—an argument that can be interpreted as denying that knowledge of the presence of the pornographic

depictions is required, or denying that the instructions omitted this element. We consider both possibilities.

1.

[7] **[8]** The statutory language is of little help.[8] It is not clear whether the word "knowingly" was intended to modify only the first or all of the words in the series that follows. *See United States v. Gendron,* 18 F.3d 955, 958 (1st Cir.1994). However, a scienter requirement is presumed to apply "to each of the statutory elements which criminalize otherwise innocent conduct," even if this is not the "most natural grammatical reading" of the statutory language. *United States v. X–Citement Video, Inc.,* 513 U.S. 64, 72, 115 S.Ct. 464, 469, 130 L.Ed.2d 372 (1994). Applying this rule to a subsection of § 2252 that bars transportation of child pornography, the Supreme Court held in *X–Citement Video* that the knowledge requirement extended to the sexually explicit nature of the material and the age of the performer even though those elements were "set forth in independent clauses separated by interruptive punctuation." *Id.* at 68, 82, 115 S.Ct. at 467, 474. This interpretation was necessary, the Court held, because the elements at issue were crucial to establishing liability. Distribution of sexually explicit material involving adults is legal, while distribution of sexually explicit material involving minors is not. Unless a distributor knew the performers were underage, the Court reasoned, he would have reasonably expected his conduct to be legal. *Id.* at 71–73, 115 S.Ct. at 469.

The same is true of § 2252(a)(4)(B)'s requirement that a matter "contain" an unlawful visual depiction. Possession of computer drives and disks, like possession of books, is ordinarily lawful. The presence of illegal images on the disks or in the books is a "crucial element separating legal innocence from wrongful conduct." *See id.* Accordingly, a defendant may be convicted under § 2252(a)(4)(B) only upon a showing that he knew the matter in question contained an unlawful visual depiction.

2.

Whether the knowledge element was omitted from the instructions depends upon the ***748** meaning of the word "matters."[9] Lacy contends the "matter" or "matters" referred to in the statute and instructions are the computer disks and hard drive that contain the GIF files, while the government argues "the 'matter' in question is the computer GIF files which contain the visual depictions of child pornography."

[9] **[10]** **[11]** **[12]** The statute indicates that at a minimum, a "matter" must be capable of containing a visual depiction. *See* 18 U.S.C. § 2252(a)(4)(B). Although both the disks and the GIF files could be viewed as "containing" the visual depiction, we conclude the "matter" is the physical medium that contains the visual depiction—in this case, the hard drive of Lacy's computer and the disks found in his apartment. This interpretation is supported by two principles of statutory interpretation, *noscitur a sociis* and *ejusdem generis.* "The first means that a word is understood by the associated words, the second, that a general term following more specific terms means that the things embraced in the general term are of the same kind as those denoted by the specific terms." *United States v. Baird,* 85 F.3d 450, 453 (9th Cir.1996) (citing 2A Norman J. Singer, *Sutherland–Statutory Construction* §§ 47.16, 47.17 (5th ed.1992)). Although canons of construction do not mandate how a phrase is to be read, they "describe[ ] what we usually mean by a particular manner of expression." *Longview Fibre Co. v. Rasmussen,* 980 F.2d 1307, 1313 (9th Cir.1992). Here, the word "matter" appears at the end of the list "books, magazines, periodicals, films, [and] video tapes," all of which are physical media capable of containing images. *See Baird,* 85 F.3d at 453 (looking to list's "theme" to determine the meaning of a general term).

[13] The trial court did not explicitly instruct the jury to find whether Lacy knew depictions of minors engaged in sexually explicit conduct were on his hard drive and disks. It might be argued that instructing the jury to find whether Lacy knew images on his disks and hard drive depicted minors engaging in sexually explicit conduct necessarily required it to find that Lacy knew these depictions were, in fact, on his disks or hard drive. However, Lacy claimed he had seen the depictions of minors engaging in sexually explicit conduct when he opened the GIF files but had

deleted the depictions from his disks and drive. If his claim were true, he knew the depictions he downloaded onto his disks and drive were of minors engaged in sexually explicit conduct, but he did not know the depictions were still on his disks and drive. To address this defense, the trial court had to instruct the jury that to convict Lacy it must find that he knew the depictions were on his disks and drive. Because the instructions allowed the jury to convict Lacy without finding that he knew the hard drive and disks contained the unlawful visual depictions, they were erroneous.

B. Jurisdiction

[14] Lacy also challenges the district court's jurisdictional instruction, which required the jury to find "that each of those matters possessed by the defendant had been produced using materials that had been transported in interstate or foreign commerce." ER 9, Instruction 12. He argues the instruction erroneously focused on the materials used to produce the "matters"—that is, on whether the materials used to produce the *computer hard drive and disks* had traveled in interstate commerce—instead ***749** of focusing on the materials used to produce the *visual depictions*—that is, as we hold below, on whether the computer hard drive and disks *themselves* had traveled in interstate commerce.

Lacy's argument is supported by the plain language of § 2252(a)(4)(B), which prohibits possession of

> books ... or other matter which contain any *visual depiction* that has been mailed, or has been shipped or transported in interstate or foreign commerce, or *which was produced using materials which have been mailed or so shipped or transported,* by any means including by computer ...

18 U.S.C. § 2252(a)(4)(B) (emphasis added); *see Kimbrough,* 69 F.3d at 729 (jurisdictional element considers "whether the pictures or the materials used to produce them traveled in commerce"); *United States v. Colavito,* 19 F.3d 69, 71 (2d Cir.1994). The government argues it could establish jurisdiction by showing that "books ... or other matter which contain any visual depiction ... [were] produced" using materials transported in interstate commerce. The altered verb tense is significant; the government's interpretation would require an ungrammatical reading of the statute. We agree with the Fifth and Second Circuits that jurisdiction exists if the "pictures or the materials used to produce them" traveled in interstate commerce. *Kimbrough,* 69 F.3d at 729; *see Colavito,* 19 F.3d at 71. Because the instruction allowed the jury to convict Lacy without making such a finding, it was erroneous. [10]

C. Plain error

[15] Because Lacy did not object to these instructions, we review for plain error. Even if we found that Lacy established plain error, however, we would not exercise our discretion to correct the error because it did not " 'seriously affect the fairness, integrity or public reputation of judicial proceedings.' " *United States v. Olano,* 507 U.S. 725, 736, 113 S.Ct. 1770, 1779, 123 L.Ed.2d 508 (1993) (quoting *United States v. Atkinson,* 297 U.S. 157, 160, 56 S.Ct. 391, 392, 80 L.Ed. 555 (1936)); *see also United States v. Perez,* 116 F.3d 840, 845–46 (9th Cir.1997) (en banc).

We examine the strength of the evidence against Lacy to determine whether the errors in the jury instructions seriously affected the fairness and integrity of his trial. *Perez,* 116 F.3d at 847–48. The evidence that Lacy knew he possessed GIF files containing pornographic images was overwhelming. Lacy's phone records reflected calls to BAMSE. BAMSE's computer reflected those calls and indicated which pornographic images were downloaded. Agents who searched Lacy's apartment found computer disks containing child pornography, many labeled with the names of the GIF files they contained. A Customs agent testified that Lacy acknowledged downloading sexually explicit images of children and admitted he knew the children pictured were as young as eight or nine years of age. Lacy did not testify.

The only evidence in support of Lacy's claim that he thought he had deleted the GIF files came from Special Agent John Hynes, who testified as follows:

Q: Did you ask ... what he did with the material after it was downloaded?

A: Yes, ma'am. He said he deleted it.

...

Q: Would you review your notes regarding the deletion comment ... ?

A: Yes, ma'am. Immediately before that when I asked him if he had any child pornography and he responded he had downloaded some stuff, I asked him what he meant and he said child pornography and stuff, he then said he was extremely nervous about keeping it and as far as he knows or knew, the material was gone....

He explained that he had called into the BAMSE bulletin board and heard on a voice mail message that they were shut down, and this had made him extremely nervous, that's why he deleted the material.

***750** **Lacy's** statements were contradicted by the presence of the images on the disks. It is implausible, to say the least, that the jury believed **Lacy**, a professional computer analyst, attempted to delete the files but somehow failed to do so.

It is also extremely unlikely that the jury, if properly instructed, would not have found that the government established the jurisdictional element of the crime. As we hold below, **Lacy** "produced" the visual depictions using his computer. The government offered evidence that **Lacy's** computer equipment traveled in interstate commerce; **Lacy** did not dispute the evidence or provide any evidence to the contrary.

IV.

[16] **Lacy** argues the government failed to prove the jurisdictional element of the crime. To establish jurisdiction under § 2252, the government was required to prove either that the visual depictions were transported in interstate commerce or that they were "produced using materials which have been mailed or so shipped or transported, by any means including by computer ..." 18 U.S.C. § 2252(a)(4)(B); *see Kimbrough,* 69 **F.3d** at 729 (describing jurisdictional element as "whether the pictures or the materials used to produce them traveled in commerce"). The government relied on the second alternative, offering undisputed evidence that **Lacy's** computer hard drive, monitor, and disks had traveled in interstate commerce. **Lacy** argues this evidence is insufficient because the visual depictions were not "produced" by his computer.

"Producing" is defined as "producing, directing, manufacturing, issuing, publishing, or advertising." 18 U.S.C. § 2256(3). **Lacy** argues that in downloading the visual depictions, he was merely "reproducing" or copying them. Although the images on **Lacy's** computer were copies of the ones on the BAMSE system, they were created—"produced"—when **Lacy** used his computer to download data. The statute requires only that *visual depictions* be produced; it does not matter that the depictions on **Lacy's** computer were copies rather than originals.

V.

Lacy's motion to suppress was properly denied. Although the jury instructions were erroneous, **Lacy** did not object to them. We will not correct these plain forfeited errors because they did not seriously affect the fairness of **Lacy's** trial. Finally, the jury's finding on the jurisdictional element was supported by substantial evidence.

AFFIRMED.

All Citations

119 F.3d 742, 97 Cal. Daily Op. Serv. 5466, 97 Daily Journal D.A.R. 8856

Footnotes

1 The BAMSE computer recorded the dates and times of calls, the caller's phone number, and the names of files the user downloaded.

2 GIF stands for "graphic interchange format," a special format used to store visual information such as photographs.

3 Some of the disks were seized from **Lacy's** apartment, while others were found in a separate storage room that was searched with **Lacy's** consent.

4 The indictment also charged **Lacy** with receiving child pornography and importing obscene material into the United States. The importation count was dismissed before trial on the government's motion. The district court acquitted **Lacy** of receiving child pornography.

5 The district court suppressed several documents, but both parties describe them as inconsequential.

6 **Lacy** challenges this information as "foundationless," citing *Weber,* in which we rejected information regarding the practices of child molesters because "there was not a whit of evidence in the affidavit indicating that Weber was a 'child molester.' " *Weber,* 923 F.2d at 1345. The affidavit in this case contained sufficient evidence that **Lacy** had downloaded computerized visual depictions of child pornography to provide a foundation for evidence regarding the practices of possessors of such pornography.

7 A warrant must describe the specific place to be searched and person or things to be seized "with particularity sufficient to prevent 'a general, exploratory rummaging in a person's belongings.' " *United States v. Rude,* 88 **F**.**3d** 1538, 1551 (**9th Cir**.1996) (quoting *Coolidge v. New Hampshire,* 403 **U.S**. 443, 467, 91 S.Ct. 2022, 2038–39, 29 L.Ed.2d 564 (1971)); *see also Andresen v. Maryland,* 427 **U.S**. 463, 480, 96 S.Ct. 2737, 2748, 49 L.Ed.2d 627 (1976). The warrant need only be "reasonably specific, rather than elaborately detailed, and the required specificity varies depending on the circumstances of the case and the type of items involved." *Rude,* 88 **F**.**3d** at 1551 (citations and internal quotations omitted); *see United States v. Spilotro,* 800 F.2d 959, 963 (**9th Cir**.1986).

> In gauging a warrant's specificity, we consider three factors:
>
> > (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued.
>
> *United States v. Noushfar,* 78 **F**.**3d** 1442, 1447 (**9th Cir**.1996) (*quoting Spilotro,* 800 F.2d at 963); *see United States v. Stubbs,* 873 F.2d 210, 211 (**9th Cir**.1989).

8 The statute makes it a crime to

> > knowingly possess[ ] 3 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if-
> >
> > > (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
> > >
> > > (ii) such visual depiction is of such conduct.
>
> 18 U.S.C. § 2252(a)(4)(B).

9 The district court instructed the jury it could find **Lacy** guilty of possession if the government proved the following elements beyond a reasonable doubt:

> > First, that on or about March 6, 1993, the defendant knowingly possessed the matters charged;
> >
> > Second, that each of those matters contained a visual depiction of a minor engaging in sexually explicit conduct;
> >
> > Third, that each of those visual depictions was produced with the use of a minor engaging in sexually explicit conduct;
> >
> > Fourth, that the defendant knew that each of those visual depictions was of a minor engaging in sexually explicit conduct, and knew it had been produced with the use of a minor engaging in such conduct; and
> >
> > Fifth, that each of those matters possessed by defendant had been produced using materials that had been transported in interstate or foreign commerce.
>
> ER 9, Instruction 12.

10 Arguing that the "matters" in question are the GIF files, the government also contends the instruction *did* require the jurors to consider whether the visual depictions were produced using materials that traveled in interstate commerce. We have already rejected the government's contention that the "matters" in question are the GIF files.

U.S. v. Lacy, 119 F.3d 742 (1997)

97 Cal. Daily Op. Serv. 5466, 97 Daily Journal D.A.R. 8856

End of Document

Waltonchain White Paper

(V 1.0.4)

Value Internet of Things (VIoT) constructs a perfect commercial ecosystem via the integration of the real world and the blockchain

Ushering human beings into the reliable digital life

Waltonchain unfolds the new era of Value Internet of Things (VIoT)

By the Waltonchain Team

2018.02.08

Table of Contents

Part 1 Introduction — The concept of the Value Internet of Things

1.1 The Inevitable Trend of Internet Technology Innovation: The Value Internet of Things

We are in an era where new technologies lead to social changes. In the age of information and the Internet, human collaboration and communication break through time and space constraints, and the world becomes an overall interactive platform.

In recent years, the Internet has entered a new business format of "Internet +". In this stage, a new form of economic and social development of "Internet + all traditional industries" driven by knowledge and social innovation 2.0 provides a broad network platform for the reform, innovation and development of various industries.

At present, the information age is entering an unprecedented important stage of development where the objects can be connected to each other through the Internet; this stage is called the third wave of the development of the world information industry following the computer and the Internet: the age of the Internet of Things (IoT). Internet of Things technology contains two meanings: first, the core and foundation of the Internet of Things is still the Internet, the Internet of Things is an extension of the Internet; second, the client side of the Internet of Things extends to the information exchange and communication between any objects, which is so called object-to-object interrelation.

However, from the Internet, to the "Internet +" and then to the Internet of things, all stages have failed to solve the problem of localization of information

dissemination (e.g. centralization). It is difficult for the Internet of things under the current central structure to accomplish the real autonomous cooperation and effective transactions, because the relevant parties of such cooperation and transactions often belong to different stakeholders with complex and uncertain trust relationship. Therefore, the collaboration and transactions of the current Internet of Things devices can only be carried out under the same trust domain, the devices to collaborate and trade must be provided or verified by the same Internet of Things service provider, which significantly reduces the true commercial value of the Internet of Things applications.

In this context, we put forward the concept of the "Value Internet of Things (VIoT)", focusing on introducing the blockchain technology into the Internet of things, to solve the problem of centralization facing the development process of the Internet of Things. The blockchain is a decentralized transaction record & storage technology based on cryptographic principles; with a distributed point-to-point network, it can achieve the permanent storage of orderly transaction record which is undeletable, tamper-resistant, open and traceable, so it is recognized as the best choice to meet the above challenges. In the ecology of the blockchain, people can trade safely without trust established in advance, because every transaction is well recorded in the "public ledger" of the blockchain, which is a perfect solution to the trust and equity issues of the Internet virtual world. The inevitable trends of the Value Internet of Things are shown in Figure 1.1.

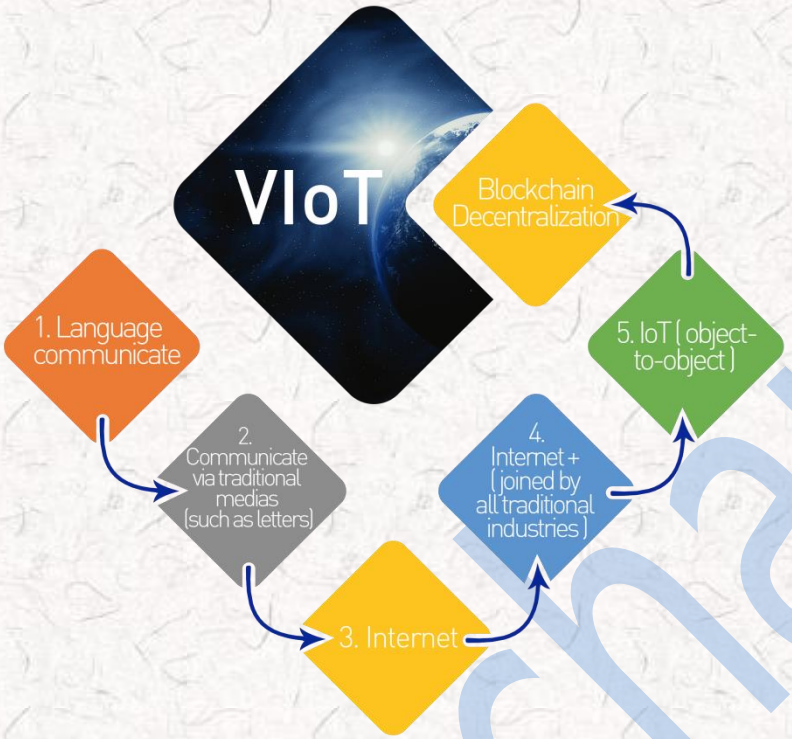


Figure 1.1: The inevitable trend of the Value Internet of Things

1.2 The Blockchain Technology Development Trend: Rapid Expansion of Application Areas

Bitcoin appeared in 2009 and began to circulate. The total market capitalization of Bitcoin has exceeded $ 30 billion, making Bitcoin a successful application of the blockchain technology in the field of digital money. Ethereum introduced smart contracts to program the complex contract rules into the blockchain by way of code. Smart contracts can be automatically executed when the agreed conditions are reached, as a result, the field of application of the blockchain has been broadened; the representative Namecoin and Datacoin extended the object of the blockchain from the electronic money trading record in the era of Bitcoin to the domain name, user data and other fields.

As an organic component of the blockchain distributed implementation, the consensus mechanism has also undergone full development; as a result, several major consensus mechanisms have appeared:

POW: Proof of Work, e.g. Work to Prove Consensus Mechanism, also known as the mining mechanism. Bitcoin is first one to use the POW mechanism to dominate the block generation. The node continues trying to calculate the block hash value corresponding to each block ledger's content to satisfy a specific condition, that is, N zeros are used as the preamble. This will increase the difficulty of Block generation, significantly reducing the risk of correct subchains being replaced by quickly generated longer malicious subchains, but will also lead to the waste of many computing resources of the mining machines at the same time.

POS: Proof of Stake, e.g. Stake to Prove Consensus Mechanism. It is an upgrade of the POW consensus mechanism to control the length of mining time based on the number of the tokens and the holding time of the node; it can effectively reduce the mining time, but still cannot avoid the problem of wasting the computing resources of the mining machines.

DPOS: Delegated Proof of Stake, e.g. Delegated Stake to Prove Consensus Mechanism. Its principle is that tokens select a certain number of nodes by voting to complete the verification and accounting work for them. This consensus mechanism can greatly reduce the number of nodes involved in accounting and verification to achieve rapid consensus verification, but it also relies on the existence of the tokens, so that some applications that do not require tokens will be limited.

PBFT: Practical Byzantine Fault Tolerance. It is a consistency algorithm by message transmission that achieves consistency through three phases to determine the final block generation. If there are 3f + 1 nodes, this algorithm can tolerate the existence of f error nodes, so that the consistency results will not be

affected. This mechanism can be divorced from the existence of coins, the consensus node can be determined by participants and regulators, and 2—5 seconds of shared delay are basically able to meet the commercial requirements.

Various consensus mechanisms have their own considerations and significance in terms of their respective business scenarios and technical means. When compared to each other, they have different improvements and enhancements in different aspects, as well as different disadvantages, so there seems to be no optimal consensus mechanism. Achieving the pluggable applications of various consensus mechanisms, choosing the right consensus mechanism according to the specific application scenario and optimizing the application of blockchain shall be the best way for further application in more fields.

Various trends indicate that blockchain technology is expanding its application to more and more areas, such as digital money and smart contracts, while the earlier relevant technologies failed to break the connection barrier between the virtual network and the real world. Applying the blockchain to the Internet of Things and smart systems and connecting the item tags and identity tags in the real world to the virtual network via RFID technology will successfully build this connection, ultimately achieve the interconnection of all things and create the era of Value Internet of Things (VIoT).

1.3 The Technical Preparation to Create the Era of Value Internet of Things (VIoT) Has Been Completed

Traditional Internet of Things (IoT) is a network which enables all the common objects that can perform independent functions to be interconnected. It connects the sensors, controllers and objective entities through network technology to realize intelligent management and control. For example, through radio frequency

identification (RFID), infrared sensors, global positioning systems, laser scanners and other information sensing equipment, it connects any item to the Internet to carry out information exchange and communication according to the agreement, to achieve intelligent identification, positioning, tracking, monitoring and management. As an extension of the Internet, the Internet of Things further promotes the connections between machine and machine, human and machine and achieves the full life cycle circulation management of data in the information world.

With the continuous advances of technology, the development and application of the Internet of Things technology have achieved remarkable results in recent years. There are already billions of sensors and smart controllers put into use so far, and the number of the sensors and smart controllers is expected to grow in the next few years. However, the Internet of Things technology is also facing many problems and challenges which may become great obstacles for the future development and application of the Internet of Things. The era of the Value Internet of Things led by RFID and blockchain technologies can provide solutions to these problems.

The technical realization of the Value Internet of Things means connecting the items tags, event tags, people and body tags and other entity tags in the real world with the virtual world of the Internet through the underlying hardware platform using the RFID tags as the core, combined with the blockchain technology delivering value and constructing trust, to achieve the real interconnection of all things.

The speed of transition from the Information Internet and traditional Internet of Things to the Value Internet of Things based on RFID and blockchain technology may be far beyond the current expectations. When the Value Internet of Things

achieves the real interconnection of all things, the RFID and blockchain technology will play a greater role.

Part 2 Journey — The Realization of Value Internet of Things

2.1 General Description

The whole system of the Value Internet of Things can be divided into two parts: hardware and software. The hardware includes the RFID tag chips and the RFID reader chips. The RFID tag acts as the interface for all assets to be connected to the chain, and the reader chip is a bridge for all assets to be connected to the chain and can be used as a node on the chain. The software includes the Waltonchain software system, the Waltonchain protocol and Waltoncoin. With the combination of software and hardware, the Value Internet of Things can really achieve the connection of all things to the chain and the digitalization of all assets.

2.2 The hardware of the Value Internet of Things

2.2.1 What is RFID?

The Radio Frequency Identification (RFID) technology is a communication technology that can identify specific targets and read and write relevant data through the radio signals without building a mechanical or optical contact between the recognition system and specific targets. RFID readers are divided into mobile readers and fixed readers. At present, RFID technology is widely used, for example, in library access control systems, for food safety traceability, etc.

The radio frequency tags are the physical carrier of the electronic product code (EPC) which are attached to traceable items, identifiable, readable and writeable and can be circulated all over the world. As a key technology for constructing the "Internet of Things", the RFID technology has received attention

in recent years. The RFID technology originated from the United Kingdom, it was used in the Second World War to identify friend or foe aircraft. Its business application began in the 1960s. The RFID technology is an automatic identification technology. The US Department of Defense states that all military supplies must use RFID tags since January 1, 2005, and the US Food and Drug Administration (FDA) recommends that the pharmaceutical companies use RFID to trace drugs easy to be faked since 2006. By using the RFID technology, Walmart and Metro retailers have further promoted the application of RFID in the world. In 2000, the price of each RFID tag was $1. Many researchers believed that RFID tags were very expensive, large-scale application could be realized only when the price went down. In 2005, the price of each RFID tag was about 12 cents, and now the price of each UHF RFID tag is about 10 cents. To achieve large-scale application of RFID, on the one hand, it is necessary to reduce the price of RFID tags, on the other hand, it depends on whether the application of RFID can bring value-added services. Eurostat statistics show that in 2010, 3% of the EU companies used RFID technology for identity documents and access control, supply chain and inventory tracking, car charges, security, production control and asset management, etc. Since 2010, due to the improvement of economic situation, the development of the Internet of Things industry and other positive factors, global RFID market continues to heat up, RFID technology has been applied to a growing number of fields, and people have had higher expectations for the development of RFID industry. The RFID technology is in a period of rapid maturity, many countries are actively promoting RFID as an important industry.

Although the prices of passive UHF electronic tags fell rapidly in the past two years, the prices of UHF RFID systems are still high relative to the overall cost of RFID chips, including readers, electronic tags, middleware, system maintenance, etc. And the cost of UHF RFID system is an important indicator for clients to

estimate the return of investment. The bottleneck caused by high cost has become an important factor restricting the development of UHF system market.

In short, the passive UHF market is still in its early stage of development. Thus, the core technology needs breakthroughs, business models need to be innovated and improved, and the industry value chain needs to be further developed and extended. Only when the core issues are effectively resolved, can we embrace the real development of RFID passive UHF market.

2.2.2 RFID tags

The RFID tag contains the stored electronic information. The tag does not need to be within the sight of the recognizer, and it can be embedded in the tracked object. RFID tags include passive tags and active tags.

Passive tags: can get energy from the electromagnetic field emitted by the reader, no battery required.

Active tags: the tag itself has power supply and can automatically send radio waves.

Figure 2.1 shows the actual application scenario of RFID.

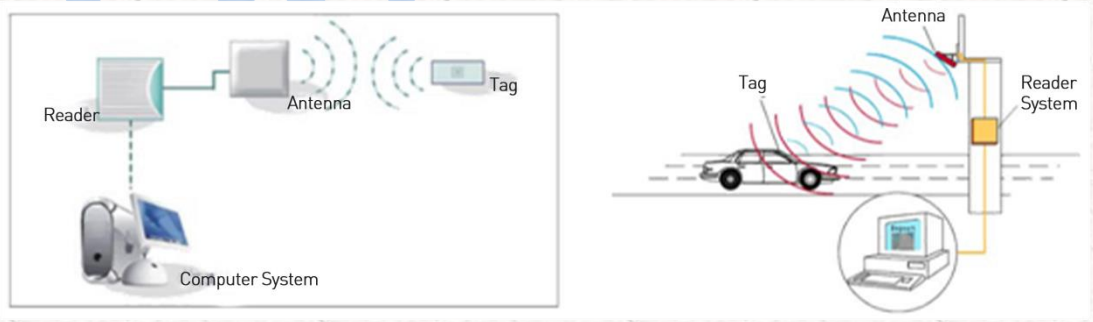


Figure 2.1: The actual application scenario of RFID

2.2.3 Introduction of UHF RFID ICs

After years of development, the RFID technology of 13.56 MHz or less has been relatively mature. At present, the industry pays most attention to the UHF RFID which operates in the frequency range 860 to 960 MHz. Its advantages are fast reading and writing, multi-target recognition, non-line-of-sight recognition, mobile positioning and long-term tracking management, long effective range (usually 3 to 10 m) and fast communication speed. UHF RFID technology has become a hot spot in the development of the industry, and passive UHF RFID tags and systems grow rapidly.

The built-in RFID IC of UHF recognizer (reader and writer) is a core component that provides readability to the recognizer. On the receiving end the Received wireless useful signal is amplified by LNA, mixed by I/Q mixer, filterer, converted by ADC, and finally inputted to the MCU; on the transmitting end the signal outputted from the MCU is mixed by I/Q mixer, amplified by PA and transmitted to the antenna, finally transmitted to the tag. Figure 2.2 shows the structure of the RFID IC of UHF recognizer (reader and writer).

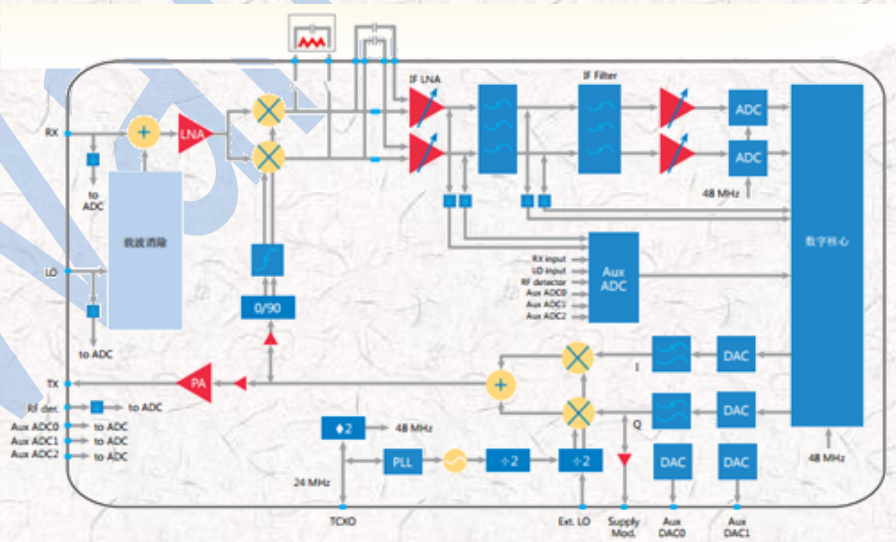


Figure 2.2: UHF recognizer (reader and writer) RFID IC structure diagram

UHF Tag IC: is a core component that provides memory and performance for tags. It manages the received wireless signal as energy, transmits the stored memory data to the antenna after the carrier modulation. Figure 2.3 shows the structure of the UHF RFID tag IC.

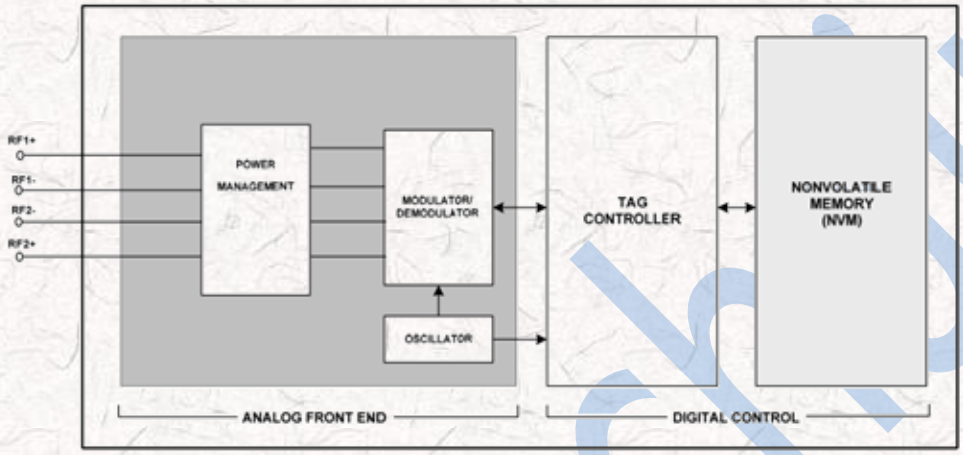


Figure 2.3: UHF RFID tag IC structure diagram

2.2.4 Analysis on the Advantages and Disadvantages of International RFID ICs

Reader ICs: due to the huge market attractiveness, many manufacturers have been involved in the relevant technology research, development and production, bringing on an upsurge of radio frequency identification technology. Based on the increasing investment in research, the RFID technology has made great progress in core hardware technology, public service platform and testing and standard. International companies have achieved many technical improvements of RF front-end, analog front end, digital baseband and storage unit of the multi-band radio frequency identification; the mainstream manufacturing process has reached 0.13 microns or less and achieved the mass production of low-power technological chips, such as R2000 by Impinj: its reception sensitivity has reached –80 dBm (10 dBm self-interference) with a transmission power of 31.5 dBm. Although the performance is excellent, the price is very high.

Tag ICs: as for the tag chip technology, the developed countries already have a relatively complete product line. With the continuous development and improvement of technology and market, the electronic tag technology continues to improve, and the industrial application of technology has entered a stage of vigorous development. The class 0 design by Alien has laid the foundation for the implementation of the first generation RFID standards. Compared to the first generation standards, the second generation EPF tag IC has many advantages: its center frequency reaches 900 MHz band, greatly improving the recognition rate to 500 to 1500 tags/sec; its backscatter data rate can be increased from tens of bits per second to 650 kbps; its scan range has increased to 30 feet. Now in the market and the laboratory, the second generation UHF RFID tag ICs with more excellent features have appeared, for example, Impinj's Monza 4 RFID tag IC has reached a more advanced level. Its outstanding performance mainly reflects in extensible memory options, innovative secrecy function, good anti-jamming capability and industry-leading sensitivity properties.

But the existing RFID chip industry cannot meet the development of Internet of Things applications, especially applications for the Value Internet of Things: there are few options available while the prices are high; the transmission power and stability need to be improved; the reception sensitivity is low, the anti-interference ability is poor and the transmission power is low. In addition, the existing RFID ICs have many problems such as high power consumption, poor matching with antenna and difficult system integration, etc.

2.2.5 The Overall Design of the RFID ICs of the Value Internet of Things

The project includes RFID tag IC and reader IC suitable for blockchain technology applications. The ICs are characterized by integrated elliptic curve and

decryption acceleration module based on the existing RFID technology and a communication interface protocol suitable for blockchain technology applications. The implementation of the project will promote the application of blockchain technology in the Internet of Things and solve the following problems in the current application of blockchain technology:

1. Each tag does not need to store node data, only need to be responsible for signature verification;

2. Tags automatically generate random public keys and private keys to ensure the security of Internet of Things applications, to ensure that the tag is unique, authentic and tamper-resistant;

3. Tags can reduce the amount of information stored to solve the problem of blockchain overload by large amounts of data in the Internet of Things applications;

4. Tags can solve the problem of slow encryption and decryption in asymmetric encryption technology;

5. Tags can help truly achieve the decentralization of property management and asset management so as to make the data tamper-resistant.

RFID reader IC is one of the core components of the reader, containing the RF section and digital signal processing section. On the receiving end the signal is amplified by LNA, mixed by I/Q mixer, filterer, converted by ADC and finally inputted to the digital processing section; on the transmitting end the digital signal outputted from the digital processing section is converted by ADC, mixed by I/Q mixer, amplified by PA and transmitted to the antenna, finally transmitted to the tag.

The RFID tag IC contains the RF section, power management section, digital signal processing section and storage section. The power management section contains electromagnetic coupling, energy storage, LDO and other circuits. It converts the received wireless signal into electrical energy to power the tag. In the transmitting section, the stored memory data is transmitted to the antenna after carrier modulation.

Though the RFID reader IC market demand continues to increase, the existing technology still has some aspects to be improved, such as the number of tags identified simultaneously, misreading, high power consumption, etc. The project provides a new design solution for the application problems and a chip architecture solution with core competencies, combined with the application of blockchain technology.

Figure 2.4 and Figure 2.5 show the block diagram of the reader IC and the tag IC, respectively. The RFID tag IC design integrates innovative encryption capabilities, so it's suitable for blockchain technology applications and has a good anti-interference ability and sensitivity index. Its demanding power design can meet the current stringent requirements for power consumption, and the on-chip antenna technology and antenna matching technology have been significantly enhanced to improve the performance.

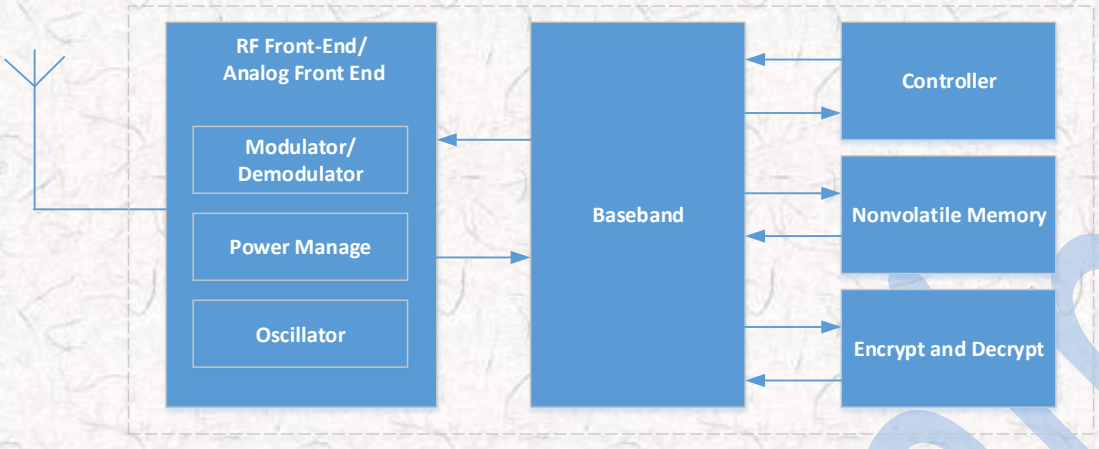


Figure 2.4: The project's reader IC solution block diagram

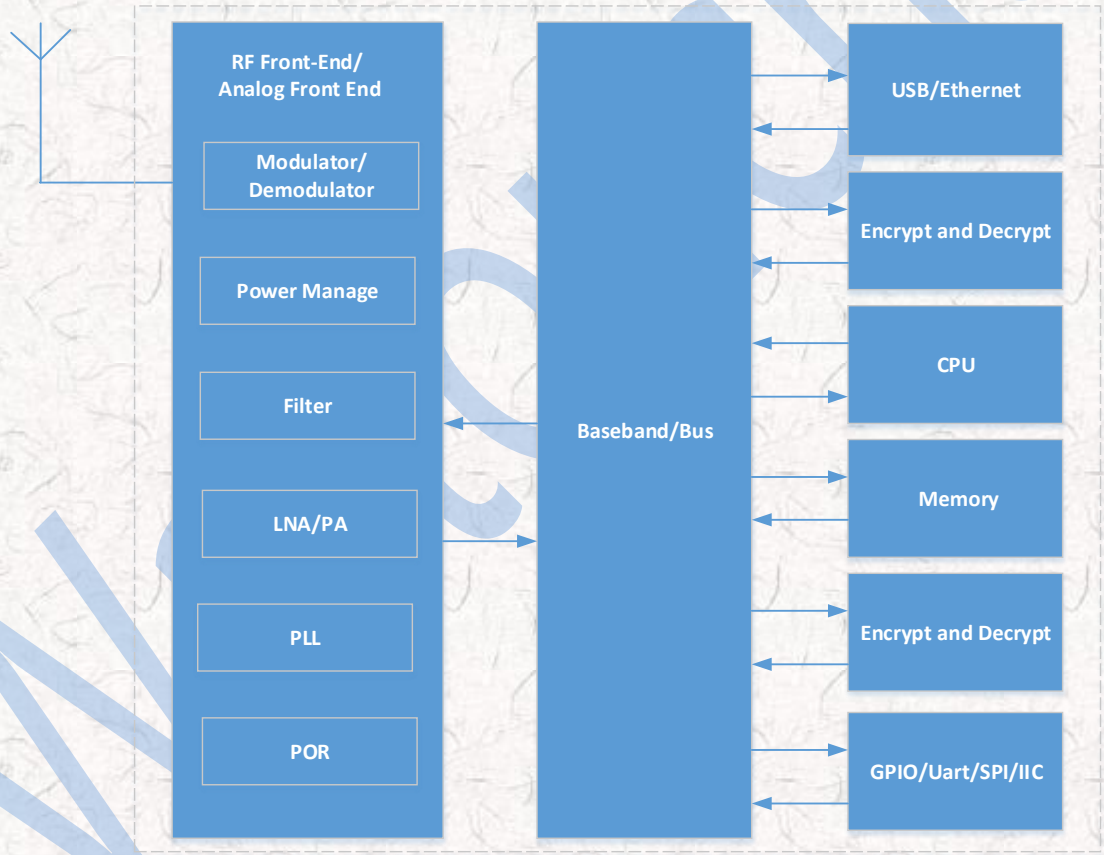


Figure 2.5: The project's tag IC solution block diagram

The project's IC design has the following significant advantages:

1) High security: The chip integrates asymmetric random password pair generation logic, uses a core asymmetric encryption algorithm with independent intellectual property rights and an optimized design without increasing the cost and power consumption of the chip, enabling higher communication security;

2) Optimized anti-collision design: The chip uses a binary tree anti-collision algorithm with independent intellectual property rights and a time division multiple access design, significantly improving the tag recognition success rate and the number of identifiable tags at the same time;

3) High sensitivity: The chip uses an optimized noise suppression technology to improve the noise factor at the receiving end and the overall receiver sensitivity, which plays an important role in increasing the recognition success rate; all these features enable the chip to have a greater advantage in application in the Internet of Things.

4) Good compatibility: The chip can achieve high-frequency and ultra-high frequency functions at the same time, the end customer can read the information and inquire about reliable product information through a smartphone.

2.3 The Software of the Value Internet of Things

2.3.1 The Interpretation of WALTON

WALTON is derived from Charlie Walton, who was born in California, died on November 30, 2011. As the inventor of RFID technology, he devoted his life to the development of RFID technology. He obtained the first patent related to RFID technology in 1973 and eventually obtained more than 50 invention patents. He started a new era of RFID and made outstanding contributions to the development

of RFID. At present, RFID technology is widely used in various applications all over the world, from identification to freeway billing, mobile and credit card payment; we can see RFID everywhere. The project was founded on November 30, 2016, the fifth anniversary of the death of Charlie Walton. To commemorate the great inventor of RFID technology, the project was named "Waltonchain" to carry forward his invention and blaze a trail to the future.

The interpretation of WALTON is as follows:

WALTON = Wisdom Alters Label, Trade, Organization and Network.

W — Wisdom

A — Alters

L — Label: RFID label

T — Trade: trade mode based on the accounting mode of blockchain

O — Organization: Organizational management model — decentralized autonomous organization (DAO)

N — Network: the Internet of Things — P2P network mode

2.3.2 The Overall Structure of Waltonchain

The Waltonchain ecosystem uses an overall structure including a parent chain and subchains (or child chains) where the parent chain is Waltonchain and the token used for circulation and payment is called Waltoncoin. During the 1.0 stage of the project, the parent chain — Waltonchain — is used to open up a complete supply chain system of the apparel industry, including production, logistics, warehousing and stores. Theoretically, there can be an infinite number of subchains. For example, recognizers of a production workshop used to monitor product quality can be used as nodes of a production subchain, and the production workshops of a variety of brands together constitute the production subchain. For

another example, stores of a variety of apparel brands can constitute a sales subchain.

The Waltonchain platform uses a hierarchical structure, including the bottom layer, core layer, middle layer and application layer; the platform architecture is shown in Figure 2.6.

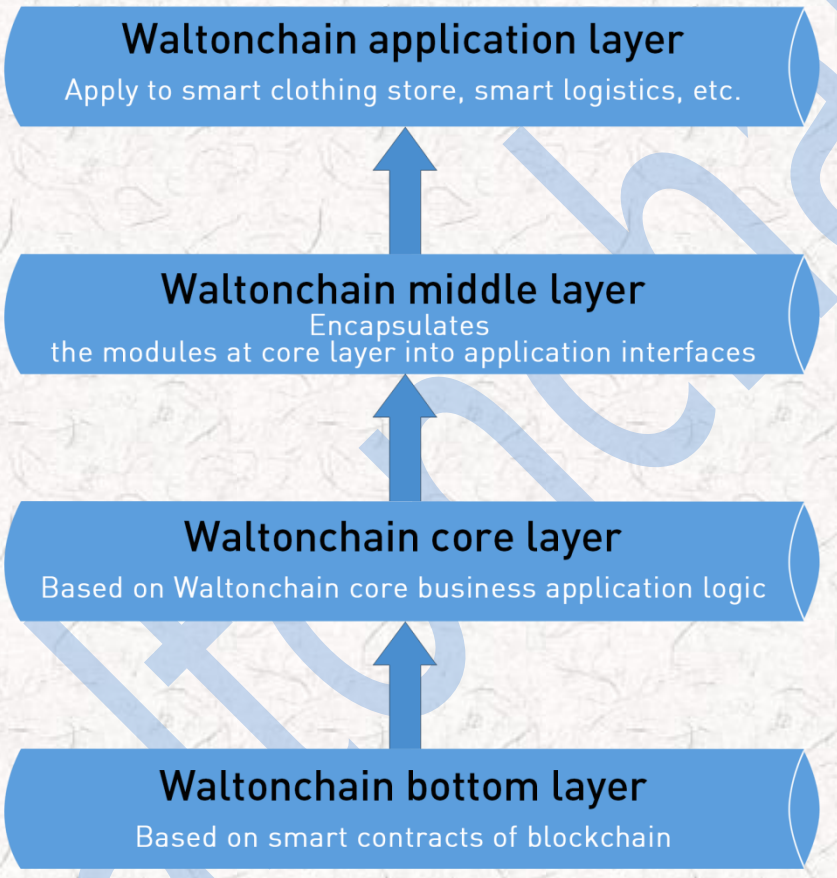


Figure 2.6: Waltonchain platform structure

Waltonchain Bottom Layer

The bottom layer is developed based on Waltonchain. Waltonchain has many advantages, please see the introduction of Waltonchain for details.

Waltonchain Core Layer

Waltonchain is developed based on the universal blockchain technology. To meet common and individual requirements of different applications, the core layer will include common and personalized features as a package to form core modules of different applications.

Waltonchain Middle Layer

For different applications, Waltonchain has dedicated and common interfaces to call for the application layer. The middle layer is used to achieve the package of these interfaces, thus simplifying the work of the application layer and reducing the application difficulty.

Waltonchain Application Layer

As for the top-layer content, users or the Waltonchain team can develop an appropriate platform or environment based on different application scenarios to meet individual, team or business needs of an application.

2.3.3 Waltonchain Protocol and Waltoncoin

The detailed structure of Waltonchain

The detailed structure of Waltonchain is shown in Fig. 2.7 below. Clothing industry application was selected as an example to show the subchain structure.

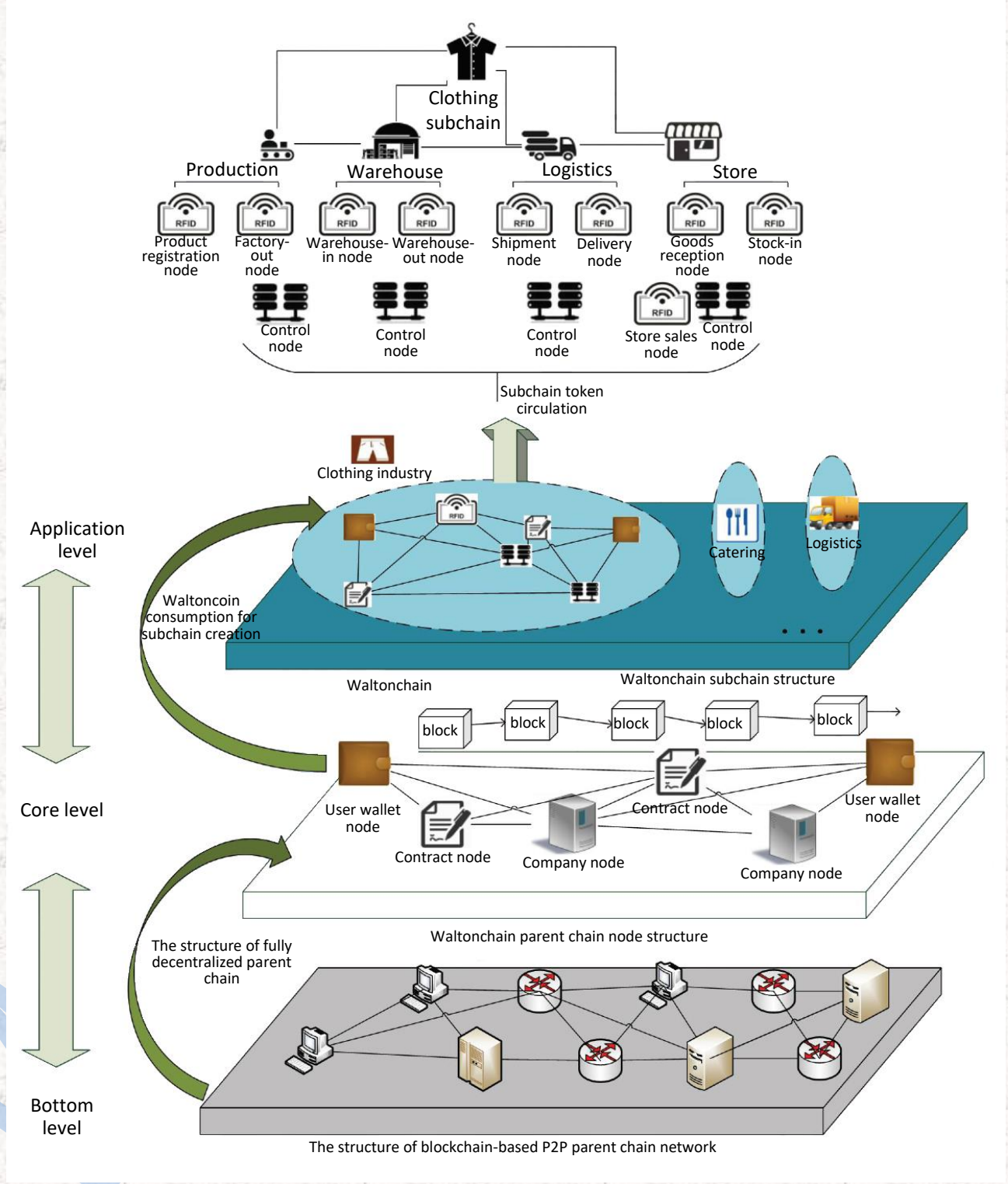


Figure 2.7: The detailed structure of Waltonchain

Waltonchain Parent Chain

The Waltonchain parent chain is the main chain of the Waltonchain blockchain, starting from the Waltonchain Genesis Block, which provides a wealth of functions including but not limited to Waltoncoin (WTC) transaction management, subchain management, smart contract, alias and account control, etc.

1) transaction management

A total of 100 million of WTCs are issued, created in the genesis block and assigned to each account in accordance with established program. The total amount of WTCs in the subsequent transactions remains the same. Through the decentralized network, more accounts will be created through the nodes, and a lot of WTC transactions will also be carried out between the accounts. Every 60 seconds, all the transactions during the current period will be recorded to a block, linked to the previous block, forming the Waltonchain parent chain. The parent chain is the public ledger of WTC transactions stored dispersedly in nodes in the network to ensure safety and reliability of transaction data.

2) subchain management

Another major function of Waltonchain parent chain is the management of subchain which can be created by any account at any time after the parent chain runs. The creator can customize the detail functions of the subchain and specific information of the subchain tokens. This custom information forms the data structure describing the subchain, which is recorded in the block of the current period by the accounting nodes in a way similar to the WTC transaction record. So far this subchain will be used as a separate blockchain, recording the transactions of the subchain tokens.

Since the WTC transactions are only recorded in the parent chain, the parent chain runs independently of the subchain. The nodes running on the parent chain only need to save the parent chain data to conduct consensus and validation of WTC transaction blocks. This flexible creation mechanism of WTC subchain makes subchains scalable, the state of subchains has no effect on the completeness and safety of the parent chain; except for recording the subchain description information, the number of subchains will not increase the size of the parent chain.

3) smart contract

In the system architecture of the Waltonchain blockchain, the smart contract based on its programmable features is responsible for building the underlying logic platform and supporting the operation of the upper architecture layers, namely the core layer, the middle layer and the application layer. It is the cornerstone of Waltonchain, which enables it to develop a wider range of custom applications.

Smart contract technology is developed by Ethereum and has been applied in the electronic token release, electronic crowdfunding, electronic contracts, electronic equity distribution and other fields. The Waltonchain blockchain technology defines two types of account concepts: one is the general account storing the tokens; the other is the smart contract account storing smart contract procedures. When a transaction is sent to the smart contract account address, the corresponding smart contract procedure will be triggered and implemented. The procedure will use the data of the received transaction, the data stored in this account and the current block status data as input data, will perform the customized operations, make transaction requests, modify the account status data and execute other result behaviors.

4) other functions

Decentralized asset transactions: supporting the decentralized asset transactions of the parent chain WTCs and subchain coins;

Decentralized grading system: grading according to the performance of the account nodes' trading behaviors such as mortgage;

Decentralized alias system: facilitating the realization of the transactions by alias;

Account control;

Voting system;

Cross currency transactions;

Waltonchain Subchain

1) subchain functional features

During its creation, a subchain can be customized to support all the functional features of the parent chain, or can be limited to certain functional features to achieve the customization of the appropriate features. The supported custom features mainly include subchain token transactions, subchain token and parent chain token transactions, cross subchain token transactions, smart contracts, aliases, voting system, account control, instant messaging and data storage.

2) subchain token transactions

By customization, the subchain can support subchain native token transactions, subchain token and parent chain token transactions and cross subchain token transactions. When a cross token transaction is made, the holder of the token makes a transaction request, the transaction request information contains the transaction type (buy or sell), the local token type, the target token

type, transaction price and the number of transaction tokens. Then the Waltonchain protocol will match the buy and sell transactions in a decentralized way, which is open, fair, reliable and traceable compared to the traditional trading centers.

Block Structure

The trading ledgers of WTCs are stored in the Waltonchain blocks that are series connected, forming the Waltonchain parent chain and subchains. These blockchains are stored in many nodes on the Waltonchain network, making the WTC transaction records open, safe, decentralized, traceable and tamper-resistant. The core component of this ambitious, secure and decentralized data structure is the block data structure designed by the Waltonchain team. It provides the parent chain with the features of safe, stable and fast response and provides subchains with a flexible combination of features, so as to adapt to a variety of Internet of Things applications and to match customized business models.

A Waltonchain block can contain up to 255 transaction records. Each transaction record contains a header carrying the identification information. The general information contained in the block is as follows:

Block depth and timestamp

Block identity

Block account ID and public key

The identity of the previous block and the hash value

The total number of tokens of the transactions contained in the block and byte fee

The transaction information contained in the block

Block payload length and payload hash value

The generated signature of the block

Accumulated coinage difficulty of the block

Consensus Mechanism

1) PoST Consensus mechanism

The Waltonchain parent chain conducts block consensus and validation based on the Proof of Stake & Trust (PoST) consensus mechanism. PoST is an innovative updated version based on the Proof of Stake (PoS) consensus mechanism.

The traditional PoS is a distributed consensus algorithm, which is an upgraded version of the Bitcoin Proof of Work (PoW) consensus algorithm. In the PoW consensus algorithm, the nodes involved in the consensus need to continue trying to solve the problem of cryptography, to confirm the transaction, then write into the block and get tokens as a reward. In most cases, this reward comes from the unallocated tokens, so the process is vividly called mining. Because the mining is more and more difficult as the "mineral resources" reduce, a lot of computing resources tend to be wasted. In the blockchain network based on the PoS consensus algorithm, in most cases, all the tokens are issued from very beginning, then the block is successfully created and written into the accounting nodes of the blockchain; the accounting reward is the byte fee paid by the transaction initiation node, so the consensus mechanism is vividly called coinage. The more the tokens held by nodes are involved in the consensus and the longer the time to hold the tokens is, the bigger the opportunity to successfully complete the block creation and writing are. This mechanism greatly reduces the operation difficulty of accounting, saves valuable computing resources and at the same time provides a

mechanism of selecting "good" accounting nodes to strengthen the security of the blockchain.

Waltonchain constructed an innovative node reputation evaluation system which added a node reputation mechanism to adjust the difficulty of coinage based on PoS and highlight the importance of reputation in business ecology, and creatively designed the PoST consensus mechanism. This consensus mechanism brings two positive effects: first, based on the commercial credit link of a combination of Waltonchain blockchain and RFID, it can further promote and train the integrity behaviors of the involved nodes through the information evaluation mechanism, for example, keeping good credit record in credit mortgage and other transactions, to cultivate a healthy business ecology; second, it provides an upgraded selection mechanism to choose more honest "high quality" nodes as coinage nodes, improving the security of the blockchain.

2) Other consensus mechanisms

The flexible structure of Waltonchain blockchain determines that the subchains can choose PoS, PoST or other consensus mechanisms to achieve the optimal application effect in different application scenarios.

By issuing different subchains, Waltonchain connects different types of Internet of Things nodes to apply to various scenarios in the business ecology. Due to the diversity of the Internet of Things, sometimes the Internet of Things needs many nodes online at the same time, which is quite different from the Internet, so we propose an innovative solution which sets the consensus mechanism flexibly based on the different application scenarios, to meet different application requirements.

Byte Fee Allocation

The byte fee is the cost paid by the transaction initiation node to the accounting node, which is used to pay for the occupancy of network bandwidth and blockchain bytes in the process of paying the transaction. The accounting node can set the minimum cost that can be accepted, and the transaction initiation node can set the maximum cost to be paid. When both conditions are met, the transaction will be successfully written to the blockchain.

The byte fee is the source power driving the blockchain to account, as the accounting node performs block calculation and consensus verification to obtain the byte fee; the node needs to pay the transaction surcharge to initiate the token transaction and the subchain creation.

1) allocation of byte fee for token transactions

Waltonchain supports parent chain token transactions, subchain token transactions and cross-chain token transactions. When dealing with various types of token transactions, the transaction initiation nodes need to pay the byte fee with parent chain tokens. This can make the parent chain token become the single token used as a reward token of the parent chain accounting node and the subchain accounting node, finally achieving the following two positive effects.

First, the parent chain and each subchain can share the accounting nodes in the network to the maximum, so that the accounting nodes will freely choose different parent chains and subchains based on the profit efficiency, without fear of inconvenient exchange and paying multiple byte fees, which is beneficial to the reasonable allocation of the node resources. And for some of the subchains in the early stages of the establishment, there is no need to worry about the problem of insufficient accounting nodes, because they can share the accounting nodes of the parent chain and other subchains.

Second, when more subchains are created and the subchain transactions become more and more frequent, the demand for the parent chain tokens which are used as the currency to pay for byte fees will rise; since the number of the parent chain tokens remains the same, the value of each parent chain token will increase. As a result, the nodes holding the parent chain tokens will gain an interest from subchain development as the number of the subchains and transactions increases.

2) allocation of byte fee for subchain creation

The Waltonchain parent chain supports the creation of subchains. When creating a subchain, the account that creates the nodes needs to pay the byte fee with parent chain tokens, to prevent the malicious creation of many subchains. Parent chain tokens will be obtained as a reward for writing the block containing the description of this subchain into the accounting node of the blockchain.

Waltoncoin

As mentioned above, in the Waltonchain ecosystem, the most core parent chain is called Waltonchain in which the token used for circulation and payment is called Waltoncoin (hereinafter referred to as WTC). WTC is the most important digital token in the Waltonchain ecosystem. The total number of WTCs is 100 million (10^8), they were created and are located in the Genesis Block. This number is constant, and no more tokens will be issued.

Waltoncoin's Main Functions

1) issuing subchains

WTCs need to be consumed to issue subchains, such as the production subchain, the storage subchain, the logistics subchain and the sales subchain. Of

course, issuing subchains is not the privilege of the Waltonchain team, as any Waltonchain ecosystem user can consume WTCs to issue its own subchains in the Waltonchain ecosystem.

The consumed WTCs are allocated to the accounting node wallet to support the parent chain. This is how the PoST mechanism is realized.

2) reward interest distribution

Waltonchain team officially issues basic subchains, such as the sales subchain used in stores (assuming the token is A coin) and the transaction subchain used in the retail industry (assuming the token is B coin). In the above high-frequency circulation sections, even if the transaction fee for each transaction is very small, many small fees can add up to a substantial number. Therefore, in order to ensure the robustness of the subchains and the parent chain at the same time, the allocation mechanism regarding the consumed fees needs some innovative adjustments. The majority (e.g. 90%) is assigned to the accounting node wallet of the subchains, and the minority (e.g. 10%) is assigned to the accounting node wallet of the parent chain.

3) credit and mortgage system

The account on the parent chain can form a credit mechanism. As the circulation and consumption amount of subchains increases, the credit rating of the corresponding account of the parent chain increases. Here is an application scenario: a customer needs to pay for his consumption at A store, A store supports A coins, but the customer does not have any A coin, then the customer can pay by mortgaging parent chain WTCs (in a frozen state), A store and the customer sign a smart contract on the chain automatically to set an agreed time to return A coins when such WTC coins will be unfrozen. Correspondingly, the credit rating of this account increases and the number of WTCs needed for mortgage decreases.

However, if the A coins fail to be paid back, the number of WTCs frozen for mortgage will increase correspondingly.

4) distributed asset exchange

If we exchange assets on the parent chain, the parent chain will be able to exchange the assets of any subchain tokens on any subchain. This allows the subchains to interact with each other and opens up many collaboration opportunities to allow cross-chain asset transactions, which is also a required function in the Waltonchain ecosystem in the long term.

5) distributed voting and governance system

This system will be the core of decentralization in the future. Safe and anonymous voting will be available for all subchains on the parent chain.

6) decentralized exchange

All the coins on the subchains can be traded in the decentralized exchange on the parent chain, where the digital currency used to act as an intermediary is WTC.

Of course, only some of the core functions of WTC are mentioned above. WTC has more functions, and as the project progresses, the Waltonchain team will give WTC more advanced features.

2.3.4 Waltonchain ecosystem

An example of Waltonchain ecosystem application for the apparel industry is shown in Figure 2.8 below.

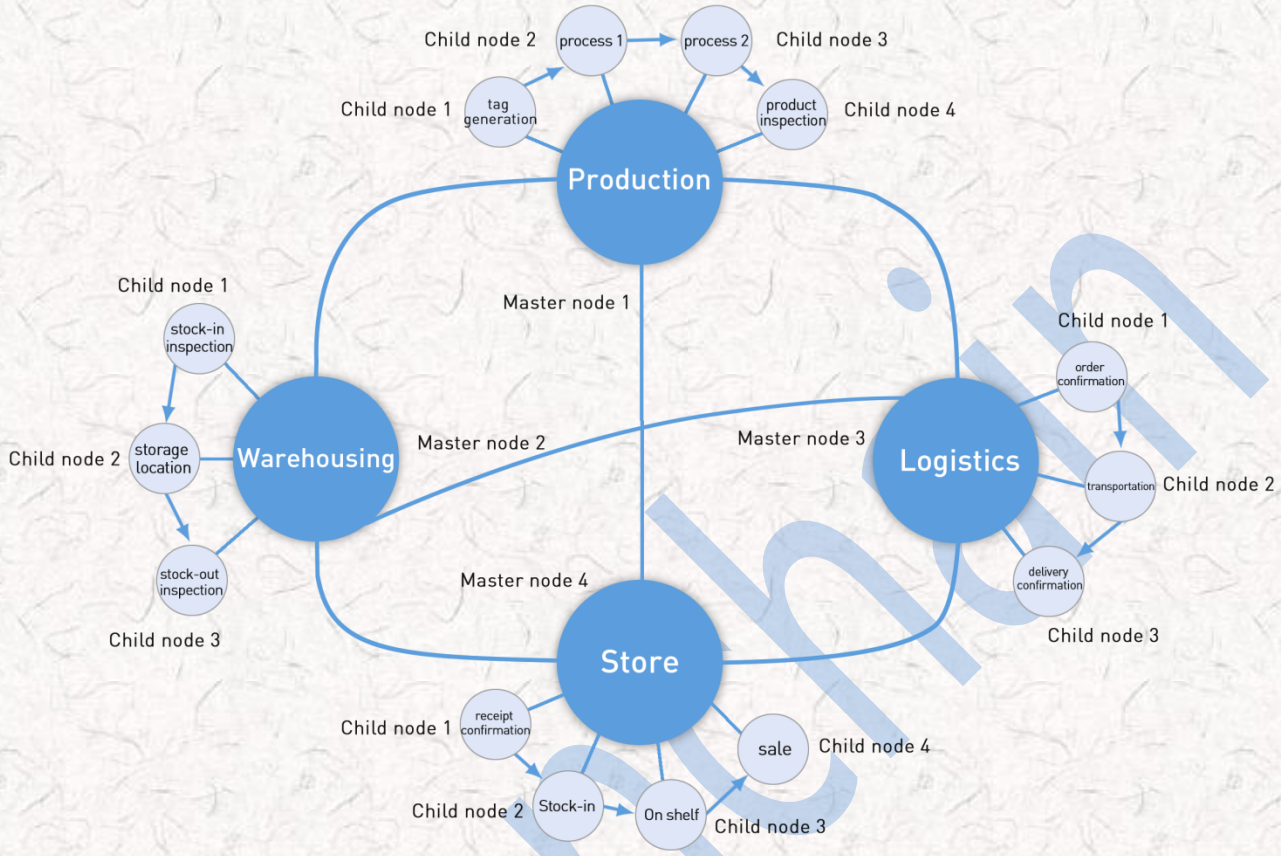


Figure 2.8: Waltonchain ecosystem 1.0 stage

The whole ecosystem is composed of several master nodes and child nodes, so the ecosystem is not limited to the applications in the apparel industry, but also applicable to the fields of warehousing, logistics, electronic license plate and asset management. Here we only take a simple example to explain the application in the apparel industry.

Production

In the early stage of production, the production target is made according to the production plan and related needs. In the first phase of production, a unique RFID will be generated for each product. The status and related information of this ID will be recorded at each child node in the production, also at each subsequent master node and corresponding child node. The contents of the status and

information are negotiated by the master nodes. Each node is rewarded according to the contribution in the form of Waltoncoin. The number of awards can be determined based on the workload or the work quality of the corresponding node or the specific situation of the application.

Warehousing

This node mainly refers to the storage after production, containing three sections: warehouse-in inspection, storage location and warehouse-out inspection. Each section has a corresponding reader to record the corresponding information and form a corresponding block in this master node of warehousing to connect with the block generated in the production.

Logistics

This node is similar to the previous one, it mainly records the status and information in the process of transportation and forms the corresponding block data.

Stores

This node can be a store, or many stores. Each store is regarded as a master node to record the status and information of the product as well as customer information and preferences. This node can give a customer the corresponding reward according to the customer's consumption situation in the form of Waltoncoins and include the customer into the master node according to the amount of Waltoncoins held by the customer and give the customer the appropriate permissions. The customer can check all product information and all billing data, but needs to pay certain Waltoncoins. The customer can also use Waltoncoins to purchase the corresponding products.

Main Characteristics of the System

1. Each child node is equipped with a reader and connected to the master node;
2. The master node is connected to the Internet, it is online in real time;
3. Each master node manages the bills. The data between the master nodes are transparent;
4. After the nodes reach a consensus, the number of various master nodes can continue to increase;
5. According to the amount of Waltoncoins held by the purchaser, the purchaser can be included in the node after the nodes reach a consensus and vote for the rights of accounting and checking to be authorized to the purchaser;
6. Checking bills and accounting will consume Waltoncoins (as handling fees);
7. The purchaser can also directly pay Waltoncoins to purchase clothing.

Main Advantages of the System

1. Can really achieve tracing the source;
2. Can really achieve the purpose of unforgeability;
3. Can achieve decentralization without the concern of trust;
4. Can reduce labor costs.

Multi-User Consensus Security Mechanism

1. The mechanism generates a set of random numbers by the master node;
2. Divides this set of random numbers into N parts (N is an integer and greater than 2/3 of the number of all users);
3. Encrypts N parts of random numbers with the public key of N users separately;
4. All users decrypt this set of random numbers with their own private key;
5. When the master node receives all the correct data, it is considered that this accounting or modification is valid.

2.4 Application Scenarios: Waltonchain Project's System Solutions for the Apparel Industry

With the rapid development and integration of the Internet of things, mobile Internet, cloud computing and other information technology, the intelligent management of information has become a key factor in the rapid growth and improvement of enterprises. As a core technology of Internet of things, the RFID is widely used in the intelligent warehousing and logistics management, and the apparel industry is one of the most promising fields for applying RFID technology.

Due to the apparel industry's particularity and complexity, thorny problems exist in various links in the value chain of traditional apparel industry, including logistics, warehousing, sorting business, store sales and inventory. For example, complex product specifications with various size, styles and rapid changes; frequent unpacking and messy piles; slow turnover in warehousing management, production, inventory and distribution; great reliance on staff experience for

searching needed commodity; big difference between stock-in and stock-out; difficulty in taking inventory; heavy workload; FCL and one-piece warehousing modes coexist; impossibility of tracing the clothing sources. Therefore, pasting, embedding or implanting RFID tags on the tag of each piece of clothing can increase supply chain management transparency and inventory turnover, reduce the loss due to out of stock, enhance the store experience and increase consumer satisfaction, while conducting real-time intelligent data analysis and collecting data to guide the garment enterprises to adjust their product design, production and inventory in a timely manner.

2.4.1 Analysis on the Dilemma of the Traditional Apparel Manufacturing

The 13th Five-Year Plan for China's apparel industry clearly points out that we need to speed up the construction of flexible supply chain management system and intelligent warehousing, logistics and distribution system with RFID as the core, to improve the system functions and the adaptability of business process reengineering, to achieve a seamless connection of various management systems, to promote big data, "Internet +" and other technology applications, to improve the intelligent level of managerial decision-making, to vigorously promote the mass customization technology and its manufacturing model, to promote the transformation from garment manufacturing to garment services and to promote the deep integration of manufacturing and services and to enhance the application level comprehensively.

In recent years, the overall retail sales of the apparel industry grew steadily, the total domestic sales volume has been increasing, online channels expand rapidly, the growth rate of offline sales going down, the domestic market loses

momentum and export faces major difficulties. The apparel industry needs to speed up structural adjustment, transformation and upgrading.

Facing the "new normal" of slow growth and steady total volume the traditional manufacturing companies are impacted by, the clothing manufacturing section is compelled to upgrade in order to improve the competitiveness of garment enterprises. The apparel manufacturing is transforming from the mode of large quantities, less varieties and long cycle to the mode of small quantities, more varieties, short delivery and customization.

2.4.2 Smart Manufacturing Solution for the Apparel Industry

The traditional apparel industry is a labor-intensive industry characterized by overall multi-variety, rapid changes and relatively low level of informatization and intelligentization. The production process is shown in Figure 2.9.

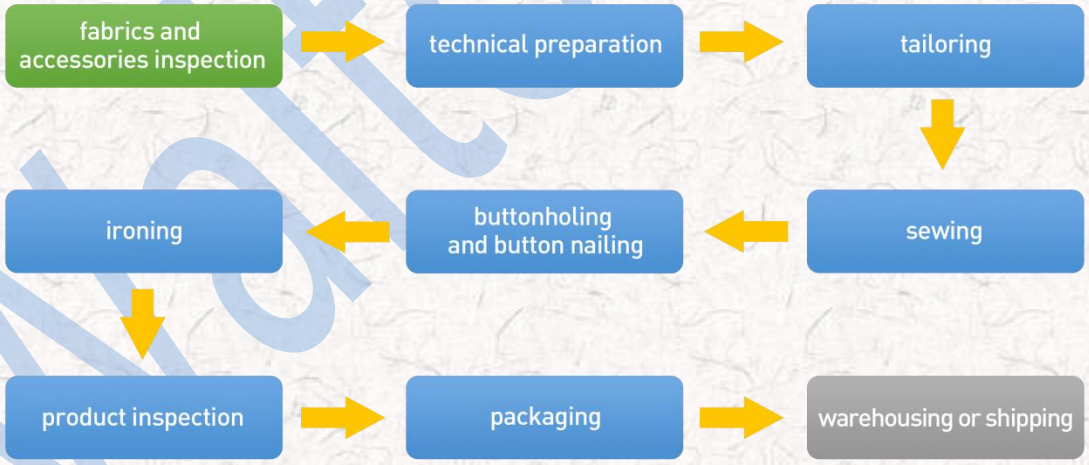


Figure 2.9: Traditional garment production and processing flow diagram

Based on the above characteristics, the future intelligent garment factory is a Customer to Manufactory (C2M) customization platform; the consumer demand directly drives the effective supply of the factory, as shown in Figure 2.10.

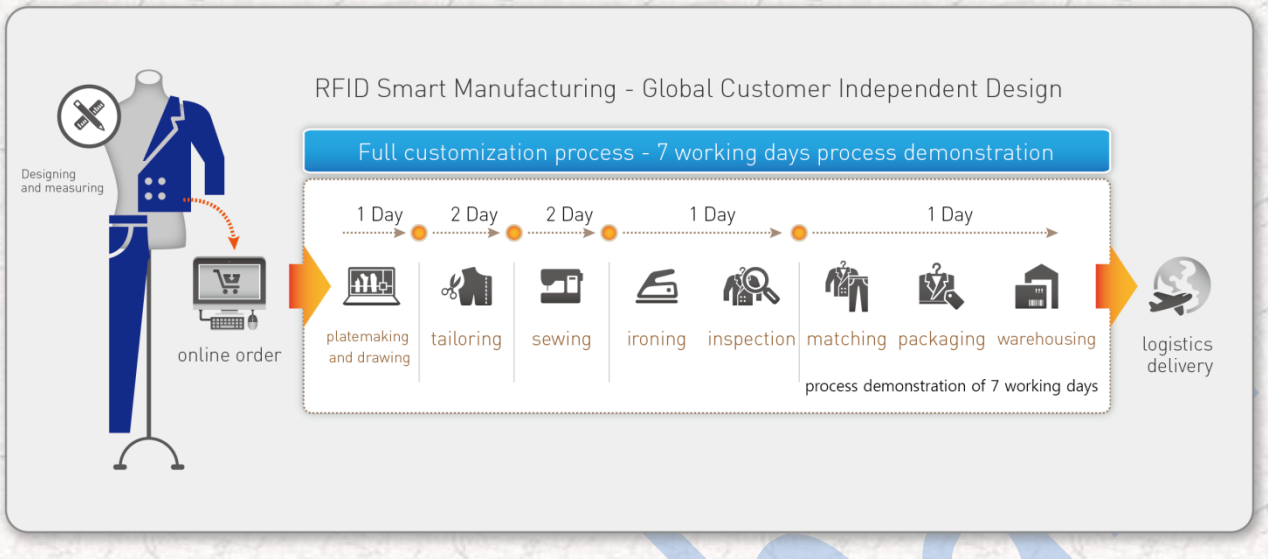


Figure 2.10: An example of an intelligent garment factory

So, with a data-driven production process, online design, order-taking, customization data transmission are all digitalized, forming an operating system of demand data collection, demand data to production data transformation, smart research and development and design, smart production scheduling, smart automatic typography, data-driven value chain collaboration, data-driven production, data-driven quality assurance, data-driven logistics and distribution, data-driven customer service and fully digital customer service. As shown in Figure 2.11, the RFID-based smart production line greatly improves the efficiency of industrialization, shortens the production cycle to 7 working days while the personalized manufacturing costs are only 10% higher than those of the mass manufacturing, truly realizing the mass customization of personalized products. Everyone will be able to afford customized clothing.

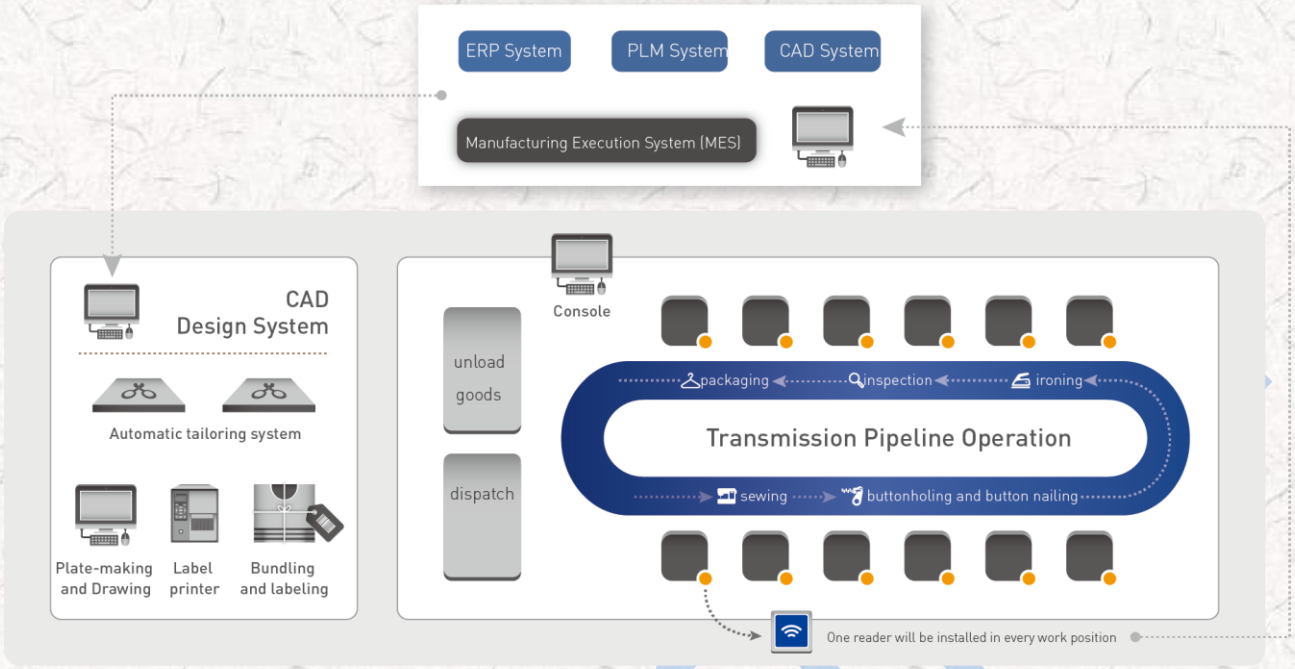


Figure 2.11: RFID-based intelligent production line structure diagram

2.4.3 Smart Logistics & Warehousing Solution for the Apparel Industry

The apparel industry logistics has the following characteristics: diverse management objects, various brands, diverse types, many SKUs (Stock Keeping Unit); diverse sales models, complex logistics channels, generally including "online + offline" model and "directly managed stores + franchises + agents" model; strong seasonality, rapid logistics response required, different products for spring, summer, autumn and winter, short product life cycle, usually 2 to 3 months; difficult inventory control, long production and marketing chain, many sections, multi-level segmented inventory, generally including factory inventory, headquarters inventory and channel inventory; multi-stage network for logistics and distribution, including Headquarters logistics distribution, branch logistics distribution and agent logistics distribution.

The apparel logistics network is a three-tier separated network where a variety of logistics channels coexist, usually with a model of raw materials and accessories distribution + finished product distribution + terminal distribution by factories + headquarters + subsidiaries . The types of business operation include wholesale, retail, e-commerce and group purchase. The products include different logistics channels of various brands. The logistics problems are as follows: long logistics channel, the overall logistics channel includes factory warehouse — headquarters warehouse — subsidiary warehouse — store or factory warehouse — headquarters warehouse — agent/dealer warehouse; high supply chain inventory, low storage efficiency, too many inventory points, the storage cycle is usually 180 days, with backward warehousing management methods and means; multi-stage transportation, complex management, the transportation modes include container shipping by the factory, distribution and transportation by the headquarters, distribution and transportation by the branch/agent, etc. Based on the above characteristics of the logistics, we put forward a smart storage solution shown in Figure 2.12.

Figure 2.12: The intelligent warehousing solution

2.4.4 Smart Store Solution for the Apparel Industry

Figure 2.13 shows the functional scenes of a smart store. At the point of arrival, before the goods go into the store, the staff shall use RFID PDA to batch read the data on the clothing tags, match with the receipt, check the quantities and models of goods and correct errors manually.

Figure 2.13: Smart store functional scene diagram

Specific functions are as follows.

Quick stocktaking function: the staff uses the PDA to collect clothing label information and transmit to the background server for data comparison, the difference is displayed on the PDA in real time for manual check and the stocktaking information on the back-end server is updated through the PDA.

Quick find function: the staff enters the label information of the product to be found into the RFID PDA to turn on the search mode and quickly locate the specific location of the product according to the beep produced based on the strength of the signal.

Smart hanger function: when the customer picks up the clothes on the smart hanger, the smart hanger automatically identifies the clothing label in the hands of the customer, the touch screen displays all the information of the clothes in a timely manner and inputs the data into the background server at the same time;

the analyzing software automatically counts the data and generates statistical reports of each period for managers to view.

Smart fitting room function: when the customer picks up the clothes and walks into the fitting room, the smart fitting room automatically identifies the clothing label in the hands of the customer, the touch screen displays all the information of the clothes in a timely manner and inputs the data into the background server at the same time; the analyzing software automatically counts the data and generates statistical reports of each period (hour/month) for managers to view and estimate the production plan and popular designs according to the fitting rate.

Quick check-out function: with RFID, the target information can be identified automatically, the receiver can read multiple tags at once within its effective working range to achieve the simultaneous identification of multiple products, thus speeding up the check-out process and improving customer satisfaction.

Figure 2.14 shows a smart fitting room. Icons 1 & 2: the staff reads the clothes label and transmits the data to the service desk; icon 3: the service desk pushes information to the match system for selection; icons 4 & 5: the customer chooses the product to try and informs the help desk; icons 6 & 7: the staff uses the PDA to quickly find the product and sends to the customer.

Figure 2.14: The smart dressing room functional scene diagram

With RFID system solution developed by the Waltonchain team based on the blockchain technology, the end customers can use bar codes or RFID tags to identify all system information of every clothing product, including accessories, fabric, production process, logistics and distribution and store it in the blockchain system. For brands in the clothing business, the functions of tamper-resistance, reliability, anti-counterfeiting and traceability can be achieved. Once the companies find any problems, they can effectively control and recall products according to the source tracing and protect the legitimate rights and interests of consumers fundamentally. Consumers can rest assured to buy their favorite products; the system enhances shopping experience and improves consumer satisfaction.

Part 3 Future — Value Internet of Things Will Change the World

3.1 The Stage Planning of the Waltonchain Project

As mentioned above, the realization of Value Internet of Things will create a new ecology of the existing business, which is based on the organic integration of the blockchain and the Internet of Things. The combination of RFID technology and Waltonchain will extend the blockchain technology from the Internet to the Internet of Things and create an authentic, trustworthy, traceable and fully transparent business ecosystem with fully-shared data. The Waltonchain team carefully planned four growth stages starting from building the underlying foundation, gradually extending to a retail and logistics network and finally integrating product manufacturers. Step by step, in the forthcoming future Waltonchain will achieve the full coverage of commercial ecology.

During the Waltonchain Project 1.0 stage, the team has developed a clothing system integration solution based on RFID technology, which has been applied in several pilots such as Tries, SMEN and Kaltendin. Now we are ready for large-scale promotion and need to lay a solid customer base. We have started to develop the RFID beacon chip with independent intellectual property rights, which innovatively integrates an asymmetric encryption algorithm based on the traditional RFID chip and expected to achieve the perfect combination of Internet of Things and blockchain. Combined with the integrated solution for the apparel industry based on RFID technology, it is expected to solve the problems of the traditional apparel industry including warehousing, logistics, stores and aftermarket, and in the meantime, to consolidate the basic platform of Waltoncoin. The application

scenarios of the project's 1.0 stage will build a Golden demonstration template for the rapid promotion of Waltonchain's applications.

During the Waltonchain Project 2.0 stage, the independently developed RFID beacon chip will be in full mass production and can be used in B2C retail industry and logistics industry. Development of a smart credit system will be completed, fully integrating payment, gifting, same currency transactions, different currency transactions, etc. through Waltonchain's flexible and powerful token creation and transaction functions. Availability of complete information, including merchandise procurement, distribution, stock-in, stock-out, stores, shelves inventory, sales, customer purchase, customer evaluation and after-sales service, on the chain will be achieved through an optimized blockchain data structure design. Customers will be provided with such functions as payment, integral management and trading, product evaluation and query, tracing and obtaining evidence for a quality problem, etc. Merchants will be provided with automatic management of business operations, information mining during procurement, sales, after-sales and information on real-time market trends. Thus a win-win-win situation will be achieved for all three parties: customers, merchants and Waltonchain. By virtue of a blockchain data structure matching multi-scenarios, the logistics industry will be able to achieve availability of full path logistics information on the chain, covering the complete business process including pricing, packing, sorting & distribution, warehouse management, sorting & sending, home delivery, customer receipt and customer feedback. Based on characteristics of RFID such as being tamper-resistant, open, traceable etc., the stage is aimed at building a safe and reliable point-to-point logistics information channel for customers and provision of a business automatic management information platform for logistics companies to avoid thorny problems, such as lost, delayed and wrong orders on a systematic basis.

During the Waltonchain Project 3.0 stage, the technology will be applied to all product manufacturers to achieve smart packaging and traceable customization. The universal data structure used in describing the production cycle will be effectively written to the blockchain. The customized data structure will be designed for different products. With RFID identity verification, the authenticity and reliability of the information added to the chain is guaranteed. The whole process will be covered, including raw material purchasing, production operations, assembly operations, product packaging and product inventory management. Raw material sources and production quality can be verified and the quality problem source can be tracked by taking the advantages of openness and traceability of blockchain. The possibility of counterfeit can be eliminated and the information barrier can be removed to ensure the consumers' interests fundamentally. At the same time, low-cost data information solutions can be provided to product manufacturers by means of standardized and reliable recording of manufacturing operation information via blockchain so as to achieve smart management for manufacturers.

During the Waltonchain Project 4.0 stage, with upgrading and iteration of the asset information acquisition hardware and improvement of the blockchain data structure, all the assets will be registered on Waltonchain in the future so as to solve the problems of asset ownership, item traceability and transaction certificate. By then, Waltonchain and Waltoncoin will be widely used in the physical world, fundamentally changing the way of life and production worldwide — Waltonchain project will bring a more convenient, intelligent and trustworthy world to everybody, and at the same time, give handsome returns to investors of Waltonchain.

In accordance with the four stages of the project, the project team will develop a variety of information collection-related chips, including dual-band RFID chips, biometric chips and various sensor chips. The team will not only provide

secure interfaces for all physical assets to be on the chain, but also provide secure interfaces for human beings, all kinds of animals, creatures to be on the chain, to realize safe and reliable networking, aggregation, digitization of all things, completely change people's way of life and bring more convenience to human life. The application scope of Waltonchain will be gradually extended to every life scene, as shown in Figure 3.1.

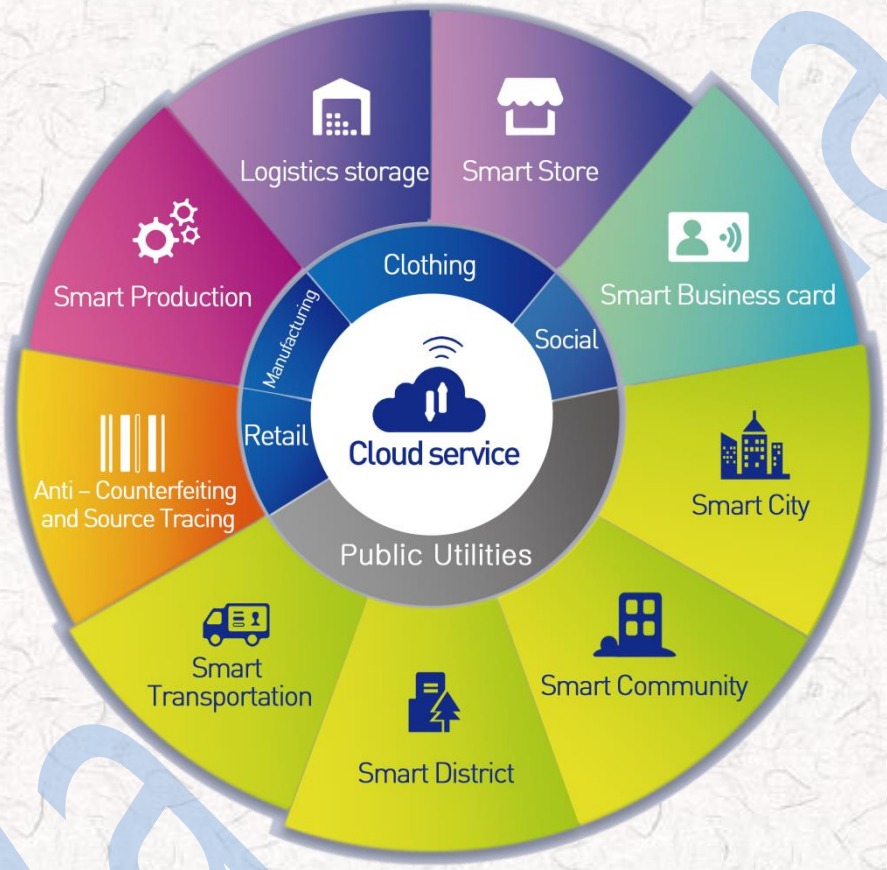


Figure 3.1: The scope of application of Waltonchain

3.2 The Investment Value of the Waltonchain Project

1) Innovation mode: the Waltonchain Project intends to develop an RFID beacon chip with independent intellectual property rights, which is expected to achieve the perfect combination of Internet of Things and blockchain. The researched and developed chips will bind Waltoncoins to create the intelligent

ecosphere of application of Internet of Things based on Waltonchain. During the course of expanding blockchain technology to the Internet of Things, Waltonchain will definitely become the leader of the changing times;

2) Market space: with a trillion-level potential market, Waltonchain has possessed the applicable program able to be quickly implemented in the total value chains in the clothing industry, including the production, storage, logistics, stores and other full circulation areas. Years of working experience and customer resources accumulated by the team members in the clothing industry and electronics industry will provide favorable conditions for the implementation of the project. In the foreseeable future, it is also expected to be used in many fields like electronic license plate and asset management, etc.;

3) High-frequency application: Waltonchain is loaded on the RFID hardware system to break through the bottleneck in commercial application of blockchain, namely, the problem of how real assets off the chain are chained quickly, efficiently and safely. Therefore, Waltonchain is a commercial ecological chain with a low threshold and high-frequency application where the range of application scenarios will be wide and popularity very high;

4) Ecological network: Waltonchain will establish the ecological chain of Internet of Things with its own content. As the only token of fundamental chain for this ecological network, Waltoncoin will be circulated in a wide range of business areas, so it has multiple significant functions including value storage, value circulation, credit trading, commodity payment medium etc. With the increasing popularity of RFID beacons and the expanding demand for the network, the demand for Waltoncoin will be expanding correspondingly, so Waltonchain's early investors will get substantial returns with the development and growth of Waltonchain.

5) Profit mechanism: Waltoncoins issued by ICO are the tokens of Waltonchain's parent chain. With the development of the parent chain and its subchains, according to the protocol mechanism of Waltonchain system, Waltoncoin, as the mother token, will receive dividends from all levels of the system in order to nurture the blockchain system of Waltonchain, making it more robust and safer and bringing about a harmonious virtuous circulation.

Part 4 Project Foundation

The project foundation was established in 2017, known as the Waltonchain Foundation. The Foundation is committed to the development of the Waltonchain project, the promotion and implementation of RFID applications and the promotion of early development of decentralized applications. 20% of the initial WTCs will be used for some industry applications and start-up projects, such as financial services, supply chain, Internet of things, blockchain, etc., including project strategic planning, project support, project promotion and token exchange. The Foundation will select the decentralized applications developed on Waltonchain and provide rewards based on the actual number of users on the applications.

The overall structure of the foundation is shown in Figure 4.1. The Decision-Making Committee shall have three subdepartments, including Technology Development Committee, Finance and Personnel Management Committee and Project Operations Committee, which shall be responsible for the development, implementation and supervision of technology development strategies; the development, implementation and supervision of the financial system; the decision-making and implementation of the overall project operation and marketing, respectively. The members of the Decision-Making Committee change every four years. The members generally include two representatives recommended by each subcommittee: a project investor representative, a community representative and a member of the Waltonchain team. The members of the subcommittees change every four years. The members are generally prominent people from related industries.

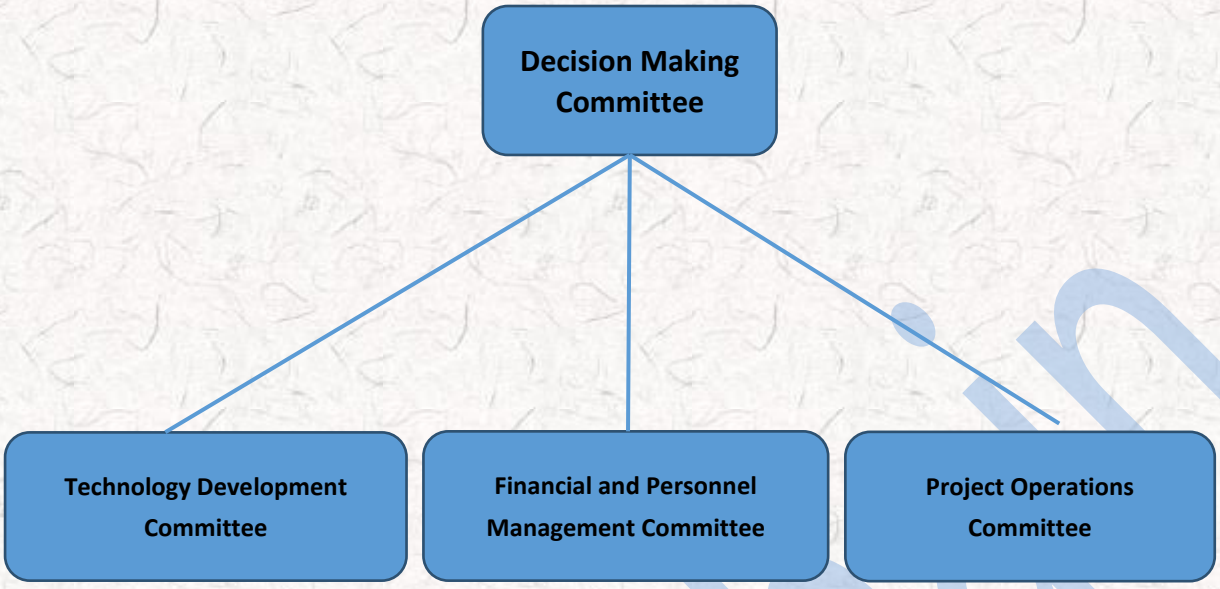


Figure 4.1: The overall structure of the Waltonchain Foundation

The Foundation promotes a transparent and efficient operational philosophy to promote the healthy development of the Waltonchain ecosystem. The governance structure mainly focuses on the effectiveness, sustainability and financial security of project management. The foundation's mission is to promote the development of blockchain technology from the Internet to the Internet of things and to invest the funds raised by ICO in the following directions:

1. Planning to develop the RFID beacon chips with independent intellectual property rights which use an asymmetric encryption algorithm with independent intellectual property rights and can achieve the perfect combination of the Internet of Things and the blockchain;

2. Establishing a smart credit system fully integrating payment, gifting, same currency transactions, different currency transactions, etc. through WTC's flexible and powerful token creation and transaction functions;

3. Availability of complete information, including merchandise procurement, distribution, stock-in, stock-out, stores, shelves inventory, sales, customer purchase, customer evaluation and after-sales service, on the chain will be

achieved through an optimized blockchain data structure design, which ends up with a win-win-win situation for customers, merchants and Waltonchain;

4. By virtue of a blockchain data structure matching multi-scenes, it is aimed at building a safe and reliable point-to-point logistics information channel for customers and providing business automatic management information platform for logistics companies to avoid thorny problems such as lost, delayed and wrong orders on a systematic basis.

5. Applying to the product manufacturers and achieving smart packaging and traceable product customization.

The projects above will provide convenient data query and traceability, analysis and processing and transaction management interfaces to customers, provide smart management interface to businesses. With the further application of machine learning and artificial intelligence, an intelligent ecosystem of the complete supply chain will ultimately be created, including a production, logistics, stores, sales and after-sales service.

Part 5 Team Introduction

第五部分 团队简介

5.1 Initiators

Xu Fangcheng (initiator in China): Chinese, majored in Business Management, former Director for Supply Chain Management of Septwolves Group Ltd., has rich practical experience in supply chain management and purchasing process management. Currently, he is the Director of Shenzhen Silicon, the Director of Xiamen Silicon and the Board Chairman of Quanzhou Silicon. He is also one of our Angel investors.

Do Sang Hyuk (initiator in Korea): Korean, Vice Chairman of the China-Korea Cultural Exchange Development Committee, Chairman of Korea NC Technology Co., Ltd., former Director of the South Korea Electronic News Media Bureau, Director of ET News, Former Director of Korean Standards Association, Chairman of Small and Medium-Sized Enterprise Committee in Seongnam, South Korea, Representative of Jiangsu Mingxing Liangcheng Environmental Protection Co., Ltd., China.

5.2 Senior Advisors

Kim Suk Ki (Internet of Things): Korean, one of the key persons in South Korean electronics industry, Doctor of Engineering (graduated from the University of Minnesota), Professor of Korea University, previously worked at Bell Labs and Honeywell USA, served as a Vice President of Samsung Electronics, senior expert in integrated circuit design, IEEE Senior Member, Vice President of the Korean Institute of Electrical Engineers, Chairman of the Korea Semiconductor Industry Association. He has published more than 250 academic papers and possesses more than 60 patents.

Zhu Yanping (blockchain): Taiwanese, Doctor of Engineering (graduated from National Cheng Kung University), Chairman of the Cloud Computing & IoT Association in Taiwan, Director of Information Management Department of National Chung Hsing University. He has won the Taiwan Ministry of Education Youth Invention Award and Taiwan Top Ten Information Talent Award. Has deeply studied blockchain applications over the years and led a blockchain technology team to develop systems for health big data and agricultural traceability projects.

5.3 Chief Experts

Mo Bing (Internet of Things): Chinese, PhD in Engineering, post-doctor, his mentor is Professor Kim Suk Ki, a well-known Korean expert in the field of integrated circuits. He is a research professor of Korea University, distinguished researcher of Sun Yat-Sen University, expert in Internet of Things, expert in integrated circuits, senior member of the Chinese Society of Micro-Nano Technology, IEEE member. He is a high-level talent of Fuzhou city under the Bringing in Talents campaign. Evaluation expert of science and technology programs at Fujian Province Science and Technology Department, evaluation expert of science and technology programs at Jiangxi Province Science and Technology Department, Director of Xiamen City Integrated Circuit Association, an expert team member at Tape-out Subsidies Review Committee. At present, he has presided over 10 scientific research projects, published more than 20 articles and applied for 18 invention patents. In 2013, he began to contact Bitcoin, is one of the earliest users of Bitcoin and Korbit. Since 2015, he mainly engaged in research of integrated circuits and blockchain. Two commercial chips have been successfully developed under his guidance.

Wei Songjie (blockchain): Chinese, Doctor of Engineering (graduated from the University of Delaware), Associate Professor of Nanjing University of Science and Technology, Core Member and Master Supervisor of Network Space Security Engineering Research Institute, blockchain technology expert in the field of computer network protocol and application, network and information security. Has published more than 20 papers and applied for 7 invention patents. Previously worked at Google, Qualcomm, Bloomberg and many other high-tech companies in the United States, served as R&D engineer and technical expert; has a wealth of experience in computer system design, product development and project management.

5.4 Team Members

Shan Liang: Chinese, graduated from KOREATECH (Korea University of Technology and Education) Mechanical Engineering Department, Venture Capital PhD, GM of Waltonchain Technology Co., Ltd. (Korea), Director of Korea Sungkyun Technology Co., Ltd., Chinese Market Manager of the heating component manufacturer NHTECH, a subsidiary of Samsung SDI, economic group leader of the Friendship Association of Chinese Doctoral Students in Korea, one of the earliest users of Korbit, senior digital money player.

Chen Zhangrong: Chinese, graduated in Business Management, received a BBA degree in Armstrong University in the United States, President of TIANYU INTERNATIONAL GROUP LIMITED, leader of Chinese clothing & accessories industry, China's well-known business mentor, guest of the CCTV2 Win in China show in 2008. Researcher in the field of thinking training for "Practical Business Intelligence" e-commerce and "MONEY&YOU" course, expert on success for "Profit Model" course. Began to contact Bitcoin in 2013 with a strong interest and in-depth study of digital money and decentralized management thinking. Has a wealth of practical experience in the business management, market research, channel construction, business cooperation and business model.

Lin Herui: Chinese, Dean of Xiamen Zhongchuan Internet of Things Industry Research Institute, Chairman of Xiamen Citylink Technology Co., Ltd., Chairman of Xiamen IOT. He successively served as Nokia R&D Manager and Product Manager, Microsoft Hardware Department Supply Chain Director. In 2014, started to set up a number of IoT enterprises and laid out the industrial chain of the Internet of Things. The products and services developed under his guidance are very popular. Assisted the government in carrying out industrial and policy research and participated in planning of multiple government projects of smart cities, IoT towns and project reviews.

Ma Xingyi: Chinese, China Scholarship Council (CSC) special student, Doctor of Engineering of Korea University, Research Professor of Fusion Chemical Systems Institute of Korea University, Korea Sungkyun Technology Co., Ltd. CEO, Member of Korea Industry Association, Associate Member of the Royal Society of Chemistry, has published his research results in the world's top journal Nature Communications and participated in the preparation of a series of teaching materials for Internet of Things engineering titled "Introduction to the Internet of Things". His current research direction covers cross-disciplines that combine blockchain technology with intelligent medical technology.

Zhao Haiming: Chinese, Doctor of Chemical Conductive Polymer of Sungkyunkwan University, core member of Korea BK21th conductive polymer project, researcher of Korea Gyeonggi Institute of Sensor, researcher of Korea ECO NCTech Co., Ltd., Vice President of the Chinese Chamber of Commerce, Director of Korea Sungkyun Technology Co., Ltd. He has been engaged in transfer of semiconductor, sensor and other technologies in South Korea. He is an early participant of the digital currency market.

Liu Cai: Chinese, Master of Engineering, has 12 years of experience in design and verification of VLSI and a wealth of practical project experience in RFID chip design process, SOC chip architecture, digital-analog hybrid circuit design, including algorithm design, RTL design, simulation verification, FPGA prototype verification, DC synthesis, back-end PR, package testing, etc. Has led a team to complete the development of a variety of navigation and positioning baseband chips and communication baseband chips, finished a series of AES, DES and other encryption module designs, won the first prize of GNSS and LBS Association of China for scientific and technological progress. Finally, he is an expert in the consensus mechanism principle of blockchain and the related asymmetric encryption algorithm.

Yang Feng: Chinese, Master of Engineering, worked at ZTE. Artificial intelligence expert, integrated circuit expert. Has 12 years of experience in VLSI research and development, architecture design and verification and 5 years of research experience in artificial intelligence and the genetic algorithm. Has won the Shenzhen Science and Technology Innovation Award. Has done an in-depth research on the principle and realization of the RFID technology, the underlying infrastructure of blockchain, smart contracts and the consensus mechanism algorithm.

Guo Jianping: Chinese, Doctor of Engineering (graduated from the Chinese University of Hong Kong), Associate Professor of the Hundred Talents Program of Sun Yat-sen University, academic advisor of master's degree students, IEEE senior member, integrated circuit expert. Has published more than 40 international journal & conference papers in the field of IC design and applied for 16 patents in China.

Huang Ruimin: Chinese, Doctor of Engineering (graduated from the University of Freiburg, Germany), academic advisor of master's degree students, lecturer of the Department of Electronics of Huaqiao University, integrated circuit expert. Mainly explores digital signal processing circuit and system implementation and works on digital signal processing technology long-term research and development.

Guo Rongxin, Chinese, Master of Engineering, Deputy Director of the Communication Technology Research Center of Huaqiao University. Has more than 10 years of experience in design and development of hardware and software for embedded systems, works on the long-term research and development of RFID and blockchain technology in the field of Internet of Things.

Li Shuai: Chinese, Master of Engineering, his research focus lies in network security and blockchain access authentication technology. The project on blockchain distributed authentication completed under his direction won the final first prize of the "2016 National Cryptography Technology Competition".

Huang Hongtai: Chinese, Bachelor of Engineering, has five years of experience in WEB front and back-end development, works on the long-term development of Internet of Things platforms and educational information platforms. Began to contact Bitcoin in 2011 and become an early graphics card mining participant. Has a strong interest in virtual currency and blockchain technology.

Dai Minhua: Chinese, graduated in Business Management, received a BBA degree from Armstrong University, senior financial expert, served as Vice President and CFO of Tanyu International Group Co., Ltd. Has 13 years of financial work experience, has a wealth of experience in developing and implementing enterprise strategy and business plans, as well as achieving business management objectives and development goals.

Liu Dongxin: Chinese, received an MBA from China Europe International Business School, Visiting Scholar of Kellogg School of Management at Northwestern University, strategic management consulting expert, investment and financing expert. His current research interest lies in the impact of the blockchain technology on the financial sector.

5.5 Angel Investors

Song Guoping: Doctor of Medicine, President of Chinese Chamber of Commerce in Korea, Director of Beijing Overseas Friendship Association, representative of Ping An International Co., Ltd., representative of Oriental Xu Fu Anti-Aging Center, Representative of Sumei Beauty Shaping.

Qiu Jun: Chairman of Shenzhen Hongtao Fund Management Co., Ltd., Vice President of Shenzhen Shanwei Chamber of Commerce. Has 20 years of capital market investment experience, experienced many magnificent market changes, achieved a number of classic investment cases, including SMIC, China Merchants Securities and Guangdong Danxia Biopharm, etc. Guangdong Danxia Biopharm was acknowledged as one of the top ten successful cases of biopharmaceutical investment in 2016.

Yan Xiaoqian: Chairman of Kaltendin Clothing Co., Ltd., Executive Vice President of Shenzhen Shanwei Chamber of Commerce.

Lin Jingwei: Director of Guangzhou Jiuying Investment Management Co., Ltd., received a master's degree in Senior Financial Accounting and an EMBA degree from Sun Yat-sen University; has 27 years of work experience at large state-owned

enterprises in China and abroad and more than 15 years of work experience as the Secretary of the Board of Directors, Chief Financial Officer and Deputy General Manager of large Chinese state-owned enterprises, has been in charge of enterprise listing, capital operation, investment, financing and financial management for a long time. Has a wealth of experience in capital operation and financial management. Has the qualifications for Secretary of the Board of Directors or Independent Director of listed companies.

He Honglian: Director of Waltonchain Investment Division, Certified Public Accountant, received an MBA degree from Xiamen University. Previously served as the Investment Center Manager of Meiya Pico, currently leads the Waltonchain investment team to research and plan investment in the field of Internet of Things and integrated circuits.

5.6 Consultant Team

I Jong Gil: representative of BSM, Chairman of the Korea Carbon Convergence Committee and Active Carbon Committee.

Go Sang Tae: Deputy Director of Editorial Board of Korea Electronic News Agency, Director of the New Media and New Industry Bureau of KI news.

Liu Xiaowei: Professor of Harbin Institute of Technology, academic advisor of doctoral students, chief expert of the Program 973. Member of the expert group on assembly of micro- and nanotechnology devices, member of the expert group on assembly of a wide range of military electronic components, Deputy Director of the Force Sensing Specialized Committee of the Sensing Technology Division of the Chinese Institute of Electronics, Deputy Secretary-General of Chinese Northeast Micro-Electro-Mechanical System Technology Consortium, editorial board member of the book titled “Sensor Technology”, Heilongjiang Province CPPCC member.

Su Yan: Professor of Nanjing University of Science and Technology, academic advisor of doctoral students, Vice President of the Naval Instrument and Control Academic Board under the Chinese Society of Naval Architects and Marine Engineers, Vice Chairman of the China Instrument and Control Society Naval Instrument and Control Branch, Executive Director of the MEMS & NEMS Society of China, CIS, Executive director of Jiangsu Institute of Instrumentation, expert on components.

Zhang Yan: Doctor of Engineering, Professor, academic advisor of doctoral students. Currently serves as Associate Dean of Harbin Institute of Technology (Shenzhen) School of Electronics. Expert in the areas of digital integrated circuit design and embedded systems.

Ma Pingping: received a Master of Economics from Xiamen University, serves as general manager at Septwolves Venture Capital Limited.

Peng Xiande: Senior Lawyer, Guangdong Wenpin Law Firm partner, expert in company law, investment and financing legal affairs with more than twenty years of judicial practical experience.

Bo Ke: graduated from Henan University of Economics and Law, Senior Lawyer of Guangdong Ruiting Law Firm, China registered lawyer, member of the All China Lawyers Association, member of Shenzhen Lawyers Association, has more than 20 years of experience in legal services.

Xiao Guangjian: Senior Accountant, Tax Accountant, Senior Economist, Secretary-General of Shenzhen Sanming Chamber of Commerce, Shenzhen Lianjie Accounting Firm partner, Senior Financial Expert, has more than ten years of experience in financial consultancy of listed companies.

Li Xiong: founder of the FINANCIAL CHAIN (www.chainfor.com), Internet finance serial entrepreneur, a veteran in blockchain industry. Has 7 years of

product design, marketing operations, brand public relations and team management experience. Embarked on entrepreneurship in blockchain industry since 2013 and founded sosobtc, ICO365, icolive blockchain service platforms. Has a sophisticated understanding of blockchain. Currently, focuses on research of blockchain and cryptocurrency ecosystems and their application.

Part 6 References

1. A. Tapscott, D. Tapscott, How blockchain is changing finance, Harvard Business Review, 2017.
2. T. Stein, Supply chain with blockchain — showcase RFID, Faizod, 2017
3. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org, 2009.
4. R. Hackett, The financial tech revolution will be tokenized, Fortune, 2017.
5. Swedberg, Blockchain secures document authenticity with smartrac's dLoc solution, RFID Journal, 2016.
6. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, Sequences II: Methods in Communication, Security and Computer Science, 1993.
7. Legay, M. Bozga, Formal modeling and analysis of timed systems, Springer International Publishing AG, 2014.
8. Back, Hashcash — a denial of service counter-measure, Hashcash.org, 2002.
9. Dickson, Blockchain has the potential to revolutionize the supply chain, Aol Tech, 2016.
10. KCDSA Task Force Team, The Korean certificate-based digital signature algorithm, IEEE Standard Specifications for Public-Key Cryptography, 1998.
11. J. Donaldson, Mojix brings transformational RFID, big data analytics and blockchain technology to NRF Retail's Big Show, Mojix.com, 2017.
12. R. T. Clemen, Incentive contracts and strictly proper scoring rules. Test, 2002.

13. J.-Y. Jaffray, E. Karni, Elicitation of subjective probabilities when the initial endowment is unobservable, Journal of Risk and Uncertainty, 1999.

14. Blockchain Luxembourg S.A., https://blockchain.info.

15. J. Gong, Blockchain society — decoding global blockchain application and investment cases, CITIC Press Group, 2016.

16. Johnston et al., The general theory of decentralized applications, Dapps, 2015.

17. P. Sztorc, Peer-to-peer oracle system and prediction marketplace, 2015.

18. R. Hanson, Logarithmic market scoring rules for modular combinatorial information aggregation, Journal of Prediction Markets, 2002.

19. Pan Wei Di, analysis of the status quo and future of virtual currency development in China, Enterprise Herald newspaper, 2016.

20. Li Wei, Studies on Virtual Currency Legal Issues, Foreign Economic and Trade University Doctoral Dissertation, 2016.

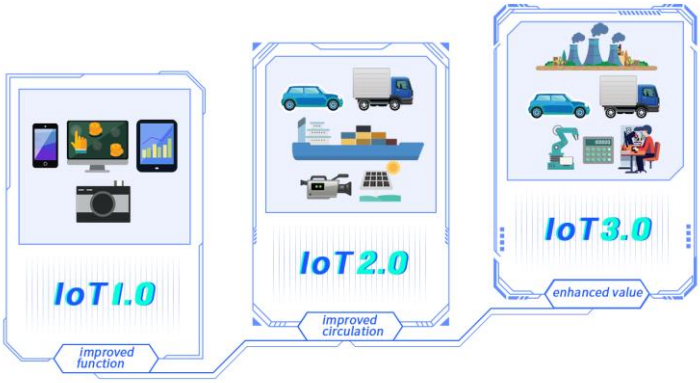
Waltonchain

WHITE PAPER

V2.0

Table of Contents

Preface



This white paper is a periodic summary of the technologies and applications related to the innovative Value Internet of Things (VIoT) concept proposed by Waltonchain. Waltonchain is committed to leading humanity into a reliable digital life, establishment of the Internet of Everything (IoE) and healthy development of a brand new business ecosystem via the blockchain technology.

We firmly believe that innovation creates value and blockchain helps us build trust. With equipment as the foundation, network as the bond, value as the center and data as the vein, we build the blockchain + IoT (VIoT) ecosystem and realize consensus, co-governance, co-sharing and co-integration of IoT data and services in the information era. We will

spare no effort to invest manpower and resources into this innovative IoT system.

The Waltonchain ecosystem framework has been applied to various business scenarios, such as collection authentication, high-end clothing identification, food & drug traceability and logistics tracking. Waltonchain uses a new IoT model to help traditional industries expand business models and product range, extend the value chain, improve operational efficiency and even reduce industry costs.

Realization of strong consistency, multi-connectivity and accessibility is among the technological breakthroughs and innovations achieved by Waltonchain. On this basis, we will eventually build a reliable, trusted, reusable and sustainable system targeted at IoT applications and data circulation.

This white paper provides a detailed overview of the Waltonchain system and guides our friends interested in blockchain. You can find the English, Chinese and Korean version on our official website (https://www.waltonchain.org).

Finally, we sincerely appreciate the valuable advice, feedback and suggestions on Waltonchain ecosystem construction and optimization from our global users.

1 The Call of the Era

With the development and maturity of the Internet, new technologies empower traditional industries faster than ever. The Internet thus comes to a turning point — the Internet of Things (IoT) era. The IoT undoubtedly brings a lot of business opportunities to individuals and enterprises in traditional medical care, logistics, transportation, warehousing and supplies. From a traditional complex network consisting of one smart device (centralized networking) to distributed interconnected physical devices, from machines and cars to household appliances — the IoT is gradually developing new service modes.

From the perspective of the whole network technology development, the number of things we can connect to increases constantly. From files and nodes to devices, it is no longer impossible to connect everything. However, while IoT penetration rates are soaring, there are some key challenges ahead.

1.1 The IoT Predicament

Fig. 1.1 Challenge faced by the traditional Internet of Things

IoT solutions focus on the security and privacy issues of devices and data collection. The predicament of IoT includes:

- **Poor compatibility:** With the increasing possibilities of hardware device interconnection, users are looking for integrated low-cost experience. Therefore, the purpose of object-object interconnection is achievement of greater operability. However, the interoperability (compatibility) of devices and platforms has become a key challenge in the development of IoT solutions because of the simple function of IoT equipment and coexistence

of multiple protocols. A single IoT platform lacks ability to connect all manufacturers' equipments.

- **Poor security:** With the rapid development of the IoT technology, its security and reliability have become a hot topic. Attackers can pose a real threat using the vulnerabilities in IoT devices and disclosing home data from online routers and private user information from social networks. DoS attacks on IoT devices prove that a large number of low-cost networking devices pose a major challenge to the IoT security. Massive data collected by millions of devices has always posed security risks and privacy problems to individuals, businesses and governments.

- **Low architecture flexibility:** When a centralized cloud-based IoT platform performs message routing (i.e. data transfer), any disruption could affect the entire network. In real society, it is a challenge to centralize the management of scattered devices, so reliability of IoT systems is relatively weak.

- **High cost:** The IoT is often associated with a large number of devices and respective network facilities. It turns out that costs associated with traditional IoT solutions are very high. The solutions also need to handle a lot of messages (communication

costs), device-generated data (storage costs) and analysis (server costs). The future development continues to add up costs.

- **Poor scalability:** As IoT communication methods and networking technologies fail to keep up with the growing complexity and interconnectivity demands of technology; the IoT is rife with problems such as outdated equipment, inefficiency and high costs.

- **Data uniformity**: The entire Internet of Things is still in state of data dispersion and information fragmentation. It is difficult to collect complete and accurate information about flow, circulation and quantity of materials, equipment and products. While there is data available for collection, aggregation and dissemination, still, ensuring data accuracy and application uniformity across business models remains a challenge.

In a survey quoted by *Biggest Opportunities and Challenges of IoT-Enabled Products and Services*, 51.3% of IoT implementers indicated that **cost** is the top issue they want to improve; **data analytics** (48.1%) and **safety** (47.5%) followed.

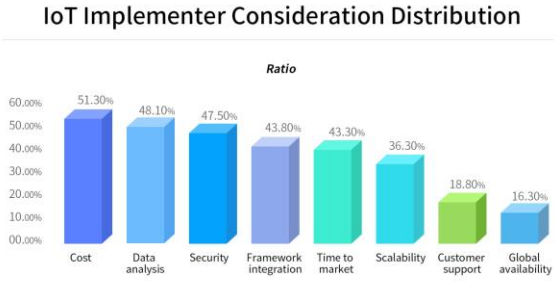


Fig. 1.2 IoT Implementer Consideration Distribution

Other issues to improve include **framework integration** (43.8%), **time to market (TTM)** for future products (43.3%) and **scalability** (36.3%), followed by **customer support** (18.8%) and **global availability** (16.3%).

5.6 percent of respondents expressed a desire to improve power consumption and performance, industry acceptance, user experience, technology and channel partnerships, and provide consumers with attractive value propositions.

1.2 The Opportunity of Blockchain

Two new concepts have recently emerged in the IoT. One is the NDN (Named Data Network). Another is the SCN (Service-Centric Networking). The user demand is no longer limited to how to connect to the network, but focused more on what can be done after accessing the network.The focuse has been converted from the connectivity of the total network to the service demand of the network.. People consider more about the use of the internet. The function of the Internet lies in information transmission; and data is the most important thing for us in the information era.

In a blockchain environment, people do not need to establish trust in advance to transact safely, because every transaction is recorded in the distributed ledger of blockchain, which is immutable and provides verifiable evidence. Blockchain can perfectly solve the trust and equity issues in the virtual world of the Internet. Waltonchain introduced the blockchain technology into the IoT to solve the centralization problems faced in the IoT development with a new idea:

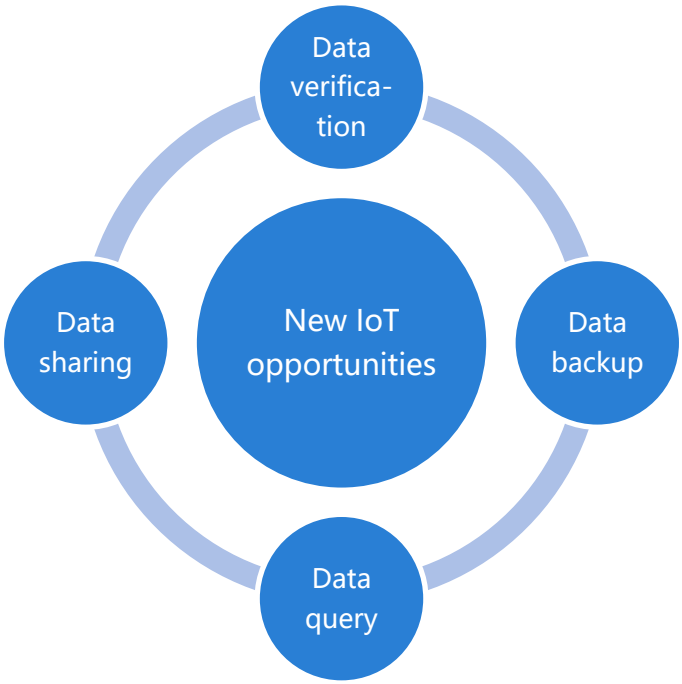


Fig. 1.3 New IoT opportunities

- **Data verification:** In the Internet of Everything, modified IoT equipment will become data generation nodes generating massive, polymorphic, time-varying and dispersive data . Therefore, enterprises face the lack of precise tools to deal with data. Waltonchain uses data labels, integrates and packages massive data and authenticates data stamps to solve the data verification problem in the IoT industry.

- **Data query:** In the large multi-chain and cross-chain ecosystem of Waltonchain, each child chain can accurately store its own data and upload it to the big parent chain ecosystem to realize cross-chain

query through data union and professional distribution of modules.

- **Data sharing:** Although the “decentralized” data sharing claimed by blockchain is a sensitive behavior in many business fields, in the Internet of Things, transparent and open data processing by blockchain can greatly reduce the communication, analysis and data storage costs, and realize differentiated data processing and sharing.

- **Data backup:** Due to immutability of records in the distributed ledger of blockchain, blockchain + IoT not only realizes data backup efficiently, but also increases the cost of data falsification.

Therefore, in the future, there should be a network where all you need to think about is the use, access channels and location of data, but not the source, security or access.

In the new era of information society, everything interconnected together should be data-centered; and data should be the core of the entire Value Internet of Things. In other words, blockchain empowering via the IoT directly adds the “credible value channel” to it, not only solves the inherent pain points of the IoT but also creates the new IoT definition.

1.3 The Vision of Waltonchain

Advancement of the entire network architecture, high cost, devices, terminals or services used for connection are no longer the focus in the IoT. What we really consider is the meaning of connection.

Blockchain just happens to establish faith to build a new-generation IoT ecosystem with software and hardware fusion, multi-chain network integration, data sharing, cross-domain query verification and value transmission:

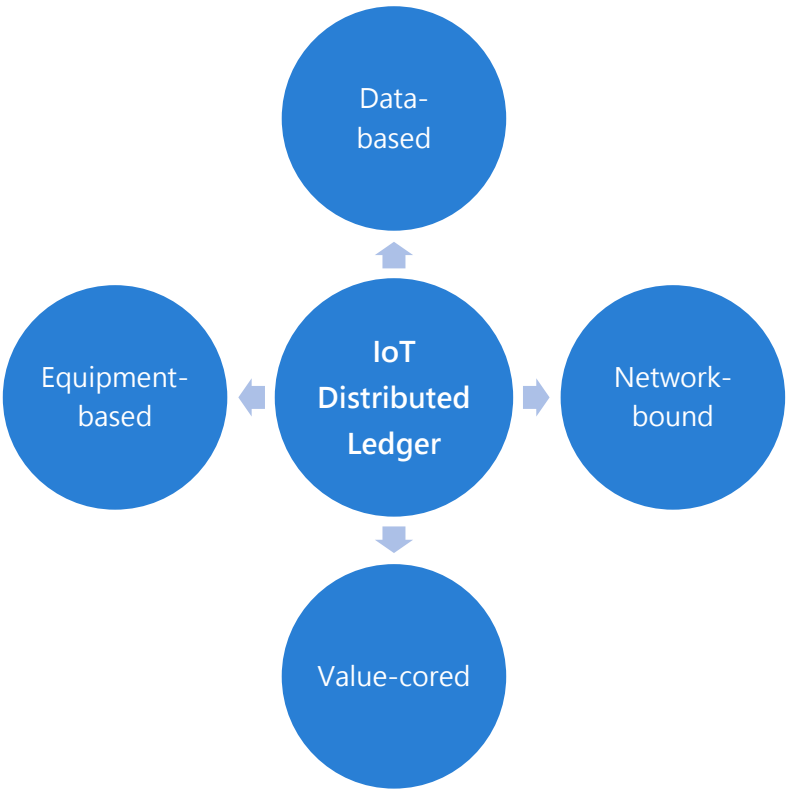


Fig. 1.4 New IoT model

- **Data-cored:** Data is valuable only when it is used. Data sources and channels are not the top concerns for the general public. The public is more concerned about data access and usage. Different access roles and scenarios should have corresponding data management and control.

- **Equipment-based:** Since data mostly happens to be multivariate and mobile, multiple vectors exist when devices connect large amounts of data. When data amount is large and problems of accuracy, credibility and consistency occur, distributed devices provide better and more convenient uploading to blockchain and distributed storage.

- **Network-bound:** Since IoT data is distributed, multivariate data will raise the standardization or uniformity problem. Blockchain's distributed ledger is naturally compatible with IoT data distribution. New business models will emerge as this distributed data begins to circulate effectively.

- **Value-veined:** The space where data exists is fragmented. The existing network data circulation is not smooth enough and therefore affects data value. When effective data circulation starts, value circulation follows and brings transactions and exchange.

This is also a problem that could be solved by blockchain's unification.

The vision of Waltonchain is to lead humanity to the reliable digital life via blockchain, realize the consensus, co-governance, co-sharing and co-integration of IoT data and services in the information era.

Fig. 1.5 Vision of Waltonchain

- **Consensus:** The blockchain technology can ensure consensus. Its real-time data uploading, tamper resistance and continuity ensure unity and integrity. These features promote effective data circulation and cooperation.

- **Co-governance:** Blockchain's distributed storage brings decentralization. With consensus mechanisms, effective data co-governance and coordination can be achieved through encryption algorithms or confidentiality agreements.

- **Co-sharing:** Waltonchain is a cross-chain ecosystem where the parent chain and child chains serve as the framework. Here data

can access data on other chains, thus realizing cross-chain data co-sharing and effective and quick indexing.

- **Co-integration:** Waltonchain is developing a main chain surrounded by various blockchains, the parent chain. In the cross-chain ecosystem with the parent chain and child chains as the framework, the exchange between data circulation and value can be realized between child chains.

Therefore, the blockchain technology will be a game changer for the traditional Internet of Things. It can add up the missing links to the IoT P2P distribution, bring IoT transactions where no third-party confirmation is needed, gradually solve the problems of scalability, single-point failure, time-stamps, records, privacy, trust and reliability.

2 Technological Superiority

At the current development stage, the superiority of Waltonchain comes not only from the combination of software and hardware, but also from the advanced equipment, software, protocols and algorithms.

Fig. 2.1 Core technology advantages of Waltonchain

Waltonchain has its own mainnet (parent chain) and works on its extension and development. We have a blockchain explorer, user terminals, management tools and on top of that the core hardware equipment of our own. We consider how to extend the existing technological base, ideas and architecture into a wider space.

2.1 Overall Structure

In acquisition, perception and processing of all available data in the IoT or an ecosystem network, Waltonchain mainly focuses on two aspects:

1) data reliability;

2) data value circulation.

We have redefined the architecture of the Waltonchain ecosystem network, which is composed of six layers: object layer, base layer, core layer, extension layer, service layer and application layer.

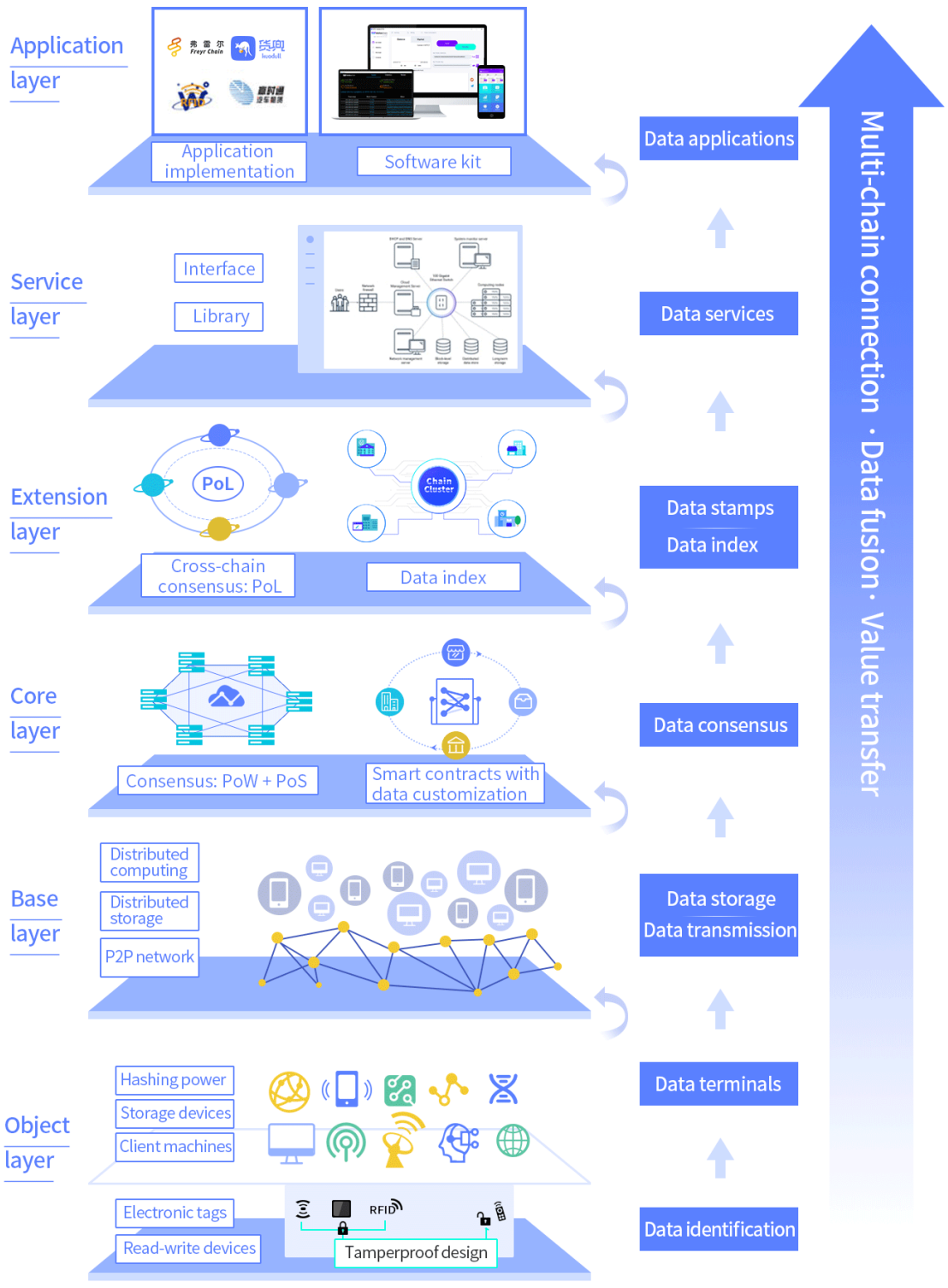


Fig. 2.2 Structure of the Waltonchain ecosystem

2.2 Hardware Design — Object Layer

We hold the idea that pure software IoT solutions are vulnerable. Programs are written by people and can be tampered with; data can also be modified. How do we ensure that it is true from the source? The solution is to upload true data to the chain, so that it is tamper resistant.

The existing blockchain applications mostly adopt software solutions and lack hardware support. Although the blockchain technology can guarantee data tamper protection, openness and transparency, because of the lack of hardware support the existing application schemes cannot guarantee authenticity and reliability of data sources. The key feature of Waltonchain is implementation of a blockchain hardware system ensuring that data is authentic and reliable from the source.

2.2.1 Two-way Authentication RFID Chip

We developed an RFID chip design with hash-and-signature-based data self-verification. This self-verification method ensures that, having a correct Access-Pass, a reader-writer can read and write to RFID chips and also provides certain control. With the hash and signature algorithm, two-way authentication between the RFID reader-writer and the RFID chip is realized to ensure that all read and write operations are undeniable and

tamper-proof, i.e. suitable for RFID technology applications and industries with safety requirements.

The working process of the two-way authentication RFID chip in blockchain applications is shown below:

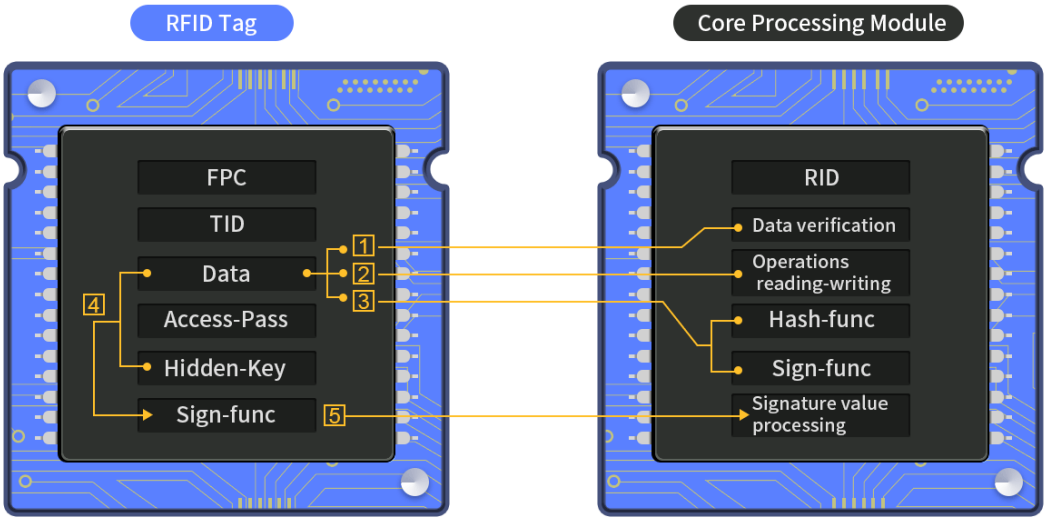


Fig. 2.3 RFID data self-verification system

Advantages of the two-way authentication RFID chip:

1. On the read-write terminal side, hash calculation helps ensure data tamper protection, integrity and accuracy.

2. Based on the signature algorithm, the two-way authentication between the RFID reader-writer and the chip is realized to ensure that the reader-writer's operations on the chip are undeniable and that a certain reader-writer is operating on the chip, thus avoiding impersonation, tampering and denial of reading and writing.

3. When signing, the signed data contains a timestamp and a reader ID (RID) for secondary reading and writing, which ensures uniqueness of each independent operation of each RFID chip and prevents replay attacks.

4. Data self-verification based on hash and signature is integrated into read-write terminals of the RFID system. It allows businesses to pay more attention to business realization, reduces the degree of coupling, but provides security and control.

2.2.2 Sensing Equipment

Data is acquired by sensing equipment, transmitted to the core control module through the interface, processed and organized into standard packets. A data stamp is extracted through hash calculation and signed. Then the master control module automatically uploads the signed data stamp or data index to the blockchain network through the communication module and at the same time uploads the assembled original data to the centralized server.

Sensing equipment can be used to monitor, analyze, process and transmit data and also perform basic AI operations to learn and identify specific source data. It will serve as a data source for blockchain

applications. Automatic stamp extraction from sensor data and automatic uploading to blockchain reduce manual operations and software processing workload. They also help verify the correct processing of products during the whole circulation process, track delivery of goods and prevent theft and falsification. Ensuring data authenticity and reliability from the source has high application value and will greatly promote the blockchain implementation.

2.2.3 Mobile Full Node Equipment

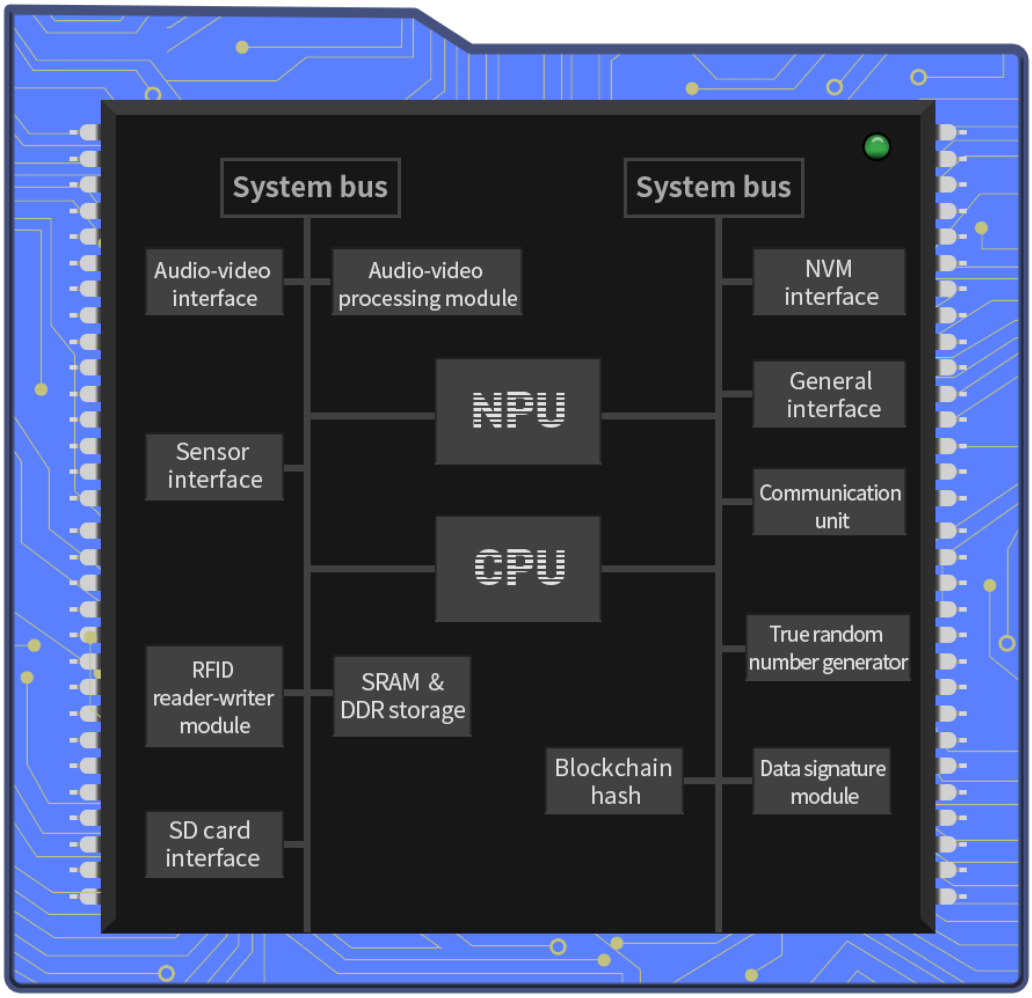


Fig. 2.4 Diagram of the core processing module of mobile full node equipment

The core processing chip of full node equipment is a powerful SoC which can also be built of separate components to realize data collection, processing, storage and running of full node programs. During the whole-core processing, a program run by the main processor controls each interface of the perception layer and obtains perception layer data.

Data cache is stored in the SRAM & DDR storage module. The program assembles the data, forms a standard data packet and invokes the blockchain hash and data signature module to calculate hash and sign the original data. A node program uploads the calculated data stamp to the blockchain, and the original data is uploaded to the centralized server — all through the communication module.

2.2.4 Network Communication Equipment

IoT protocols and interfaces are diverse; therefore our hardware integrates multiple popular physical interfaces. Other units, such as sensor interface, NPU, video processor, common interface, etc., can be Plug and Play add-ons according to user requirements.

As shown in the figure below, the existing IoT protocol standards and interfaces are diverse. A large number of sensing devices are deployed at various application sites. Due to commercial, technological immaturity or historical reasons, various IoT standards are inconsistent, e.g. hardware protocols, data model standards, network protocols, sensor standards, equipment connection standards, platform compatibility, third-party application interfaces, service interfaces, etc. The inconsistency may lead to waste of resources and problems in equipment interoperability. Thus users need to develop various perceptual networks independently, which

increases the difficulty and complexity of upper-level application development.

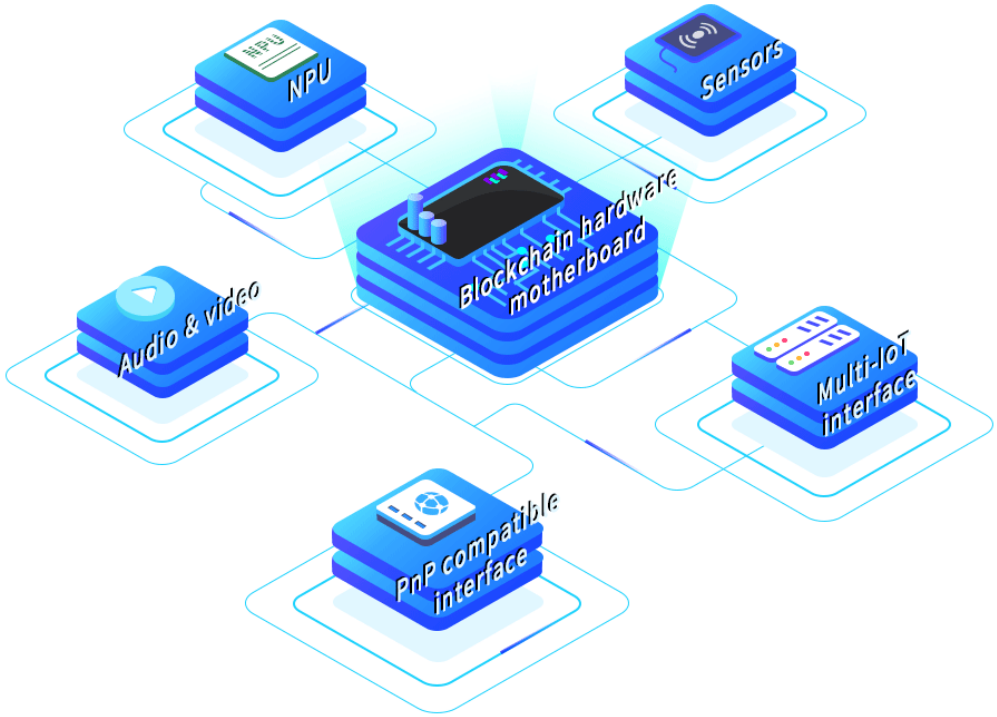


Fig. 2.5 Plug and Play compatible interface

In the existing network layers, interface protocols are not unified. The Waltonchain hardware system is a blockchain hardware system with independent intellectual property rights. It can be compatible with mainstream IoT communication interfaces and adopts the hardware asymmetric encryption technology to ensure data security and prevent attacks. Compatible IoT transmission standards include 5G, NB-IoT, LoRa, ZigBee, PLC and other common interfaces.

The first step to realize the data-oriented value blockchain ecosystem is construction and gradual improvement of the data network through acquisition of terminal data.

2.3 Core Layer and Extension Layer of the Waltonchain (Parent Chain)

In general, data in a blockchain + IoT ecosystem is also a simple ecosystem. Parts of the ecosystem are fragmented. Different domains build their own data ecosystem around their data, or build their own blockchain architecture. Even blockchains may adopt different structure and technical systems. The main aim of Waltonchain is to connect data. We use integrated hardware and software, smart contracts with data customization, the Waltonchain cross-chain technology and WPoC consensus mechanism to achieve data integration, circulation, verification and storage between different blockchains (child chains), and thus connect different data sources and obtain wide data circulation.

As the Waltonchain (core layer) has evolved from Go Ethereum, it carries and extends its consensus mechanism and smart contracts. However, to realize data circulation and value transfer, Waltonchain has to change its core features in the following aspects:

2.3.1 WPoC Consensus Mechanism

Waltonchain consensus mechanism WPoC (Waltonchain Proof of Contribution) is one of the important mechanisms to maintain the benign development of the Waltonchain ecosystem. WPoC includes three

components: PoW (Proof of Work) + PoS (Proof of Stake) +PoL (Proof of Labor).

PoW and PoS are used on the Waltonchain parent chain and both ensure that parent chain blocks are unique and secure. PoW provides reliable data protection through computing (hashing) power; still, it does not prevent the risk of 51% attacks and also lacks the features of environmental protection and energy saving. Therefore, to reach the balance we use PoS, as it reduces wasting of calculation resources and the risk of 51% attacks. Through the interaction of PoW and PoS algorithms, our parent chain can solve the trust issues of data verification, storage and circulation in economic activities within the ecosystem.

PoL is a brand new consensus mechanism for data transmission and token exchange between various parent chain, child chain and cross-child-chain nodes on the Waltonchain network, i.e. SMN (Super Master Nodes), GMN (Guardian Master Nodes) and MN (Master Nodes).

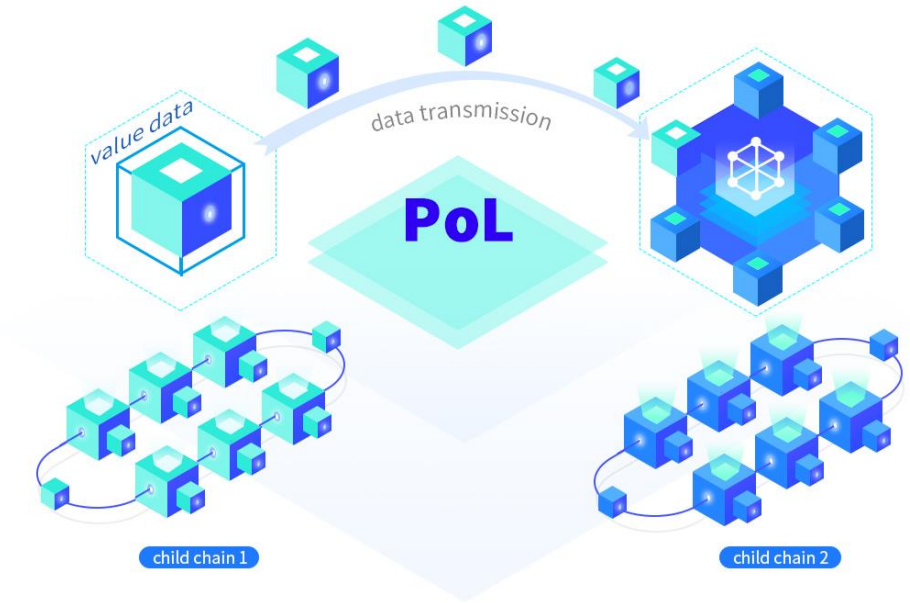


Fig. 2.6 PoL cross-chain consensus mechanism

The whole Waltonchain ecosystem ensures blockchain self-protection through calculation and tokenization based on the reasonable fuel (Gas) mechanism. Therefore it is necessary to both realize cross-chain transmission without affecting data circulation and maintain the Turing complete ecosystem mechanism of Waltonchain as follows:

- **Cross-chain data transmission:** Extraction of hashes or indices basing on data features and storage on the Waltonchain parent chain makes it convenient to search for data in the Waltonchain network in the future. Using our cross-chain index mechanism, the required data can be found quickly; its authenticity can be verified quickly through cross-chain data.

- **Cross-chain token exchange** is realized via a ledger based on atomic token swaps; it is used to record every transaction between Waltoncoin and child chain coins or tokens. Refer to the conversion process between a child chain token and Waltoncoin below.

Only in this way can we realize multi-chain connection and data fusion. With the implementation of "black box" operations of traditional network communications to obtain data, ecosystem users and enterprises no longer need to consider problems such as access, communication protocol or absence of network connection for IoT devices and can focus on what data is needed, what to use it for and how to show it to the others.

Fig. 2.7 Cross-chain token circulation

The second step to realize the data-oriented value blockchain ecosystem: with data storage and query index, users get accurate data according to their requests; all the relevant data is not provided directly without filtering; data rights are allocated effectively; data privacy is protected.

2.4 Smart Contracts with Data Customization Support

The smart contract language supported by the Waltonchain network is also Turing complete. It is because of the powerful smart contract language that the originally complex real-world business logic and applications can be easily implemented on blockchain. However, due to the operating mechanism of blockchain, even if smart contracts are abnormal, they will run repeatedly and independently on all blockchain nodes. Therefore, in terms of computing and storage resources, it is very expensive to run smart contracts on the Waltonchain parent chain and child chains (alliance chains).

Application users and enterprises are more concerned about the data format used. Where is data stored? How to get this data? What about Gas?

We set up the unique Data Pattern for Smart Contract to drive business events. We keep the logic of the data-specific smart contract language simple, reduce Gas consumption, standardize operations such as data reading and event triggering, and provide output data in standard formats (e.g. Json). Our smart contracts can be reused and inherited.

In fact, many operations (such as writing data to blocks of the Waltonchain parent chain) are not suitable for direct execution on the

parent chain; therefore contracts support events at the language level. The relevant parties can be directly notified to start processing when the expected event occurs. The contract developer doesn't need to repeat the same logic, thus cross-chain data transmission is standardized in the ecosystem. Refer to the principle in the following figure:

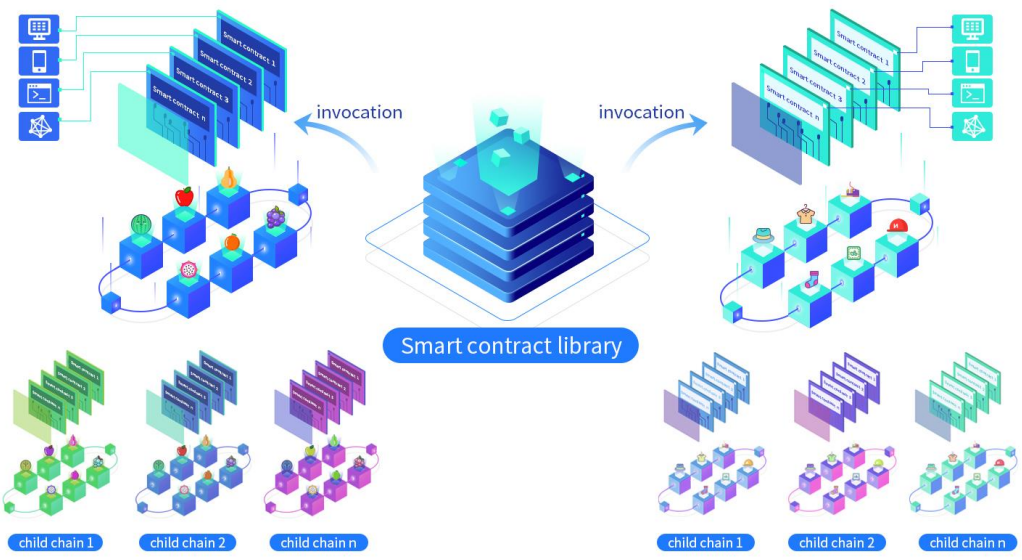


Fig. 2.8 Smart contract library

We designed and built a number of smart contract libraries where smart contracts can be quickly queried, invoked, inherited and reused via the event function index. The relevant data is self-generated. After a developer, user or enterprise obtains a relevant standard data file, data interaction between an application and other child chain systems can be achieved.

Data consistency, normalization, access and circulation within the Waltonchain value blockchain ecosystem can be realized step by step:

- **Consistency:** The core of consistency is consensus. Due to a huge amount of data in the IoT ecosystem, data recognition problems occur among different industries, equipment and attributes. Therefore, the unique mechanism of blockchain is used for data consistency.
- **Normalization:** The diversity of data leads to the lack of data standards or uniformity. However, the basic condition for unification is actually the liquidity of data. Only when data can circulate on more levels can it be normalized in social networks.
- **Accessibility:** Data circulation also has its value — usability. The real value of data can be realized only when more people can access it from different environments and devices.
- **Liquidity:** Data is like scattered pearls; the space where it exists is fragmented. Only after we arrange and combine this scattered data can we truly realize and develop its value and thus complete the transaction and exchange process in social networks.

The third step to realize the data-oriented value blockchain ecosystem is data services. The questions arising here are: What to use the data for? How to present it? How to make it visible to others?

2.5 Child Chain Data Application Templates

The Waltonchain supports smart contracts of popular blockchains, such as Fabric and Ethereum. Therefore we provide child chains with different architecture according to requirements of different scenarios. Rapidly constructed prototype child chains serve as data application templates. They help users and enterprises quickly build child chains, regardless of their experience in blockchain development. The child chains built in the Waltonchain ecosystem can also quickly link the interface and functions of the Waltonchain parent chain and realize the ability to derive and expand.

2.5.1 Fabric Smart Contracts

Fabric smart contracts (chaincode) are divided into system chaincode and user chaincode. System chaincode realizes system level functions; and user chaincode realizes user application functions. Chaincode is compiled into a stand-alone application that runs in an isolated Docker container.

Unlike Ethereum, Fabric's Chaincode is separated from the distributed ledger. During Chaincode upgrades, there is no need to transfer ledger data. Thus the real separation of logic and data is achieved. Chaincode supports writing in Go, Java and Node.js; it interacts with peer nodes via gRPC to realize data applications for alliance chains (Fabric child chains).

2.5.2 Ethereum Smart Contracts

When it comes to writing smart contract programs on Ethereum, Solidity is the main programming language. Its four key elements are: Contract, Variable, Function and Event.

Contract is the core concept in Solidity, so we use Web3 to transmit data and provide API on Ethereum alliance chains (child chains).

When a token is defined using the ERC20 standard, a new event is defined. When token transactions occur, such events can be detected by the JavaScript API and its Web3 service is invoked.

Many basic chains use Solidity as a programming language for smart contracts. Some basic chains such as EOS provide a C++ API for writing smart contracts. This is just a matter of choice by different platforms for different purposes. Therefore Waltonchain smart contract library will be constantly updating to provide more data application services and meet the needs of different blockchains.

2.6 Chain Cluster

Multiple chains need to be effectively connected to form a cluster. A chain cluster is a natural derivative under the large public-chain ecosystem. A public chain can carry countless child chains through hierarchical structure. It is assumed that as this “data value machine” becomes bigger, data in circulation must seek normalization. Thus chain clusters are inevitable. Different chain clusters can realize secondary propagation and integration of data value, more efficient cross-chain exchange and query.

Fig. 2.9 Chain cluster

The Waltonchain is the first public chain in the industry to advocate for such data value specifications. This public chain will also carry child chains of multiple industries to form an expansive business ecosystem with a benign development model. In this business environment, data generated

between different child chains can be exchanged, traded, queried, etc. Data between different child chain ecosystems must coincide to a certain degree. Thus we believe that, with data circulation, exchange and integration, ecosystem chain clusters will inevitably appear. In the vast Waltonchain ecosystem, these chain clusters realize the second reorganization of value and enrich the whole ecosystem order.

3 The Current Ecosystem

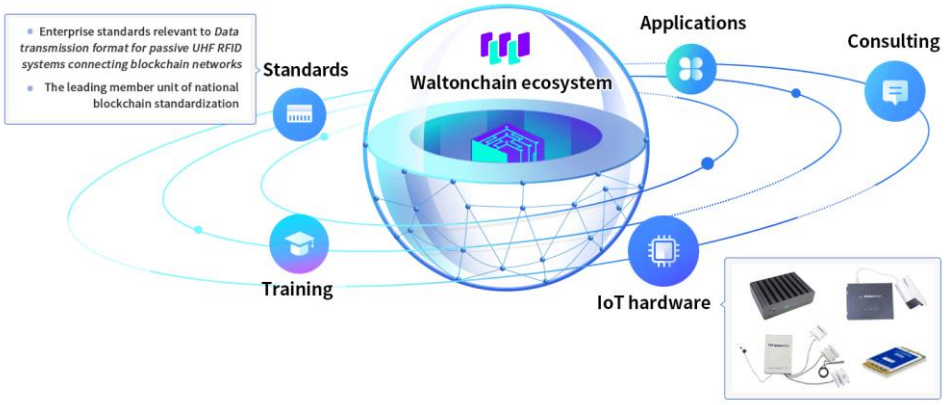


Fig. 3.1 Waltonchain ecosystem

The Waltonchain team and the community have been committed to establishing a complete, reliable, credible, scalable and transferable data-value-oriented blockchain ecosystem of the Internet of Everything, and strives to make Waltonchain an integrated data collection equipment manufacturer, data communication researcher and developer, and data service provider.

3.1 Equipment Developers

The Waltonchain technical team has developed a smart RFID reader-writer with independent intellectual property rights, which can collect data, process it and upload to blockchain automatically.

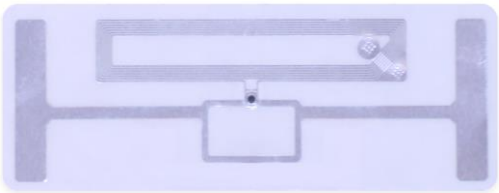


Fig. 3.2 RFID tags

Fig. 3.3 RFID read-write terminal

Fig. 3.4 Encrypted data collector

We also developed a smart data collecting device with independent intellectual property rights, which automatically collects, processes and uploads various sensor data, audio and video, location information, etc. to blockchain.

3.2 Application Designers

3.2.1 Food Traceability System

The food traceability system based on the Waltonchain blockchain technology and relevant hardware equipment includes video collecting equipment, sensors, smart terminals, a food traceability child chain, cross-chain nodes and a data inspection system platform. After adopting the system, data hashes can be extracted and uploaded to blockchain automatically through smart terminals to ensure that the data is tamper proof. Consumers can easily check the relevant data through the data inspection system platform.

Fig. 3.5 Food traceability: soil information collection

Waltonchain technical team developed the S.I. Two-way Traceability Marketing Platform targeted at traditional traceability systems in the food

industry. Waltonchain conducted the Blockchain+ transformation of its traceability platform: to ensure tamper protection, traceability information is uploaded to blockchain.

Fig. 3.6 Food traceability system

3.2.2 Clothing Traceability Authentication System

The clothing traceability authentication system based on the Waltonchain blockchain technology and relevant RFID hardware system includes RFID tags, smart RFID reader-writers, clothing child chains, cross-chain nodes and an inspection system platform for data applications. The system can facilitate data circulation in production, logistics,

warehousing, sales and other links, and ensure data authenticity and traceability of each garment. It can simplify the process, reduce cost for enterprises and ensure consumers' interests by allowing them to check authenticity and quality of the purchased clothes easily.

Fig. 3.7 Functions of the clothing traceability authentication system

The KALTENDIN Production, Warehousing and Store System is an information management system for the clothing industry developed by KALTENDIN Group through adoption of the RFID IoT technology and blockchain technology. It utilizes RFID tags to read commodity information quickly and the blockchain technology to link traceability information and ensure it is tamperproof.

Fig. 3.8 Demonstration of the clothing traceability authentication system

3.3 Technology Disseminators

As the saying goes, “It takes ten years to grow trees, but a hundred to rear people.” The Waltonchain team is dedicated to training new forces and ensuring sustainable development.

Waltonchain has established a curriculum system, experimental system and professional laboratory in Blockchain + IoT. It trains professionals with industry competitiveness for global secondary and higher vocational colleges, universities and training institutions to build a team of talents.

Together with authoritative educational and marketing platforms in the industry we have selected educational products to develop and promote Blockchain + IoT. We have reached comprehensive cooperation on respective training platforms, courses, textbooks, skill appraisal, skill competition and school-enterprise cooperation. Our educational products will also include short-term theoretical training and applied practical courses on blockchain.

Waltonchain will cooperatively provide new-generation smart chip, module and system solutions based on the sensor technology and strong technical support for the industry layout, product positioning and promotion, and secondary development and application of Blockchain + Education.

3.4 Consulting Service Providers

The foundation of our self-development is the Waltonchain Value Blockchain. In the course of our business services which include development of blockchain systems and DApp products, alliance chains, exchange platform systems and product uploading to blockchain, we have been constantly accumulating experience and benefit from a clearly defined corporate culture. Due to the bold and innovative thinking, we have attracted a large number of outstanding high-tech and business talents from ZTE, Huawei, domestic and overseas blockchain companies to join our team, and aim to make Waltonchain the leading blockchain consultant in China.

Refer to the list of project requirements and related services below:

Project	Industry	Application	Service Content
Skynovo	Agricultural products	Food traceability	Cooperation in application development; technical and consulting services
Huodull	Logistics	Logistics tracking	Technological development and consulting services: child chain construction

Project	Industry	Application	Service Content
KALTENDIN	Clothing	High-end clothing traceability	Technological development and consulting services: child chain construction and DApp development
Freyrchain	Art collection	Collection traceability	Technical consulting
ProdutorAgro (Brazil)	Agriculture	Food traceability	Solution consulting and technical support
Yandeh (Brazil)	Auto parts	Auto parts tracking	Solution consulting and technical support
Volcity Wine (New Zealand)	Red Wine	Product traceability	Solution consulting
MitoQ (New Zealand)	Biology	Product traceability	Solution consulting
Global eSolutions Group (USA)	Medical care	Medical certificates	Solution consulting

3.5 Standard Setters

Based on practical experience in technology development, the technical team of Waltonchain has developed enterprise standards related to *Data transmission format for passive UHF RFID systems connecting blockchain networks* and work on their promotion to industry standards and national standards.

When data is collected by a UHF RFID reader and uploaded to the blockchain network to increase data integrity and authenticity, a UHF RFID data storage and management method is combined with the blockchain technology. Standardization of data transmitted by readers to blockchain networks is favorable for reader manufacturers and facilitates equipment interconnection between blockchain network service providers.

Although the industry welcomes progress in implementation, there is still no consensus on blockchain industry standards in China. On August 1, 2018, the National Standard Kick-off Meeting of the *Information Technology, Blockchain and Distributed Ledger Technology Reference Architecture* was held in Kunming, China. This is the first national standard approved in the blockchain field. The Waltonchain technical team was invited as a member of the China Blockchain Technology Standards Working Group and is actively participating in development of standards.

We will contribute to the formulation of cross-chain service management, smart contracts, storage and other domains; promote the benign industry ecosystem development and the new industry stage.

4 Development Blueprint

Waltonchain has divided its path to build the complete Waltonchain ecosystem into five steps.

The first step is to realize token circulation. Waltonchain built, deployed and launched its parent chain and WTC client applications in 2018. Nodes on the Waltonchain can exchange tokens and maintain the parent chain.

The second step is to realize data circulation. In 2018, we focus on the implementation of:

- Freyrchain, the art collection chain; uploading to blockchain and transmission of all kinds of collection data;
- the Huodull logistics child chain; uploading to blockchain and transmission of all kinds of online logistics data;
- the KALTENDIN clothing child chain; uploading to blockchain and transmission of all kinds of clothing industry data.

Waltonchain will enter more child chain domains and upload data from different industries to blockchain for circulation.

The third step is to realize value circulation. Waltonchain are about to complete and deploy the cross-chain architecture. It connects the parent chain and child chains; child chain data can be uploaded to the parent chain. Using the cross-chain mechanism, child chain tokens are exchanged for WTC and can be further exchanged for other child chain tokens, thus value circulates on blockchain.

The fourth step is provision of customized services. After the completion of the cross-chain architecture, the parent chain and child chains connect and interact. Waltonchain has started to provide customized services for various industries. Meanwhile, child chain nodes will query information or use services on other child chains simply by using child chain tokens.

The fifth step is the ecosystem construction. After the above four steps, the Waltonchain business ecosystem is formed via the parent-child and child-child chain integration.

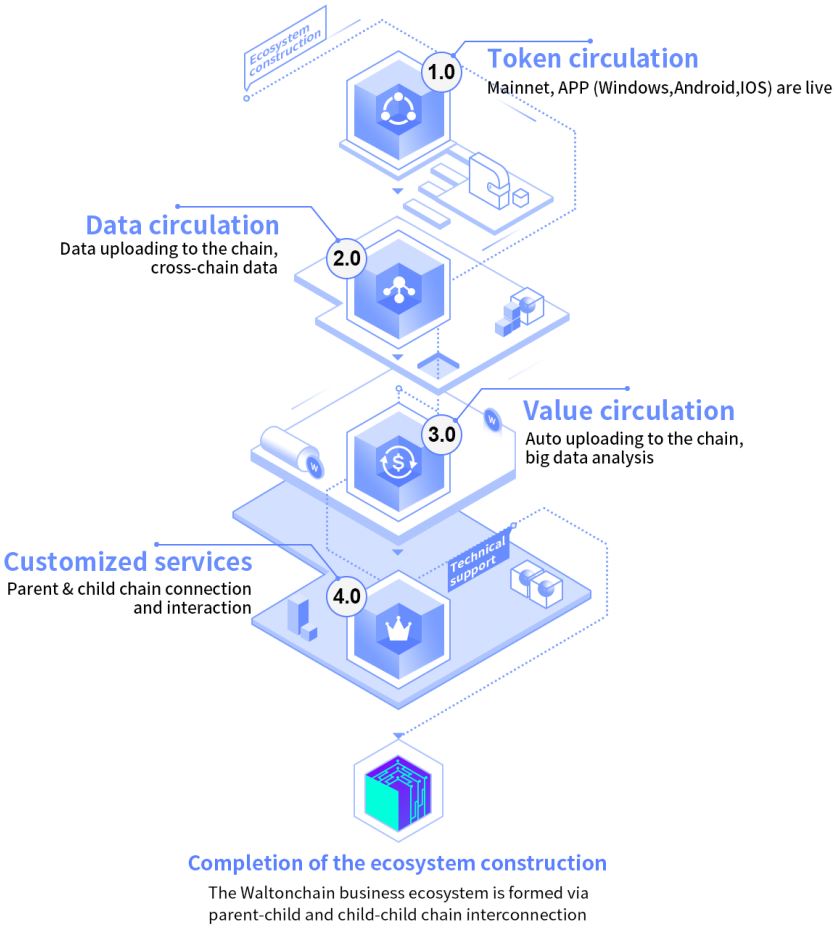


Fig. 4.1 Waltonchain development roadmap

5 Walton Chain Foundation

Walton Chain Foundation Ltd. (the Foundation) is a non-profit organization established in Singapore in 2017. As the management organization of Waltonchain, the Foundation is committed to the Waltonchain ecosystem construction and its benign development, including promotion of technology R&D, project cooperation, massive implementation of applications and community maintenance.

Walton Chain Foundation Governance Structure

The Foundation advocates a transparent and efficient operational philosophy to promote the healthy development of the Waltonchain ecosystem. The governance structure focuses on the effectiveness, sustainability and financial security of project management.

Having established a reasonable governance structure, Walton Chain Foundation agreed on the working rules and procedures of each sub-committee, so as to make rational decisions on major issues of the Foundation and promote daily work precisely.

Members of the Decision Making Committee change every four years and generally include two representatives recommended by each subcommittee, one community representative and one member of the

Waltonchain team. Members of the subcommittees change every four years; they are generally prominent people from related industries.

The Committee is the top decision-making body of the Foundation. Its main goal is to discuss and resolve important issues faced in the course of the Foundation and community development, including:

- change of the Foundation governance structure;
- formation and rotation of the Committee;
- appointment and removal of members of each subcommittee;
- review and amendment of the Foundation Statute;
- decision on the Waltonchain development strategy;
- change and upgrading of the core technology of Waltonchain;
- urgent decision making and crisis management agenda.

The overall structure of the Foundation is shown in the following figure. There are four committees under the Decision Making Committee, namely Technical Committee, Operation Committee, Incentive Committee and Audit Committee.

Fig. 5.1 Walton Chain Foundation governance structure

6 Team Introduction

6.1 Member Introduction

Xu Fangcheng (initiator in China): Chinese, majored in Business Management, former Director for Supply Chain Management of Septwolves Group Ltd., has rich practical experience in supply chain management and purchasing process management. Angel investor.

Do Sang Hyuk (initiator in Korea): Korean, Vice Chairman of the China-Korea Cultural Exchange Development Committee, Chairman of Korea NC Technology Co., Ltd., former Director of the South Korea Electronic News Media Bureau, Director of ET News, Former Director of Korean Standards Association, Chairman of Small and Medium-Sized Enterprise Committee in Seongnam, South Korea.

Kim Suk Ki: Korean, one of the key persons in South Korean electronics industry, Doctor of Engineering (graduated from the University of Minnesota), previously worked at Bell Labs and Honeywell USA, served as a Vice President of Samsung Electronics, senior expert in integrated circuit design, IEEE Senior Member, Vice President of the Korean Institute of Electrical Engineers, Chairman of the Korea Semiconductor Industry Association. He has published more than 250 academic papers and possesses more than 60 patents.

Zhu Yanping: Taiwanese, Doctor of Engineering (graduated from National Cheng Kung University), Chairman of the Cloud Computing & IoT Association in Taiwan. He won the Taiwan Ministry of Education Youth Invention Award and Taiwan Top Ten Information Talent Award. Has deeply studied blockchain applications over the years and led a blockchain technology team to develop systems for health big data and agricultural traceability projects.

Mo Bing: Chinese, PhD in Engineering, post-doctor. Research professor of Korea University, expert in the IoT, expert in integrated circuits, senior member of the Chinese Society of Micro-Nano Technology, IEEE member. Evaluation expert of science and technology programs at Fujian Province Science and Technology Department, evaluation expert of science and technology programs at Jiangxi Province Science and Technology Department, Director of Xiamen City Integrated Circuit Association. At present, he has presided over 10 scientific research projects, published more than 20 articles and applied for 18 invention patents. Since 2015, he has been mainly engaged in research of integrated circuits and blockchain. A number of commercial chips have been successfully developed under his guidance.

Wei Songjie: Chinese, Doctor of Engineering (graduated from the University of Delaware), blockchain technology expert in the field of computer network protocol and application, network and information security. Has published more than 20 papers and applied for 7 invention patents. Previously worked at Google, Qualcomm, Bloomberg and many other high-tech companies in the United States, served as R&D engineer and technical expert; has a wealth of experience in

computer system design, product development and project management.

Shan Liang: Chinese, graduated from KOREATECH (Korea University of Technology and Education) Mechanical Engineering Department, Venture Capital PhD, GM of Walton Chain Technology Co., Ltd. (Korea), Chinese Market Manager of the heating component manufacturer NHTECH (a subsidiary of Samsung SDI), economic group leader of the Friendship Association of Chinese Doctoral Students in Korea.

Chen Zhangrong: Chinese, graduated in Business Management, received a BBA degree in Armstrong University (USA), leader of Chinese clothing & accessories industry, China's well-known business mentor, guest of the CCTV2 "Win in China" show in 2008. Researcher in the field of thinking training for "Practical Business Intelligence" e-commerce and "MONEY&YOU" course, expert on success for "Profit Model" course. Has a wealth of practical experience in business management, market research, channel construction, business cooperation and business models.

Lin Herui: Chinese, successively served as Nokia R&D Manager, Product Manager and Microsoft Hardware Department Supply Chain Director. In 2014, started to set up a number of IoT enterprises and laid out the IoT production chain. Products and services developed under his guidance are very popular.

Zhao Haiming: Chinese, Doctor of Chemical Conductive Polymers of Sungkyunkwan University, core member of Korea BK21th conductive polymer project, researcher of Korea Gyeonggi Institute of Sensor, researcher of ECO NCTech Co., Ltd. (Korea), Vice President of the Chinese Chamber of Commerce (Korea). He has been engaged in transfer of semiconductor, sensor and other technologies in South Korea.

Liu Cai: Chinese, Master of Engineering, has 12 years of experience in design and verification of VLSI and a wealth of practical project experience in RFID chip design process, SoC architecture, digital-analog hybrid circuit design, including algorithm design, RTL design, simulation verification, FPGA prototype verification, DC synthesis, back-end PR, package testing, etc. Has led a team to complete the development of a variety of navigation and positioning baseband chips and communication

baseband chips, finished a series of AES, DES and other encryption module designs, won the first prize of GNSS and LBS Association of China for scientific and technological progress. Expert in the consensus mechanism principle of blockchain and the related asymmetric encryption algorithm.

Yang Feng: Chinese, Master of Engineering, worked at ZTE. Artificial intelligence expert, integrated circuit expert. Has 12 years of experience in VLSI research and development, architecture design and verification and 5 years of research experience in artificial intelligence and the genetic algorithm. Has won the Shenzhen Science and Technology Innovation Award. Has done an in-depth research on the principle and realization of the RFID technology, the underlying infrastructure of blockchain, smart contracts and the consensus mechanism algorithm.

Guo Jianping: Chinese, Doctor of Engineering (graduated from the Chinese University of Hong Kong), IEEE senior member, integrated circuit expert. Has published more than 40 international journal & conference papers in the field of IC design and applied for 16 patents in China.

Huang Ruimin: Chinese, Doctor of Engineering (graduated from the University of Freiburg, Germany), integrated circuit expert. Mainly explores digital signal processing circuit and system implementation, works on R&D of digital signal processing technology for a long time.

Guo Rongxin: Chinese, Master of Engineering. Has more than 10 years of experience in design and development of hardware and software for embedded systems, works on R&D of RFID and blockchain in the IoT for a long time.

Li Shuai: Chinese, Master of Engineering, research focus: network security and the blockchain access authentication technology. The project on blockchain distributed authentication completed under his direction won the final first prize of the “2016 National Cryptography Technology Competition”.

Huang Hongtai: Chinese, Bachelor of Engineering, has five years of experience in WEB front and back-end development, develops IoT and educational information platforms for a long time. Has a strong interest in the blockchain technology.

Liu Dongxin: Chinese, received an MBA from China Europe International Business School, strategic management consulting expert, investment and financing expert. Research interest: the impact of the blockchain technology on the financial sector.

6.2 Angel Investors

Song Guoping: Doctor of Medicine, President of Chinese Chamber of Commerce (Korea), Director of Beijing Overseas Friendship Association, representative of Ping An International Co., Ltd., representative of Oriental Xu Fu Anti-Aging Center, Representative of Sumei Beauty Shaping.

Qiu Jun: Chairman of Shenzhen Hongtao Fund Management Co., Ltd., Vice President of Shenzhen Shanwei Chamber of Commerce. Has 20 years of capital market investment experience, experienced many magnificent market changes, achieved a number of classic investment cases, including SMIC, China Merchants Securities and Guangdong Danxia Biopharm, etc. Guangdong Danxia Biopharm was acknowledged as one of the top ten successful cases of biopharmaceutical investment in 2016.

Yan Xiaoqian: Chairman of Kaltendin Clothing Co., Ltd., Executive Vice President of Shenzhen Shanwei Chamber of Commerce.

Lin Jingwei: Director of Guangzhou Jiuying Investment Management Co., Ltd., received a master's degree in Senior Financial Accounting and an EMBA degree from Sun Yat-sen University; has 27 years of work experience at large state-owned enterprises in China and abroad and more than 15 years of work experience as Secretary of the Board of Directors, Chief Financial Officer and Deputy General Manager of large Chinese state-owned enterprises, has been

in charge of enterprise listing, capital operation, investment, financing and financial management for a long time. Has a wealth of experience in capital operation and financial management. Has qualifications for Secretary of the Board of Directors or Independent Director of listed companies.

He Honglian: Director of the Waltonchain Investment Division, Certified Public Accountant, received an MBA degree from Xiamen University. Previously served as Investment Center Manager of Meiya Pico, currently leads the Waltonchain investment team to research and plan investment in the field of the IoT and integrated circuits.

7 References

1. A. Tapscott, D. Tapscott, How blockchain is changing finance, Harvard Business Review, 2017.
2. T. Stein, Supply chain with blockchain — showcase RFID, Faizod, 2017
3. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org, 2009.
4. R. Hackett, The financial tech revolution will be tokenized, Fortune, 2017.
5. C. Swedberg, Blockchain secures document authenticity with smartrac's dLoc solution, RFID Journal, 2016.
6. D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, Sequences II: Methods in Communication, Security and Computer Science, 1993.
7. A. Legay, M. Bozga, Formal modeling and analysis of timed systems, Springer International Publishing AG, 2014.
8. A. Back, Hashcash — a denial of service counter-measure, Hashcash.org, 2002.
9. B. Dickson, Blockchain has the potential to revolutionize the supply chain, Aol Tech, 2016.
10. KCDSA Task Force Team, The Korean certificate-based digital signature algorithm, IEEE Standard Specifications for Public-Key Cryptography, 1998.
11. J. Donaldson, Mojix brings transformational RFID, big data analytics and blockchain technology to NRF Retail's Big Show, Mojix.com, 2017.
12. R. T. Clemen, Incentive contracts and strictly proper scoring rules. Test, 2002.52
13. J.-Y. Jaffray, E. Karni, Elicitation of subjective probabilities when the initial endowment is unobservable, Journal of Risk and Uncertainty, 1999.
14. Blockchain Luxembourg S.A., https://blockchain.info.
15. J. Gong, Blockchain society-decoding global blockchain application and investment cases, CITIC Press Group, 2016.

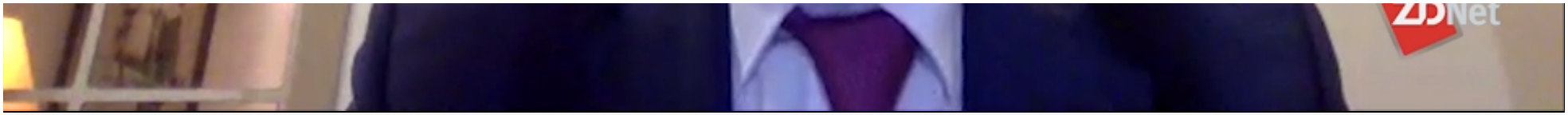
16. D. Johnston et al., The general theory of decentralized applications, Dapps,2015.
17. P. Sztorc, Peer-to-peer oracle system and prediction marketplace, 2015.
18. R. Hanson, Logarithmic market scoring rules for modular combinatorial information aggregation, Journal of Prediction Markets, 2002.
19. 潘炜迪, 浅谈我国虚拟货币发展现状及未来, 企业导报, 2016.

MUST READ: Windows 10 October update delete your files? This tool might recover them

Qure.ai launches AI system to read head CT scans and find abnormalities

Fractal Analytics is funding the Qure.ai efforts and plans to invest up to $30 million over the next few years. Qure.ai's dataset and AI validation are published.

By Larry Dignan | April 26, 2018 -- 19:54 GMT (12:54 PDT) | Topic: Artificial Intelligence



Qure.ai, a healthcare startup funded by Fractal Analytics, has launched an artificial intelligence based system to identify abnormalities in head CT scans.

The effort is the latest example of how AI and machine learning are working through the health care industry. Qure.ai released a clinical validation study (http://headctstudy.qure.ai/) showing its algorithms were nearly on par with radiologists in a sample of 21,000 patients.

In addition, Qure.ai is making a dataset of 500 AI analyzed head CT scans available for download.

Qure.ai is aimed at a key supply and demand choke point in the healthcare system. Images from MRIs and radiology are outpacing the humans available to interpret them. The general idea is that AI can be used to interpret results and free physicians up for patient care. Speed is also an issue when it comes to interpreting a head CT scan of a stroke victim.

Fractal Analytics buys Final Mile as AI, data science meld with behavioral science (https://www.zdnet.com/article/fractal-analytics-buys-final-mile-as-ai-data-science-meld-with-behavioral-science/) | Death and data science: How machine learning can improve end-of-life care (https://www.zdnet.com/article/death-and-data-science-how-machine-learning-can-impact-hospice-referrals-improve-last-days-of-life/)

The Qure.ai model was trained with 313,318 anonymized head CT scans and their clinical reports. Out of that sample, 31,095 scans were used to validate the algorithms. From there, AI was clinically validated on 491 CT scans and compared against a panel of three radiologists.

According to Qure.ai, its algorithms were more than 95 percent accurate.

The results were published via Cornell University and the paper is publicly available along with the data set.

Fractal Analytics is planning to invest up to $30 million in Qure.ai in the next few years.

Here's what a Qure.ai AI-driven CT analysis looks like.

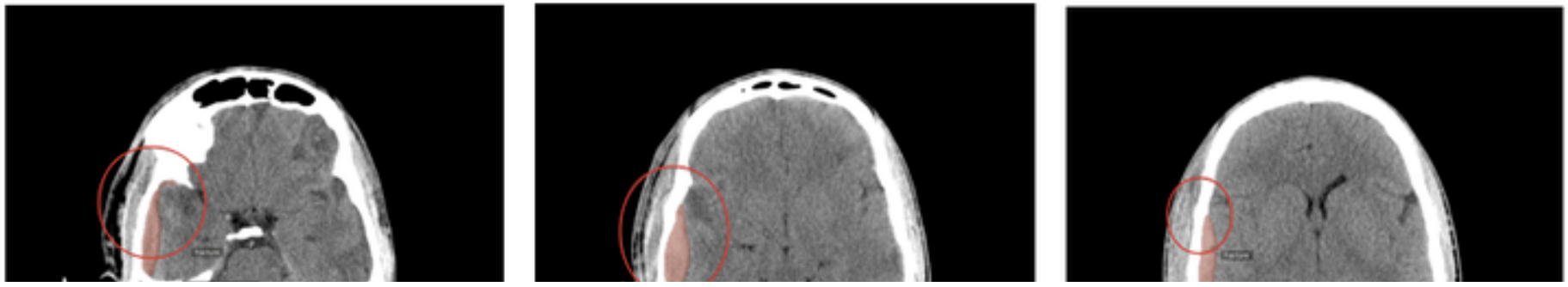
qure@qure.ai

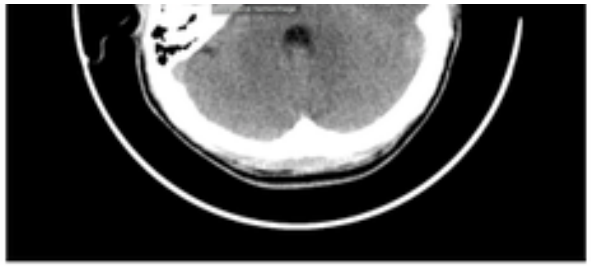
Raheja titanium, off western exp hwy,
Goregaon east, Mumbai, 400076

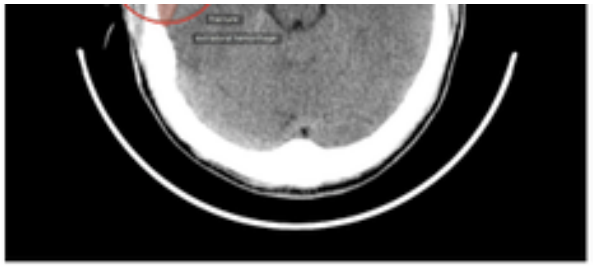
Patient:	abc xyz	D.O.B :	01/05/1939
Radiologist:		Exam Date:	2017-11-23
Referring physician:	abc xyz		

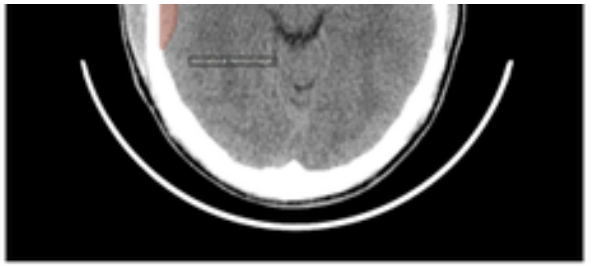
Head CT Report

- Extradural hemorrhage of 20.06 ml in right temporal region.
- Fracture.
- Midline shift.
- Mass effect.









Electronic signature